Cyber presentation for norima

Oslo /December 5 - 2018

STROZ FRIEDBERG
an Aon company

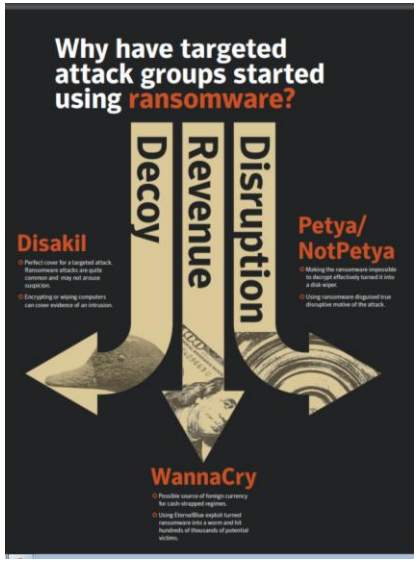
AON
Empower Results®

Agenda

1	Setting the Scene
2	The Importance of the Right Approach
3	Are you aware of the changing exposure?
4	The components of Cyber Coverage
5	The Cyber Insurance Market
6	Key Takeaways

Setting the scene

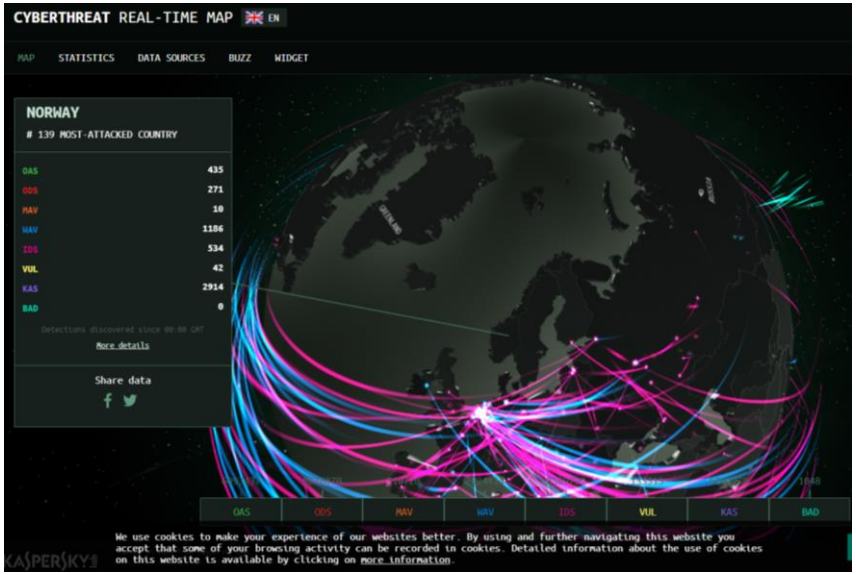
The Evolving Cyber Threat



"We are at the beginning of a revolution that is fundamentally changing the way we live, work, and relate to one another. In its scale, scope and complexity, what I consider to be the fourth industrial revolution is unlike anything humankind has experienced before."

