AON

OASC Conference

September 14th 2022

Presented by:

Ady Sharma

Covering the Complete Risk Management Spectrum

Helping to protect today and safeguard tomorrow

Our Unique Value

Digital Forensics & Incident Response

Solving your cyber events

Respond to the incident, create an investigation strategy, contain the incident while preserving evidence, and confidently communicate with your stakeholders

Find the smoking gun.

Security Advisory

Identifying your security weaknesses

Evaluate and remediate your vulnerabilities, determine your readiness to respond, and improve your organization's cyber resilience.

See your company like never before.

Testing

Illuminating your systems' vulnerabilities

Leverage real-world testing and simulations to help you better understand your weaknesses and strengthen your defenses.

Clear your way for peace of mind.

eDiscovery

Navigating the complex issues

Benefit from professional guidance through ever-changing technical and legal challenges.

Bring order to the disorder.

Investigations & Intelligence

Using knowledge to empower

Help protect your organization by applying traditional investigative techniques to the digital environment.

Protect your organization's brand.

Quantification

Optimizing your total cost of risk

Model cyber loss scenarios and stress test your current insurance limits to enhance your risk financing strategies.

Strategize for your company's future.

Broking

Securing your future

Protect your organization from the financial impact of a cyber incident.

Know it's not one size fits all.

Our People

Protectors and Problem Solvers

- Forensic computer analysts
- Penetration testers
- IT security engineers
- Information security analysts
- Security architects
- Former CISOs
- Fraud examiners
- Security risk consultants
- Investigators
- Criminologists
- Forensic accountants
- Governance & risk mgmt. professionals
- Privacy professionals
- Claims advocates
- Evidence Technicians
- Brokers
- CPAs

Oath Takers

- Former law enforcement*
- Former prosecutors
- AM Law 100 former partners

More than the Sum of Our Parts

- Former Big 4 Professionals
- Actuaries
- Statisticians
- Data analysts

* Includes former Head of the Cyber Division at FBI Headquarters and former founder of the FBI's computer crime squad in New York

Agenda

1

Setting the Scene (The Threat Landscape)

- All about ransomware, what Is it? Sources & progression
- Other cyber risk factors to consider
- Maintaining basic cyber risk hygiene
- Awareness Vs Preparedness

2

Cyber Insurance

- How does it help protect an organization?
- State of the Market
- Premium changes throughout 2021
- Requirements and recommendations before applying for cyber insurance in 2022

