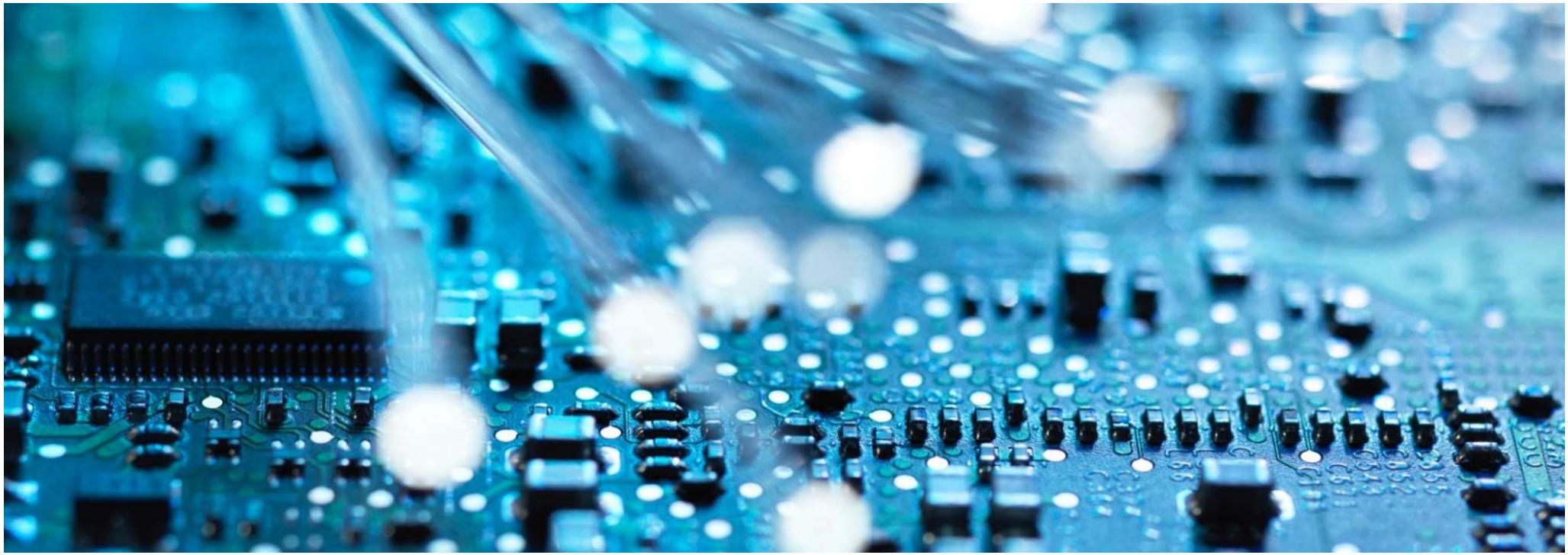


Cyber – an overview

Prepared by Aon's Cyber Solutions
Proprietary & Confidential

Empower Results®

Global Risk Management Survey Risk Ranking

1 Economic slowdown/ slow recovery	2 Damage to reputation/brand	3 Accelerated rates of change in market factors	4 Business interruption	5 Increasing competition	6 Cyber attacks/ data breach	7 Commodity price risk
8 Cash flow/ liquidity risk	9 Failure to innovate/ meet customer needs	10 Regulatory/ legislative changes	11 Failure to attract or retain top talent	12 Distribution or supply chain failure	13 Capital availability/ credit risk	14 Disruptive technologies/ innovation
15 Political risk/ uncertainties	16 Exchange rate fluctuation	17 Concentration risk (product, people, geography)	18 Workforce shortage	19 Counter-party credit risk	20 Aging workforce and related health issues	21 Property damage
22 Environmental risk	23 Weather/ natural disasters	24 Third party liability (incl. E&O)	25 Technology failure/ system failure	26 Major project failure	27 Failure of disaster recovery plan/ business continuity plan	28 Injury to workers
29 Failure to implement or communicate strategy	30 Asset value volatility	31 Climate change	32 Absenteeism	33 Merger/ acquisition/ restructuring	34 Loss of intellectual property/data	35 Interest rate fluctuation
36 Geopolitical volatility*	37 Growing burden and consequences of governance/ compliance	38 Globalization/ emerging markets	39 Corporate social responsibility/ sustainability	40 Product recall	41 Impact of digital economy*	42 Impact of Brexit*
43 Lack of technology infrastructure to support business needs	44 Directors & Officers personal liability	45 Inadequate succession planning	46 Natural resource scarcity/availability of raw materials	47 Fraud	48 GDPR requirements*	49 Rising healthcare cost*
50 Unethical behaviour	51 Outsourcing	52 Theft	53 Resource allocation	54 Workforce generation gaps*	55 Terrorism/sabotage	56 Safety & Pharmacovigilance*
57 Share price volatility	58 Embezzlement	59 Impact of Artificial Intelligence (AI)*	60 Pandemic risk/ health crises	61 Harassment/ discrimination	62 Sovereign debt	63 Pension scheme funding
64 Gender pay gap*	65 Impact of Blockchain tech*	66 Kidnap & ransom	67 Extortion	68 Off Label Promotion*	69 Impact of cryptocurrencies*	