Klaus Schwab

Founder and chairman World Economic Forum

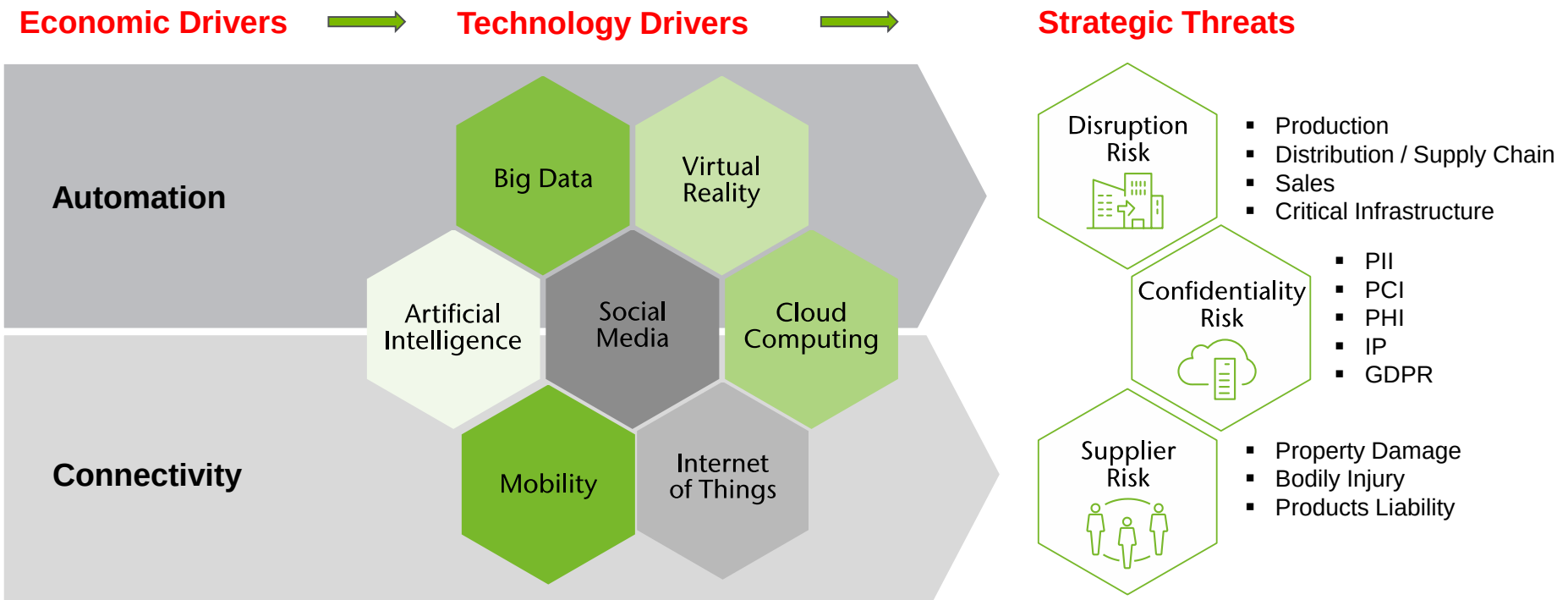


Norway is listed as the 139 most attacked country in the world (SE 53, DK 95 FI 116)