The Cyber Threat Landscape

AON

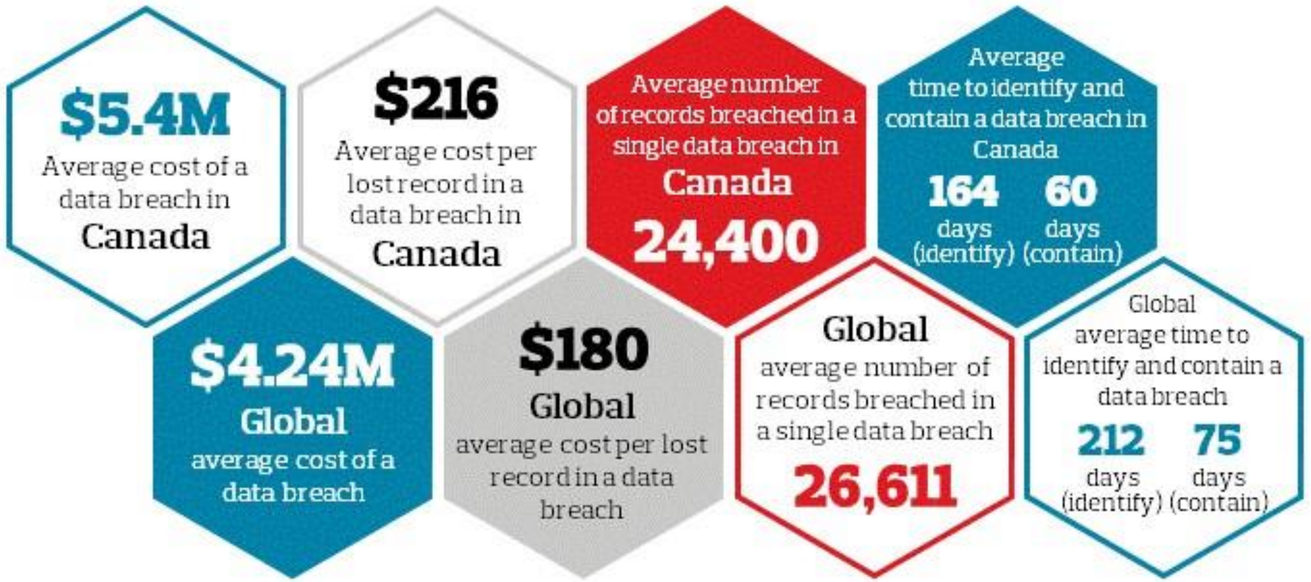
Setting the Scene

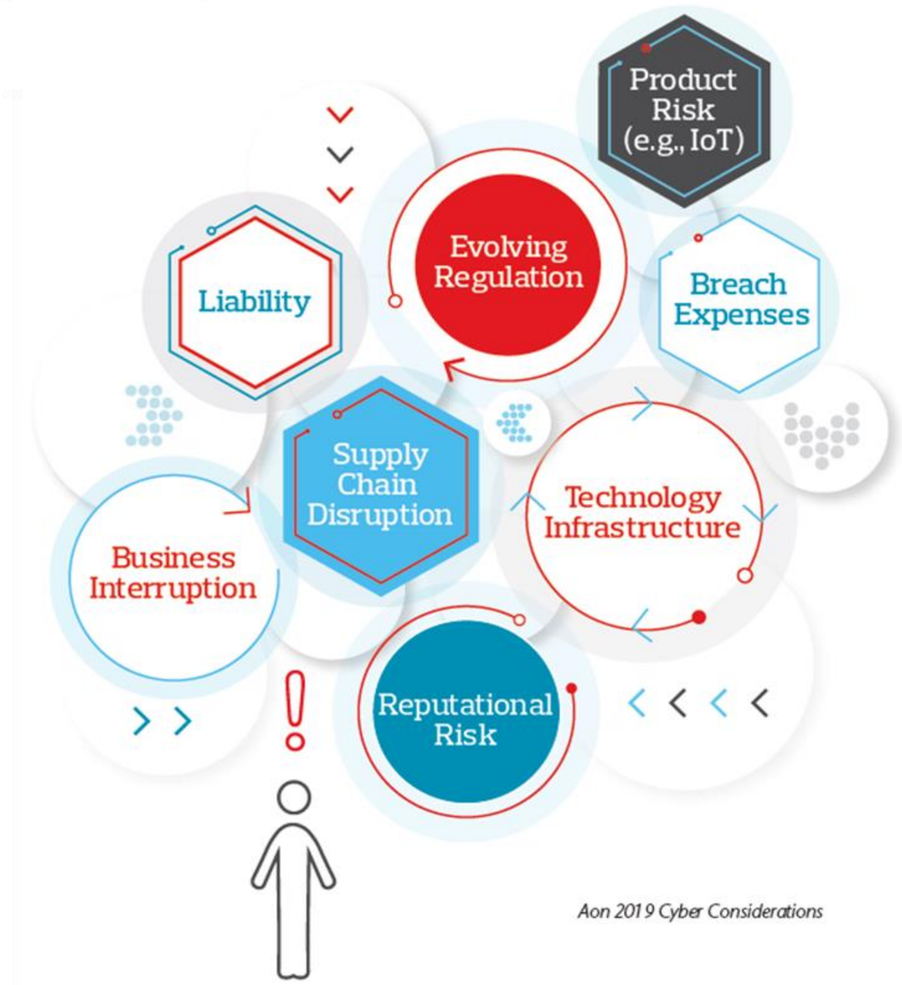
$6tn

Total cost of cybercrime in **2021**

$10.5tn

Total cost of cybercrime by **2025**



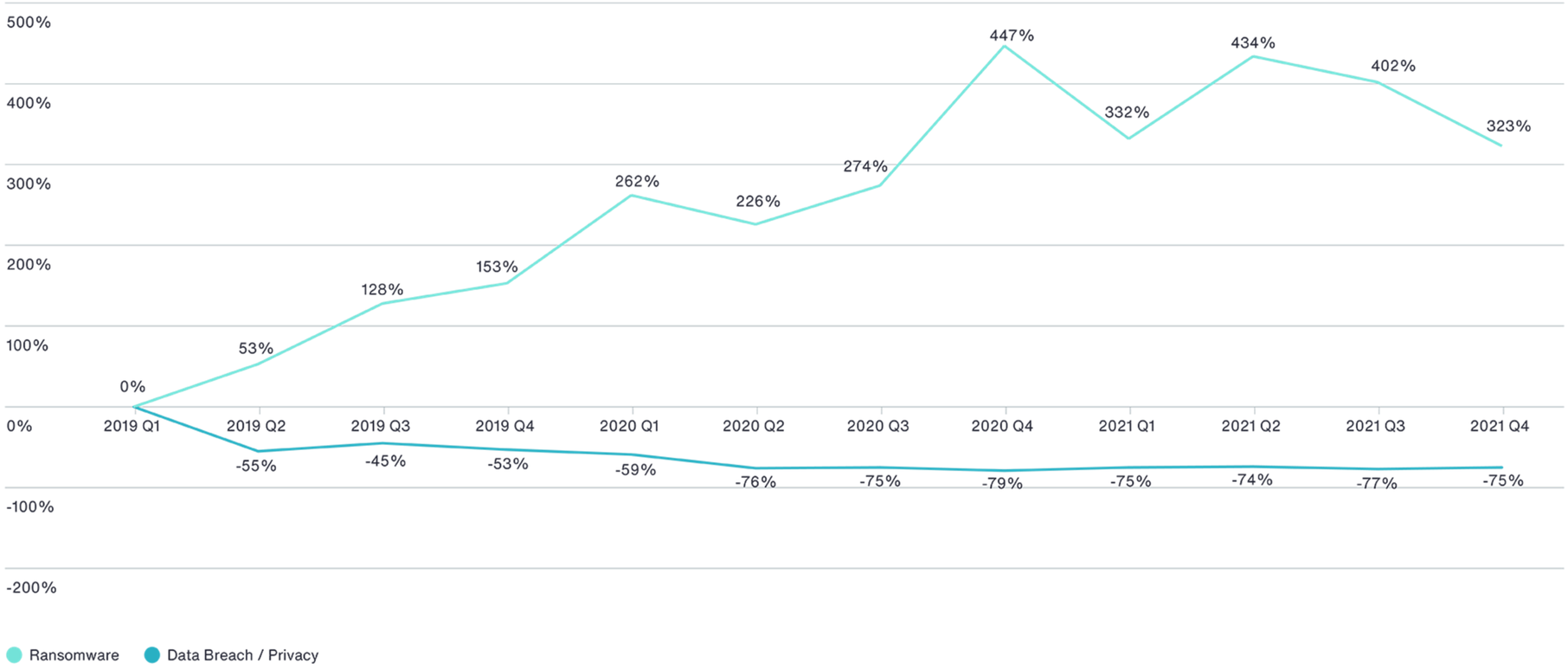


Source: Ponemon/IBM Institute “Cost of a Data Breach Study 2021”
Cyber Security Ventures: Cybercrime To Cost The World $10.5 Trillion Annually By 2025

Ransomware – Real Life Dialogue Box

Ransomware Trend – How Bad is It?

Throughout 2021 Aon's team observed a slight reduction in the frequency of cyber claims, although they have risen dramatically since 2018. E&O and media liability claims remained consistent year-on-year. Severity increased slightly on all fronts, with more material cyber claims in the market than prior years and a slight increase in large E&O and media liability losses.