Insurable | Partially insurable | Uninsurable

* Denotes new risks added to the Global Risk Management Survey for the first time

AON
Empower Results®

Aon's 2019 Cyber Security Risk Report – What's Now and What's Next

8 Key Risk Areas

RISK 1 Technology

Embracing Digital Transformation Creates New and Unanticipated Risks

RISK 2 Supply Chain

Supply chain security wake-up calls grow more insistent

RISK 3 IoT

IoT is everywhere, and it is creating more risks than organisations realize

RISK 4 Business Operations

Technology for operational efficiencies can lead to security deficiencies that disrupt organisations

RISK 5 Employees

Excess privileges and shadow IT increase employee risk

RISK 6 Mergers & Acquisitions

Vulnerabilities from deal targets increases as dramatically as M&A value

RISK 7 Regulatory

Managing the intersection of cyber security policy and enforcement

RISK 8 Board of Directors

Directors and Officers face growing personal liability relative to cyber security oversight

Aon's 2019 Cyber Security Risk Report

Threat Landscape of Mid-Market Organisations

Mid-market organisations are increasingly the focus of cyber attacks and often serve as a launch pad for bigger campaigns.

Despite this growing threat level, many remain ill-prepared for cyber attacks, showing lower than average maturity levels.

55% of security alerts are investigated by mid-market organisations[1]

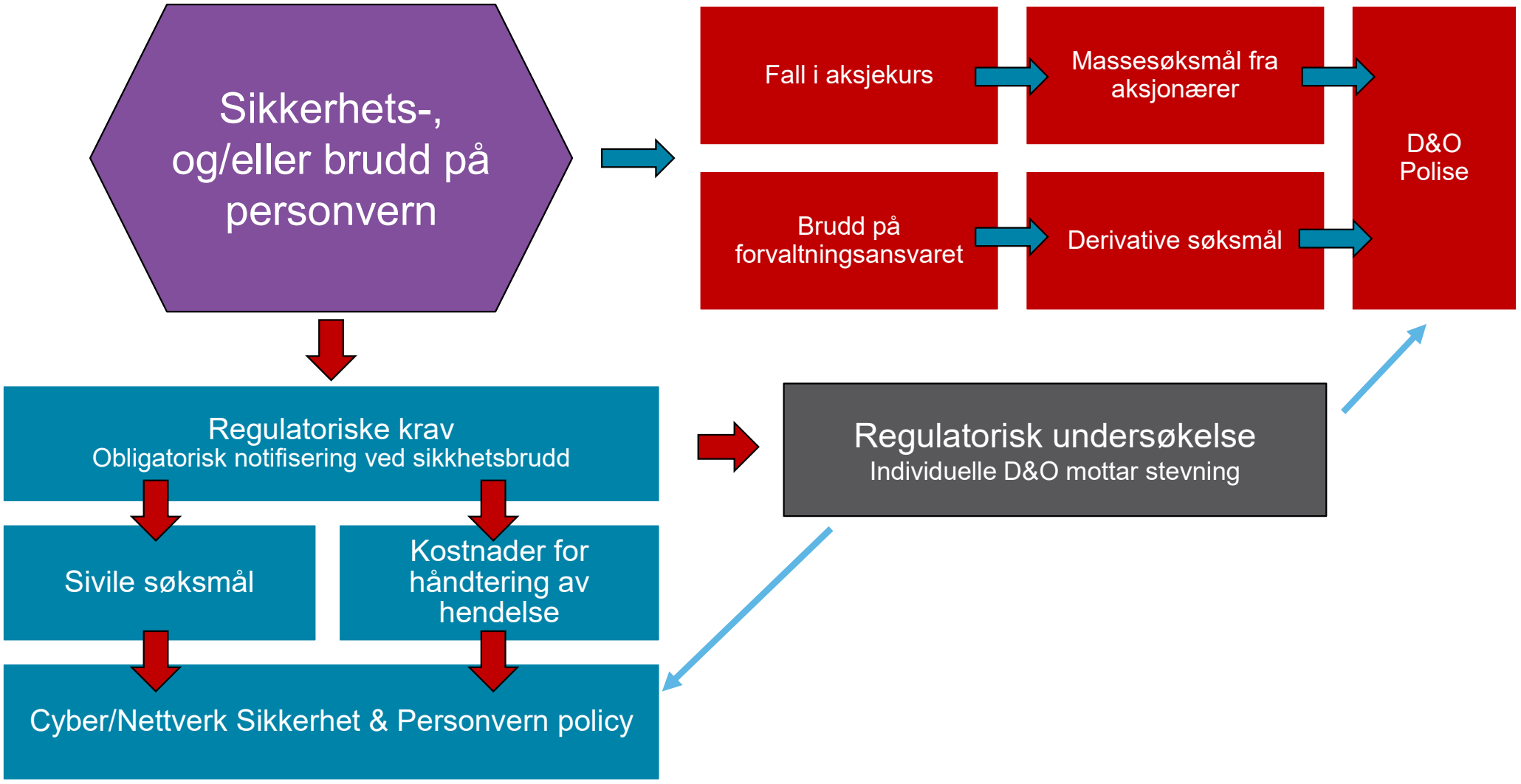
53% of mid-market organisations in 26 countries experienced a breach[1]