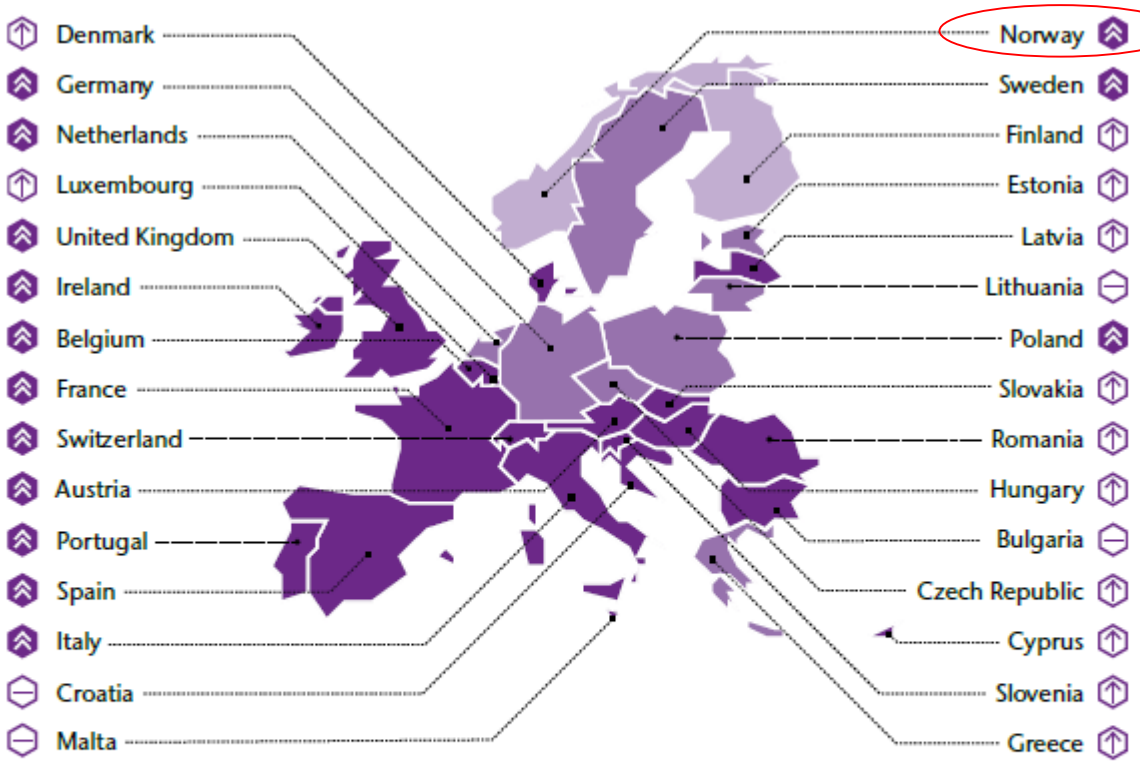
Kaspersky real time map.

The Evolving Cyber Threat

Organizations across all industries continue to invest in deploying digital technologies to stay competitive and drive quality and efficiency objectives