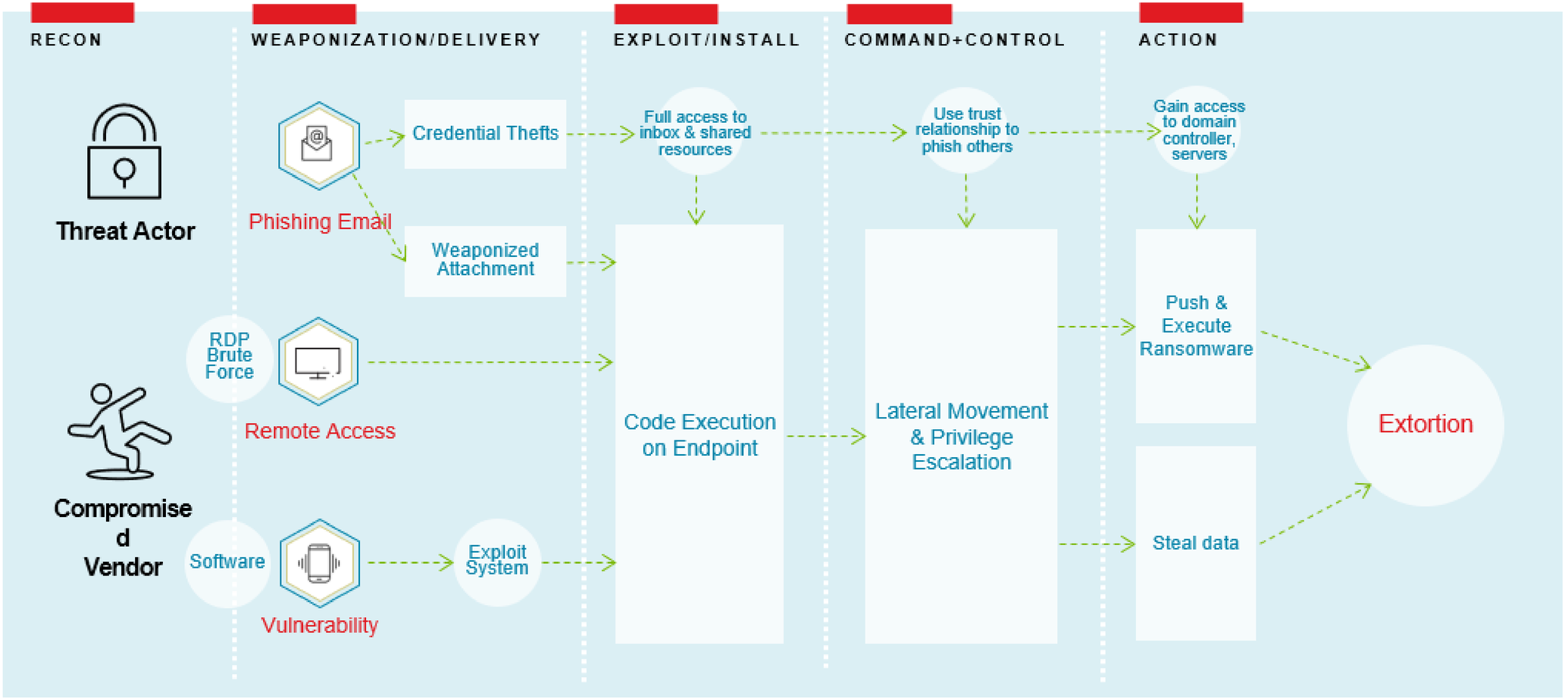


Key observations

- Ransomware activity has dramatically outpaced Data Breach/Privacy Event activity.
- Ransomware up 323% from Q1 2019 to Q4 2021.
- Eight figure losses are commonplace – business interruption represents the largest component of loss, litigation still to come.
- Data exfiltration occurred in 83% of ransomware cases per Coveware in Q3 2021.
- Average days of business interruption in Q3 2021 was 22 days, according to Coveware

Ransomware Attacks: How Do They Happen?