54% of all cyber attacks result in financial damages of more then $500,000[1]

20% of mid-market organisations reported breaches costing $1 million - $2.5 million[1]

[1] 2018 Cisco Cybersecurity Report: Special Edition SMB

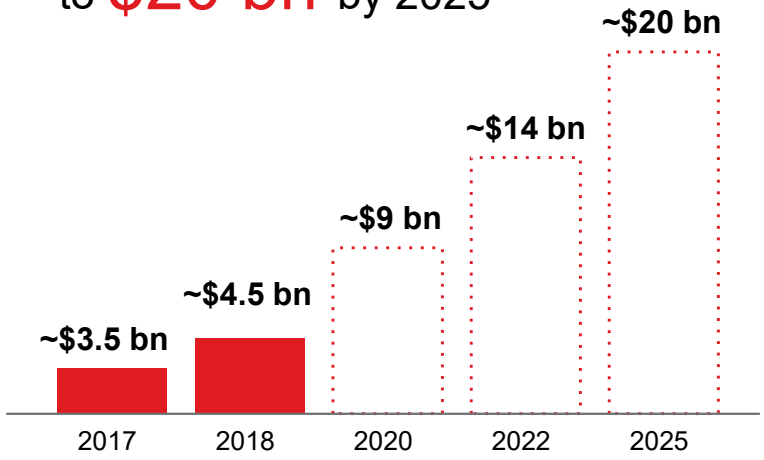
Cyberrisiko er et ledelsesansvar

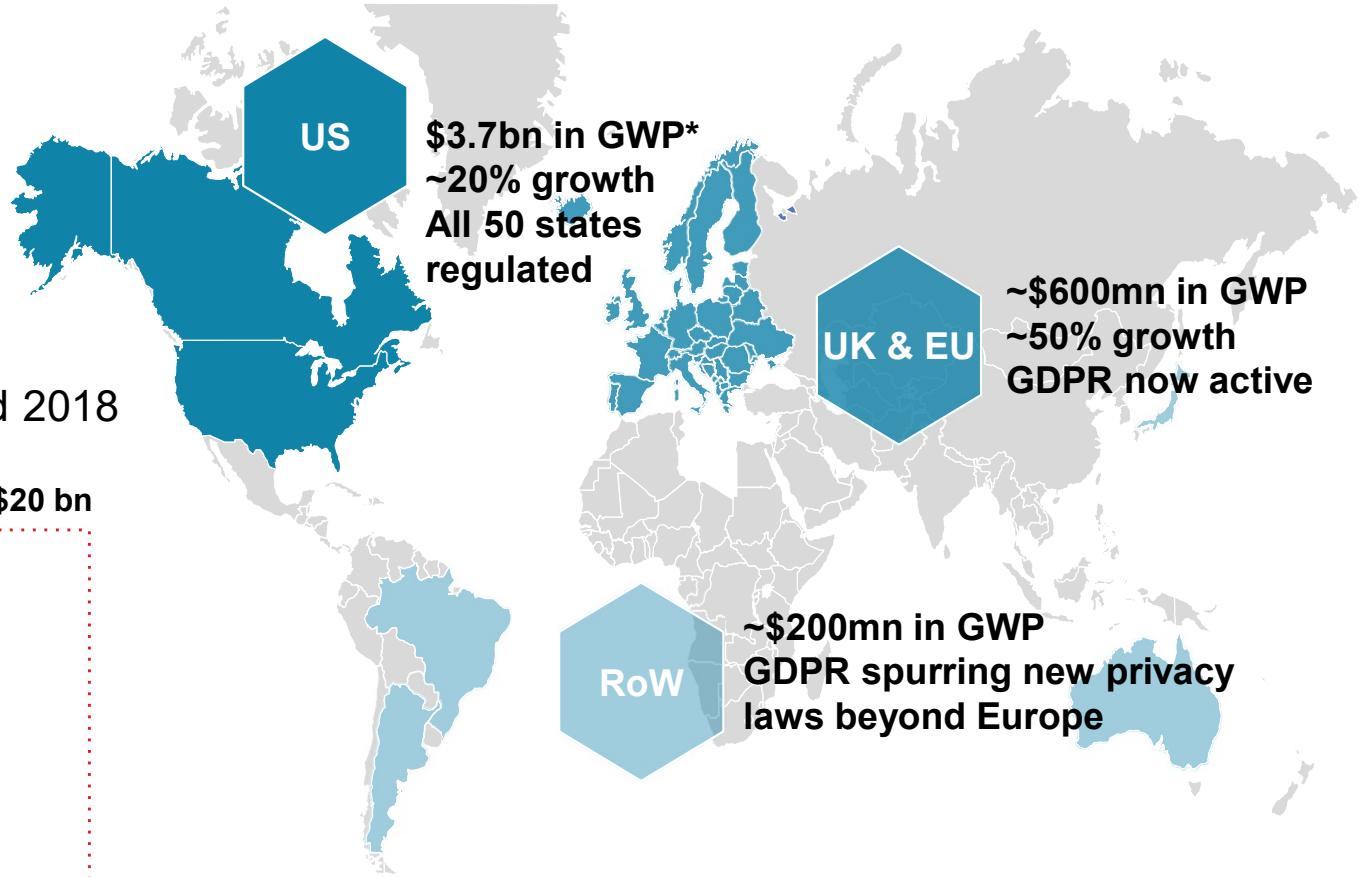


The Take-Up of Cyber Insurance is on the Rise

Cyber insurance

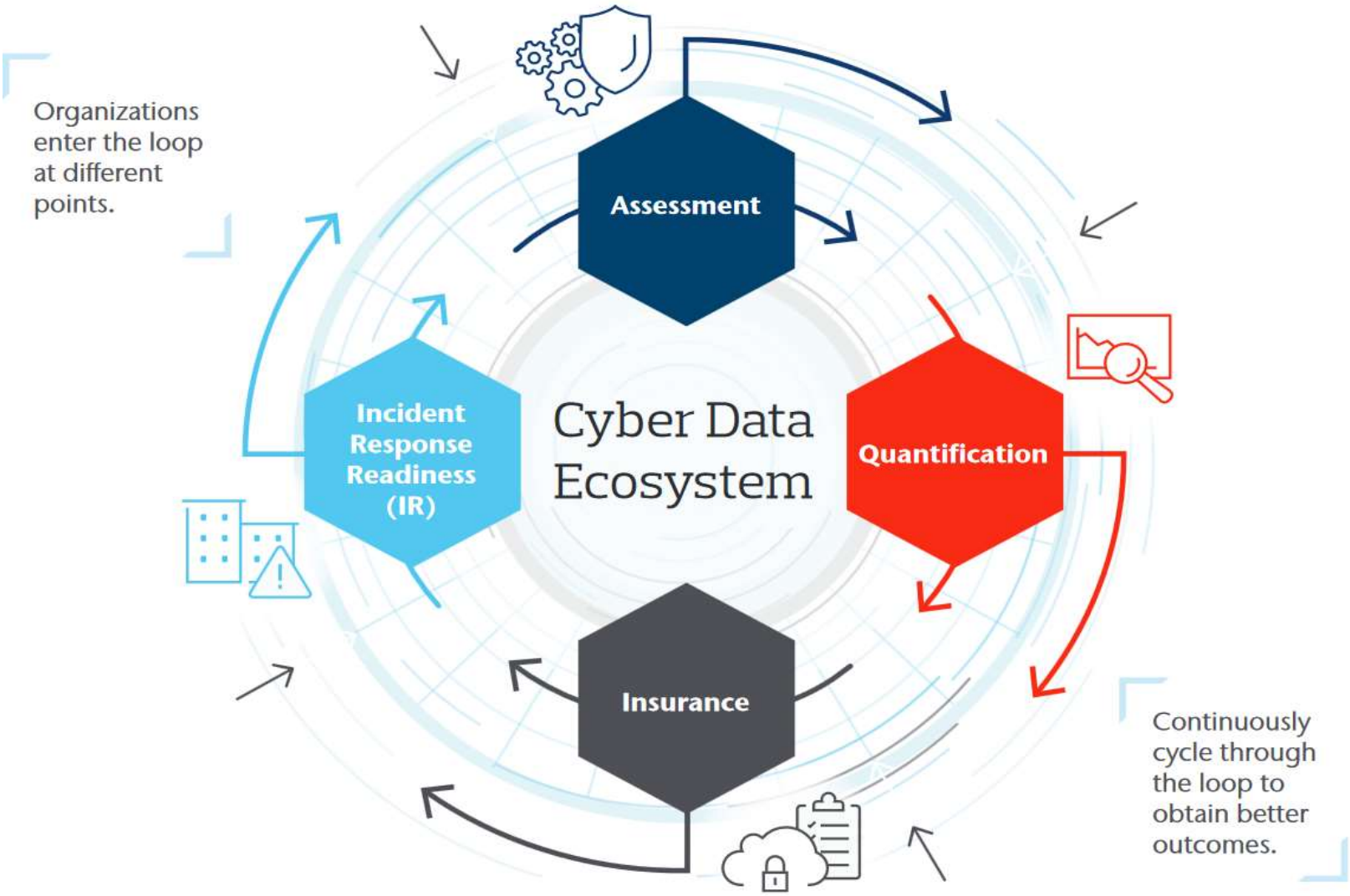
projected to grow
from $4.5 bn at year-end 2018
to $20 bn by 2025





Sources: Aon proprietary data; Aon Inpoint; 2017 "Global Cyber Risk Transfer Comparison Report," Aon/Ponemon Institute; 2016 Cyber—The Fast Moving Target: Benchmarking views and attitudes by industry; Insurance Business America, PwC, The Betterley Report, Advisen, Allianz, Allied Market Research

The Cyber Loop: Managing cyber risk requires a circular strategy



Source: Aon's White Paper The Cyber Loop