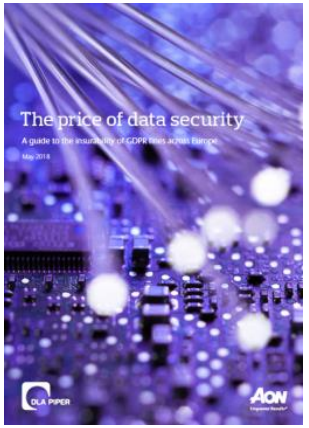
GDPR heat map – DLA Piper



Key

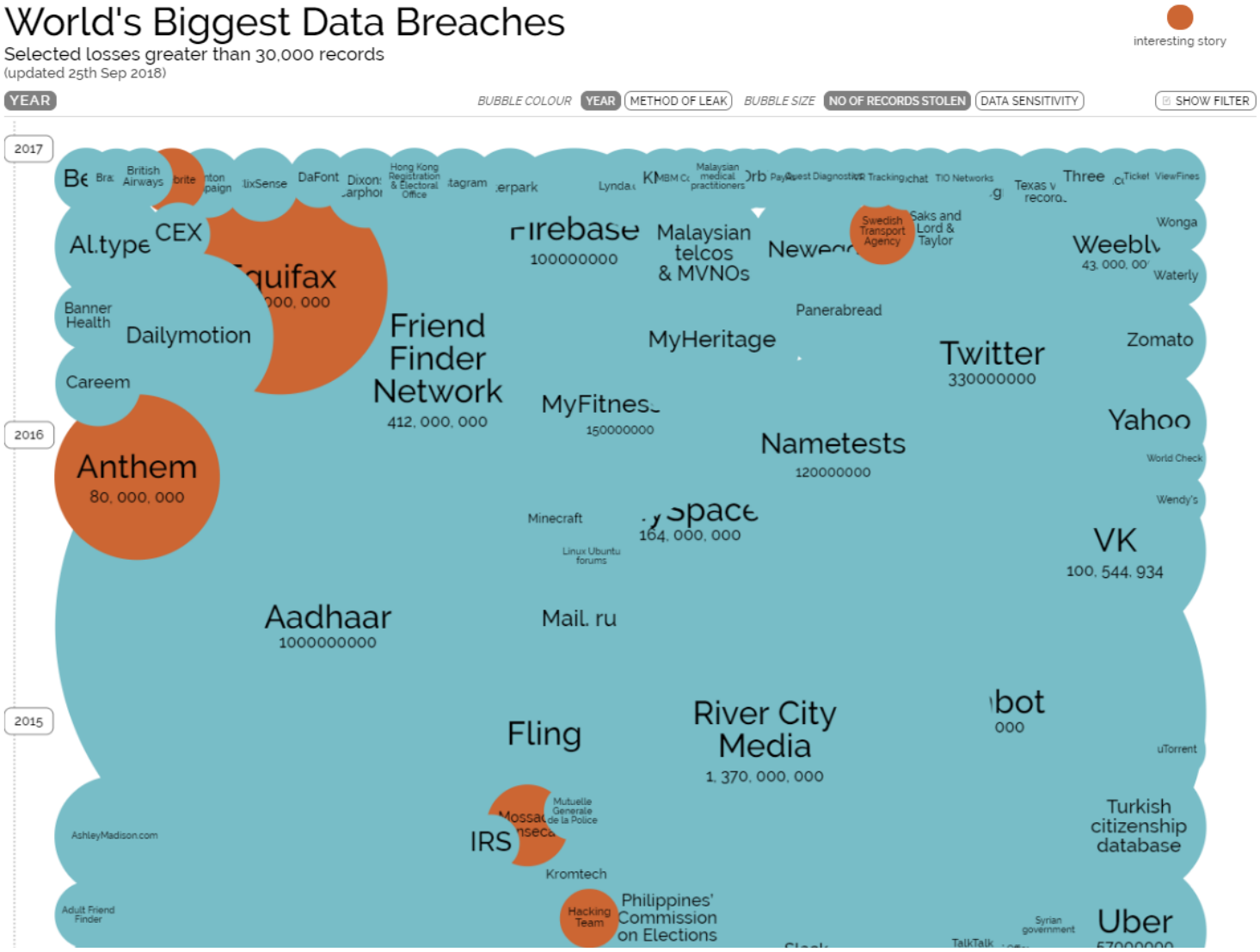
Insurability of GDPR fines	Insurable	Unclear	Not insurable[1]
Data regulatory environment[2]	High	Fairly high	Moderate

Source: DLA Piper 16 May 2018



www.aon.com/GDPRfinesguide

World’s Biggest Data Breaches



Click Me!