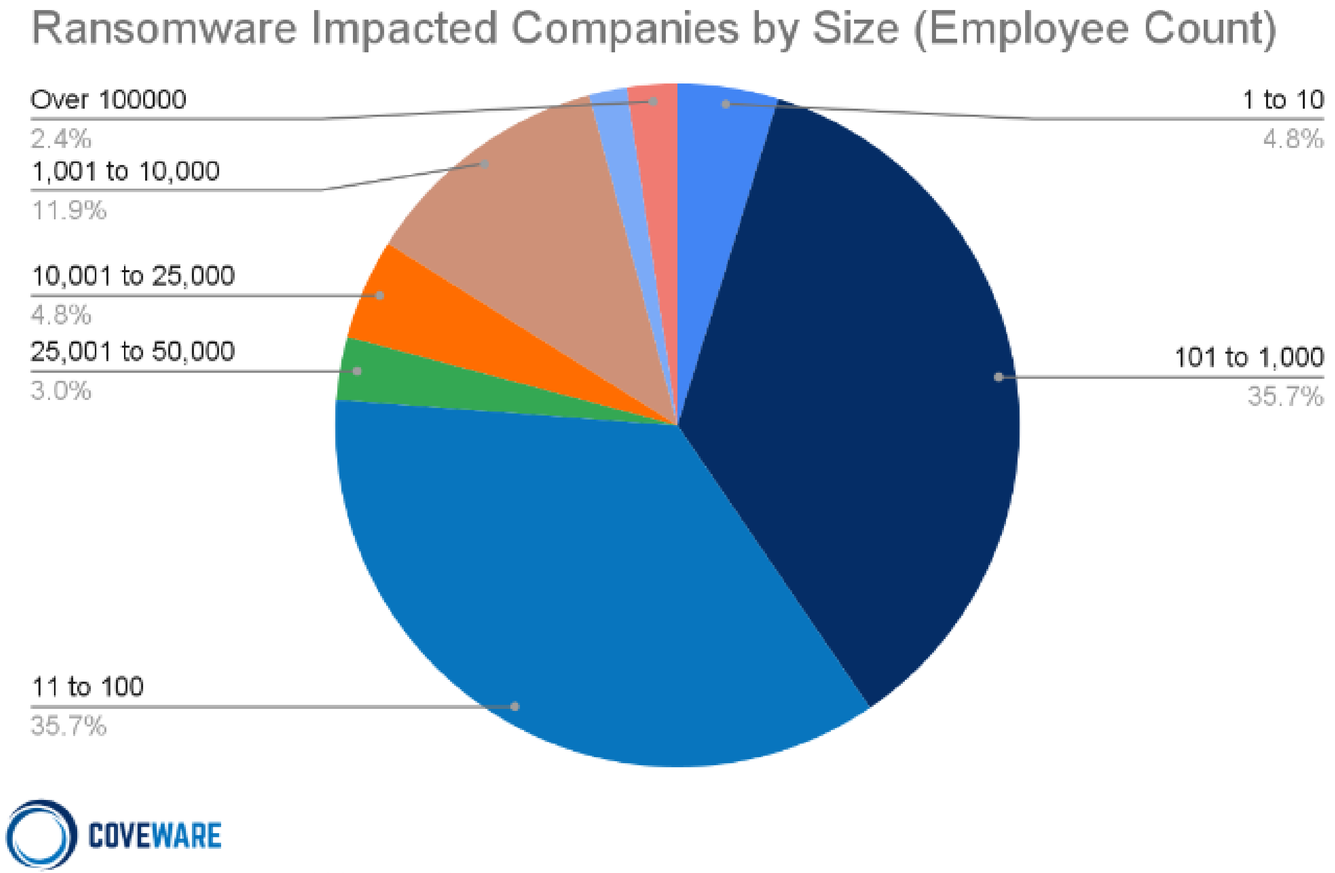
From the three attack vectors, attackers deploy malware, propagate and infect other systems



AON

Ransomware Attacks are Focused Small-mid sized organizations

- Companies with 1,000 or less employees represent 76.2% of ransomware attacks
- Why? Mid-market, SMB companies typically have lower cyber security maturity



COVEWARE

Lockbit 2.0 Affiliate: *"You can hit the jackpot once, but provoke such a geopolitical conflict that you will be quickly found. It is better to quietly receive stable small sums from mid-sized companies…"*