Seek Shield Solve

Seek

We help clients to understand and quantify their risk.

- Assess your organisation's security posture
- Align with proven security frameworks
- Proactively test and hunt for malicious activity
- Quantify the potential financial damage from a cyber incident
- Provide prioritised action lists to improve your cyber resilience

Shield

We know how to protect an organisation and its critical assets.

- Protect your company from the financial loss of a cyber incident through cyber insurance
- Understand the risks of your investments
- Develop tailored security policies and standards
- Remediate vulnerabilities
- Provide strategic cyber security guidance and develop a programme

Solve

We search for the truth and help our clients recover quickly.

- Respond defensibly to an attack
- Minimise business interruption
- Use cutting edge forensics
- Effectively respond to your situation by deploying our team, drawn from the most respected cyber entities trained in the regulatory, financial and legal consequences of a breach
- Help maximise coverage and cost recuperation

CyQu Evaluation

Gain instant visibility

Upon completing CyQu, immediately receive your CyQu Score, a snapshot of your cyber maturity, and gain visibility into which control areas represent the greatest points of vulnerability. Within five to ten business days, receive your CyQu Report detailing prioritized risk mitigation and transfer strategies customized for your organization's environment and industry.

Help strengthen security / facilitate risk transfer

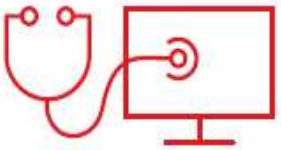
Establish stronger collaboration across internal risk and IT teams. Receive a detailed cyber risk management plan to help strengthen your risk posture and protect your balance sheet. Use your CyQu Report as market submission to streamline the insurance underwriting process.