Notable NotPetya Commercial Impacts

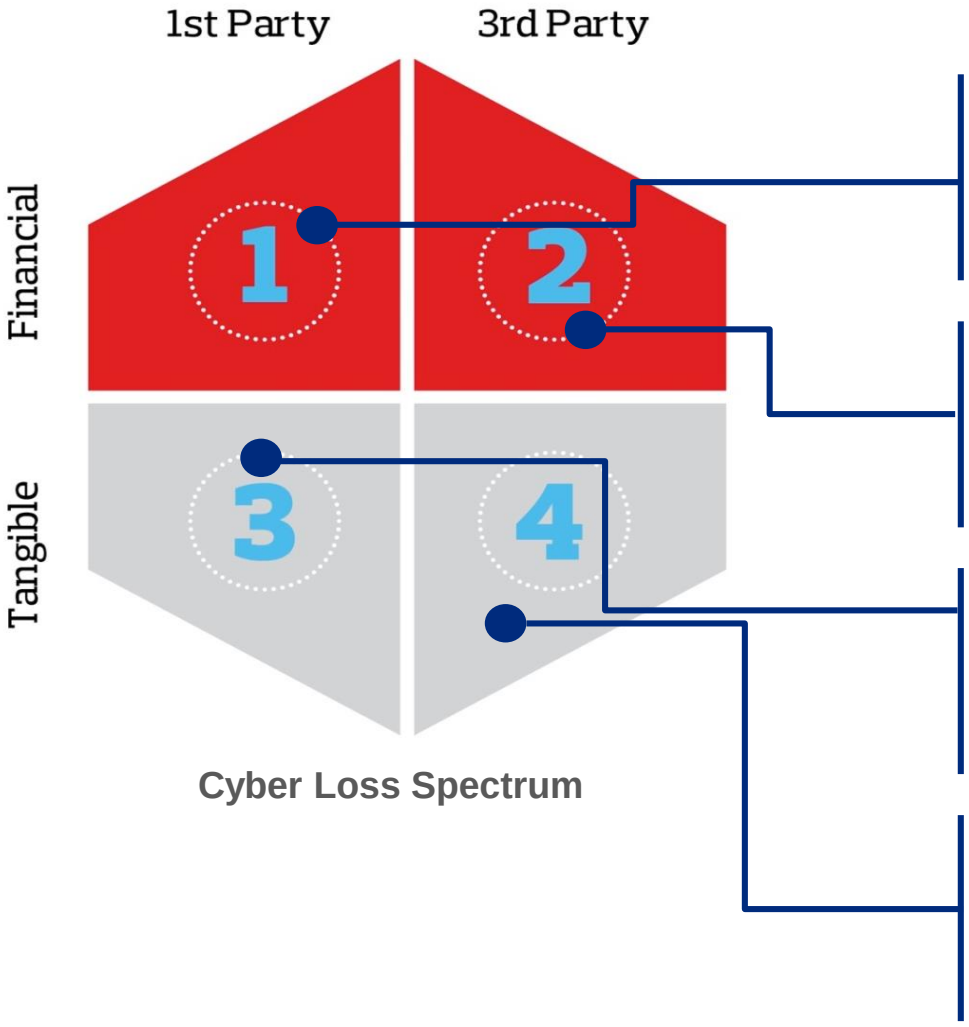
Organisation	Commercial Impact	Financial Components	Source
A.P. Moller – Maersk	$250-300 million	Earnings Reduction	Q4 2017 Financials
Beiersdorf AG	Minimal sales impact €15 million	€35mm sales shifted Q2 to Q3 Additional expenses	Q2 2017 Financials Q4 2017 Earnings Call
FedEx (TNT Express)	$400 million	Earnings Reduction	Q3 2018 Financials
Merck & Co.	$460 million $355 million	2017, 2018 Sales Reduction Additional Expenses	Q4 2017 Financials Q1 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 $30 million	2017 Sales Reduction Additional Expenses	Q1 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 Data Breach / Intrusion Commercial Impacts

Organisation	Commercial Impact	Financial Components	Source
Anthem	$263 million	Gross Expenses ($148mm) Security Improvements ($115mm)	Regulator Settlement U.S. District Court
Equifax	$242.7 million $439 million	Gross Expenses to Date Total Estimated Gross Expenses	Q1 2018 Earnings Release Q1 2018 Earnings Call
Global Payments	$141 million	Gross Expenses	10-K Filing 2015
Heartland Payment Systems	$148 million	Gross Expenses	10-K Filing 2013
The Home Depot	$298 million	Gross Expenses	10-K Filing 2017
Sony Corporation (2011)	~$171 million ¥14 billion	Consolidated Operating Income	2010 Forecast Revision
Sony Corporation (2014)	~$41 million ¥4.9 billion	Investigation & Remediation Expenses	Q4 2014 Financials
Target Corporation	$292 million	Gross Expenses	10-K Filing 2017
The TJX Companies	$187 million	Gross Expenses	10-K Filings
Yahoo! Inc. (Altaba Inc.)	$350 million $35 million $80 million	Reduced Acquisition Price SEC Fine Securities Class Action	Verizon Press Release SEC Press Release U.S. District Court