Source: *Coveware blog, Q1 2022

AON

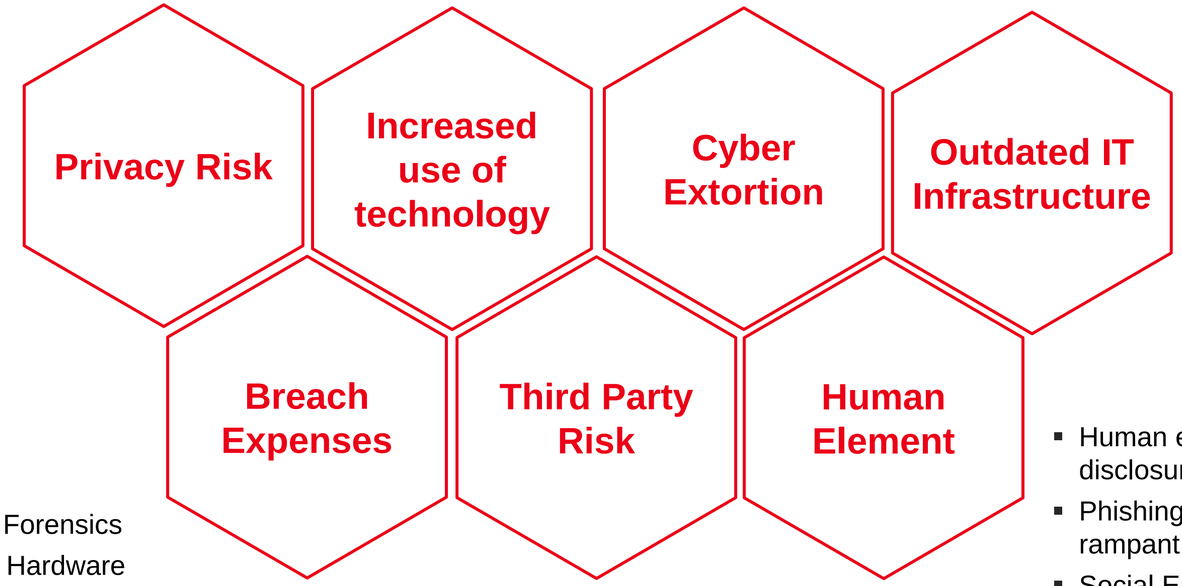
Cyber Risk – Other Factors to consider

- Gathering, maintaining, disseminating or storage of private information
- Mandated Record Retention Periods
- Liability incurred due to loss of PII

- High dependence on technology
- Relying on or operating critical infrastructure
- Information Technology Platforms
- Operational Technology

- Ransom Demands – Bitcoin / cryptocurrency
- Extortion expenses – termination consultants
- Phishing attacks
- Interruption of service

- Budgetary constraints
- Outdated security measures and controls



- Computer Forensics
- Software / Hardware Replacement
- Data Restoration
- Notification / Legal Costs

- High dependence on independent contractors, and additional service providers
- 3rd party due diligence

- Human error – accidental disclosure of information
- Phishing emails are rampant
- Social Engineering
- Rogue and disgruntled employees

Maintaining Basic Cyber Risk Hygiene

1. Assess, assess, assess!
2. Quantify your cyber risk
3. Utilize multi-factor authentication (MFA), intrusion detection, response and prevention systems
4. Create a cyber security culture: user awareness training, enforce strong password policy, and more
5. Prepare for an attack: backups, incident response & continuity plans, cyber insurance
6. Install software updates regularly and quickly along with patch management systems

AON

Awareness Vs Preparedness

2021 Global Risk Management Survey – YoY

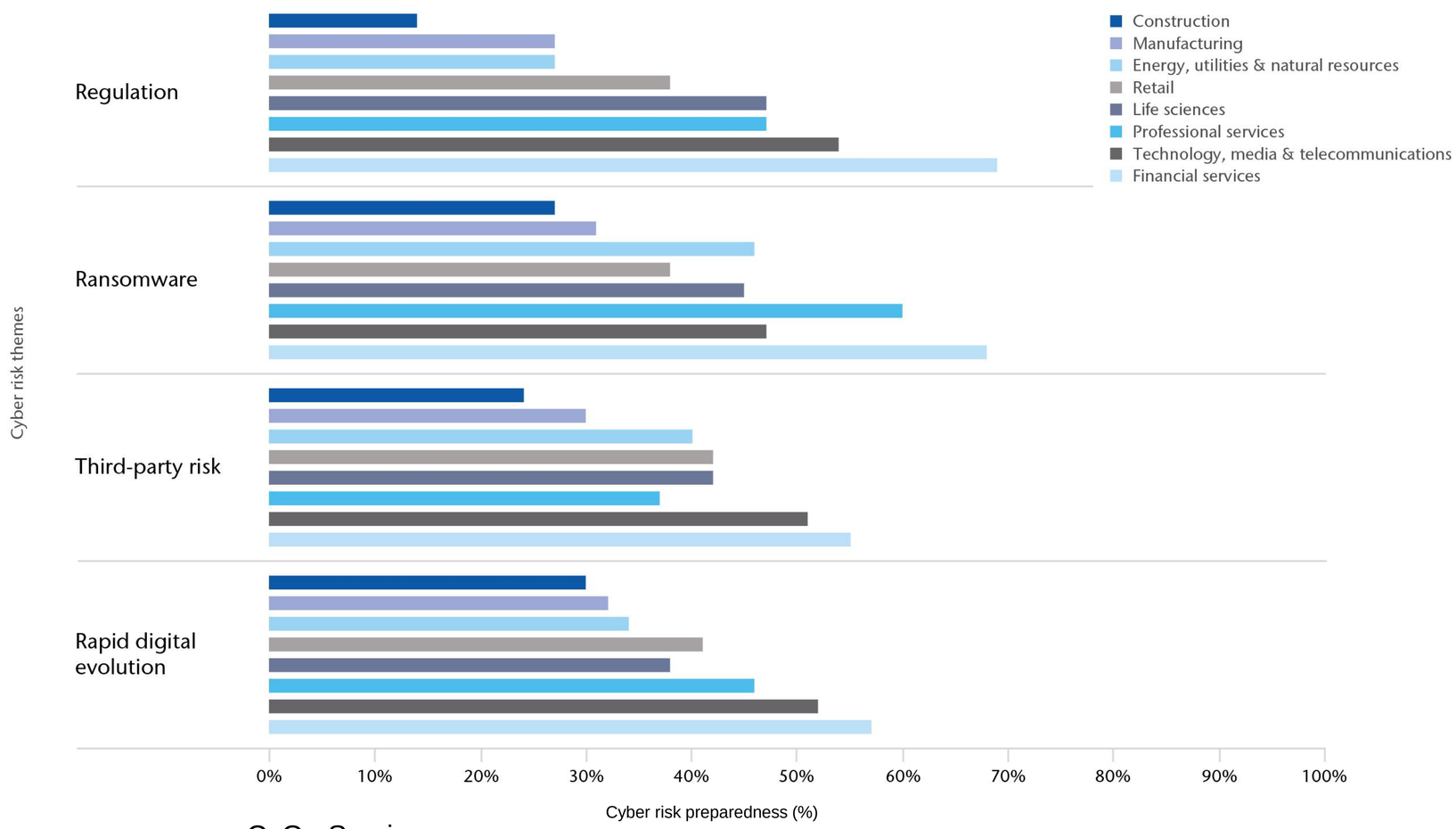
Top 10 risks identified by executives and professionals