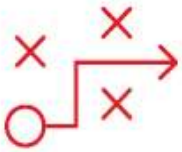
Benchmark against peers

Gain immediate insight into how your CyQu Score measures up against peers within your industry, by critical control area. Compare your CyQu Score to target scoring for your industry to understand where to prioritize mitigation strategies. Benchmarking is driven by Aon and Stroz Friedberg proprietary data and combined claims and incident response experience.

Next Step

Steps to Empower Security Improvement.





Complete CyQu

Current Stage: Complete CyQu

Enablers of Improvement

Prioritize Enablers of Improvement

Identify and prioritize improvement opportunities that should receive immediate focus to enhance the current level of security performance

Execute Strategies to Empower Improvement

Enhance Improved Cybersecurity

Validate and execute the improvement roadmap

Control Areas	Your CyQu	Quick Wins for Risk Reduction
Training	1.0	Mandate security training for all developers annually
Physical Penetration Testing	1.0	Engage third party for external penetration testing
Tampering and Alteration	1.0	Perform physical tampering inspections for all systems
Data Classification	1.0	Classify data regularly and during significant changes
Third Party Inventory	1.0	Maintain an inventory of all key 3rd party partners and suppliers

Markedssituasjon

Desto flere skader, desto bedre blir dataen for forsikringsselskapene.	Dekningen fortsetter å utvikle seg, og gir mer verdi for kundene	Kapasiteten fortsetter å vokse på kryss av geografi.	Egenandeler er under vurder vurdering	Prisutvikling er konkurransedyktig men økende for visse industrier.
▪ Kompleksiteten I sikkerhetsbrudd driver kostanden ved hendelseshåndtering hos den forsikrede. ▪ Skader og taps informasjon har medført bredere tilbudt dekning, og sikrere aktuar beregninger. ▪ Man ser et økt fokus fra regulatoriske myndigheter, med høyere sanksjoner. ▪ E&O skader er en av hovedårsaken til større tap hos forsikringsselskapene.	▪ Forsikringsselskapene fortsetter å oppdatere vilkårene sine for å møte behovet i markedet. ▪ Dekningsomfang fortsetter å utvide seg. ▪ Forsikringsselskapene differensierer seg med nye og bedre løsninger. ▪ Sterkt fokus på bruk av forhånds avtalte konsulenter ▪ Bredere dekning for systemfeil og betinget avbruddsløsning.	▪ Over 75 forsikringsselskaper tilbyr PI/Cyber kapasitet. ▪ Kapasitet er tilgjengelig lokalt, bade primær og excess kapasitet. ▪ Et økende antall forsikringsselskaper utvikler appetitt for store og komplekse risikoer. ▪ Teoretisk er der over 8 milliarder I kapasitet tilgjengelig I PI/Cyber markedet.	▪ Egenandeler på alle nivåer er tilgjengelig I markedet, men kan variere stort basert på industri, størrelse og unik eksponering. ▪ Ved å endre egenandelen kan må se bredere dekning og/eller fleksibilitet I prising.	▪ Man ser en gjennomsnittlig rate nedgang, men betinger industri, skadehistorikk, og omfang av dekning. ▪ Excess raten fortsetter å være konkurransedyktig med gode priser. ▪ Noen kunder har fått betydelig bedre dekning ved å betale høyere premie.

Note: Dette er en generell sammenfatning og kan variere basert på kunde, industri og størrelse.

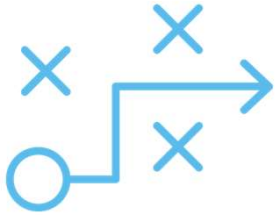
Key Pillars of a Cyber Insurance Policy

Prevention

- Pre-breach assessments
- Access to pre-vetted vendors
- Cybersecurity information

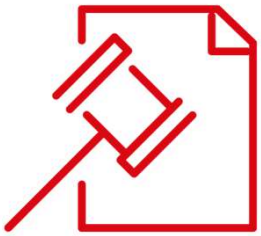
Assistance

- Forensic investigators
- Legal services
- Notification
- Credit Monitoring
- Call Center Services
- Crisis Management/Public Relations



Operations

- Costs incurred to keep or return the business to operational
- Loss of revenue, income, turnover
- Costs incurred to recreate/restore data and information



Liability

- Legal costs and damages from claims alleging privacy breach or network security failure

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

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

Contact List

Morten Landrø
Senior Broker
Broking
+47 92 22 33 55
morten.landro@aon.no

Connect: aon.com - Cyber Solutions