The importance of the right approach

Cyber Risk may impact All Loss Quadrants



Any major cyber event will result in

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

Third parties will seek to recover

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

Physical damage is possible

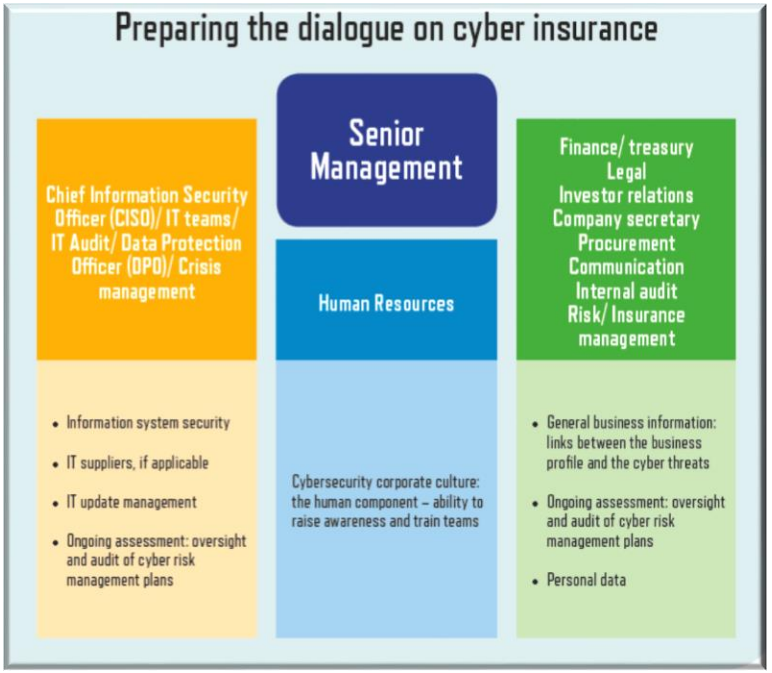
- Property damage
- Bodily injury

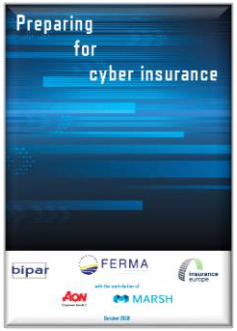
Physical damage may cascade to others

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

Assessing and understanding cyber exposures

- Any organisation wishing to implement some form of risk mitigation for its cyber risks, must first **assess as accurately as possible its exposures and potential vulnerabilities.**
- As a first step, the organisation needs to conduct **internal research and build a picture of its cyber risks and how it manages them**.
- Conducting this research can be challenging, especially for organisations that do not have a dedicated function in charge of risk management or the resources to outsource it.
- May not be obvious which functions within the organization to ask or **which questions to ask**.

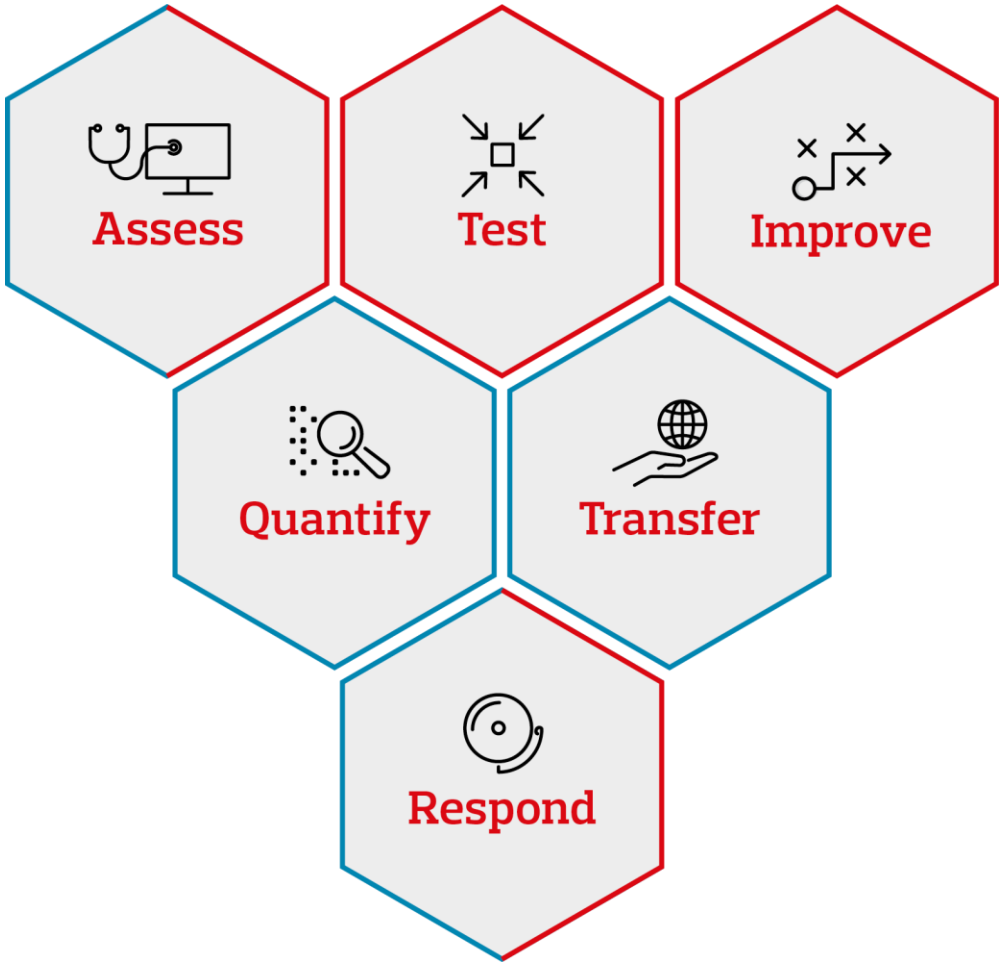




FERMA & partners report

Understanding Cyber

Cyber Risk Management



Cybersecurity Management

Are you on top of the changing exposure?

Are you on top of the shifting exposure ensuing from the digital revolution?

One of the most visible effects of the digitalization is the dramatic shift in a typical company's value > from tangible to intangible. A typical distribution of value today is 80% intangible, while 40 years ago it was the reverse…

(The fourth revolution blog)

A recent study amongst your peers shows:

- Companies commit four times more insurance spend on protecting physical assets than intangible.
- The impact of business disruption to cyber assets is 50% greater than to property, plant and equipment assets (PP&E)
- Only 15% of the probable maximum loss (PML) potential for information assets is covered by insurance; almost two thirds (60%) of total PP&E asset values are protected
- Only 30% of respondents state they are 'fully aware' of the economic and legal consequences of an international data breach or security exploit

2017 EMEA Cyber Risk Transfer Comparison Report

Some words on Cyber Insurance Coverage

Scope of a “typical” Cyber Insurance Coverage

Defence Costs + Damages + Regulator Fines	Insured’s Loss	Response
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) ▪ Data Restoration	**Expense / Service Sections** ▪ Crisis Management ▪ Breach-related Legal Advice ▪ Call Center ▪ Credit Monitoring, Identity Monitoring, ID Theft Insurance ▪ Cyber Extortion Payments

Cyber Coverage in Relation to Other Lines of Insurance

Silent CYBER

- Remote hacking of Jeep resulted in Chrysler recalling 1.4M vehicles
- Internet of Things (“IoT”) creates additional products exposure

- Zurich Insurance Co. v. Sony Corp. of America - ISO Exclusion – Access Or Disclosure of Confidential or Personal Information and Data-Related Liability
- AIG announces that they will affirmatively cover Cyber bodily injury subject to AP and additional underwriting

- Potential overlap with Business Interruption (“BI”), Dependent BI and Data Restoration coverage
- FM Global Cyber solution – cutting back on capacity, AP
- Malware / DDOS attacks do not constitute “physical perils” and do not damage “tangible property”

- Social Engineering Losses – Cyber policies exclude loss of monies
- Crime policies require intent – theft of money, securities or tangible property

- Cyber extortion claims filed under K&R policies → Guaranteed Cost, though scramble for access to experienced vendors
- As multi-year K&R policies expire, carriers are affirmatively excluding cyber

- Home Depot data breach-related derivative lawsuit – settlement required HD to adopt certain cyber-security related corporate governance reforms (and pay up to $1.125M in plaintiff’s attorneys’ fees)
- Equifax follow-on D&O claims arising out of a network security breach

Cyber Insurance Market

2018 Cyber Market trending Snapshot

Capacity is continuing to grow across geographies	Coverage continues to evolve and become more valuable for Insureds	Stronger data is being gathered as more breaches are reported	Retentions are being reviewed since WannaCry, NotPetya and Equifax incidents	Pricing trends are competitive, but increasing for some industries
▪ Over 75 unique Insurers providing E&O / Cyber Liability capacity ▪ Capacity is available locally (primary and excess), London (primary and excess) and Bermuda (excess only, generally excess of $50M) ▪ Growing number of Insurers developing appetites for large, complex risks ▪ There is over $700M in theoretical capacity available in the E&O/Cyber market place	▪ 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	▪ Increased ransomware activity and business interruption concerns ▪ 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 modeling purposes ▪ Increasingly punitive legal and regulatory environment	▪ 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	▪ Average premium rates reflect a decline – however dependent on industry, claims history 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*

International Cyber Insurance Market

Nordic Market Carriers

LOCAL NORDIC

- Alm Brand
- Codan / TH
- Gjensidige
- IF
- OP
- Protector
- *RiskPoint (MGA)*
- Storebrand
- TopDanmark
- Tryg / Moderna

Nordic Market

Behavior

- Careful, increasing trend but only slowly so
- Prefer first party loss
- Prefer to bundle

Capacity

- Capacity is available but not automatically deployed, so whilst we have seen recent EMEA placements attract in xs of 600 MUSD in capacity (!) we typically see smaller limits in Norway, generally around EUR 15 Million for the largest accounts and then we typically see requests for NOK 50 M or NOK 100M options for the accounts in the next tier.
- For SME, typically bought in a package from the local insurers such as Gjensidge, Tryg, or If, we see lower limits: MNOK 10 to MNOK 25 for example.
- Availability of limit depends on exposure and quality of data and assessment.
- For a few of our largest Nordic clients we have placed limits between EUR 50-200 Million.

2018 Purchasing Trends

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 organisations 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, organisations' 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**

Key Takeaways

Key Takeaways

Business Disruption

- **Financial statement impact of breaches shift to business disruption**
  - Denial of service & ransomware attacks can be more severe than data breaches
  - 2017 WannaCry and NotPetya ransomware attacks resulted in extended business disruption

NOT a FI issue

- **Everyone is at risk**
  - Traditional non-internet based businesses can be used as conduits in attacks or be massively affected despite being only collateral damage (Maersk – ransomware demand was 300$)
  - From credit card & social security data theft to global business

Thoughtful Approach

- **Understanding risk is key**
  - Understand exposure and steer investment where it has best effect on your total cost of risk:
    - risk assessment,
    - risk transfer,
    - crisis response
  - Who do I want to share that knowledge with

D&O Attention

- **D&O follow-on claims represent an increasing exposure**
  - Attracting internal D&O attention.

Contact List

Fredrik Forsström
Nordic Chief Broking Officer
+45 61306413
Fredrik.forsstrom@aon.com

Christian Rindlisbacher
Norwegian Cyber Champion
+47 91 79 48 15
christian.rindlisbacher@aon.no

Connect: aon.com - Cyber Solutions