	2021	2019	2017	2015	2013	2011	2009	2007
1	Cyber Attacks/ Data Breach	Ecomonic Slowdown/ Slow Recovery	Damage to Reputation/ Brand	Damage to Reputation/ Brand	Economic Slowdown/ Slow Recovery	Economic Slowdown/ Slow Recovery	Economic Slowdown/ Slow Recovery	Damage to Reputation/ Brand
2	Business Interruption	Damage to Reputation/ Brand	Economic Slowdown/ Slow Recovery	Economic Slowdown/ Slow Recovery	Regulatory/ Legislative Changes	Regulatory/ Legislative Changes	Regulatory/ Legislative Changes	Business Interruption
3	Economic Slowdown/ Slow Recovery	Accelerated Rates of Change in Market Factors	Increasing Competition	Regulatory/ Legislative Changes	Increasing Competition	Increasing Competition	Business Interruption	Third-Party Liability
4	Commodity Price Risk/Scarcity of Materials	Business Interruption	Regulatory/ Legislative Changes	Increasing Competition	Damage to Reputation/ Brand	Damage to Reputation/ Brand	Increasing Competition	Supply Chain or Distribution Failure
5	Damage to Reputation/ Brand	Increasing Competition	Cyber Attacks/ Data Breach	Failure to Attract or Retain Top Talent	Failure to Attract or Retain Top Talent	Business Interruption	Commodity Price Risk	Market Environment
6	Regulatory/ Legislative Changes	Cyber Attacks/ Data breach	Failure to Innovate/ Meet Customer Needs	Failure to Innovate/ Meet Customer Needs	Failure to Innovate/ Meet Customer Needs	Failure to Innovate/ Meet Customer Needs	Damage to Reputation/ Brand	Regulatory/ Legislative Changes
7	Pandemic Risk/ Health Crises	Commodity Price Risk	Failure to Attract or Retain Top Talent	Business Interruption	Business Interruption	Failure to Attract or Retain Top Talent	Cash Flow/ Liquidity Risk	Failure to Attract or Retain Top Talent
8	Supply Chain or Distribution Failure	Cash flow/ Liquidity Risk	Business Interruption	Third Party Liability	Commodity Price Risk	Commodity Price Risk	Supply Chain or Distribution Failure	Market Risk (Financial)
9	Increasing Competition	Failure to Innovate/ Meet Customer Needs	Political Risk/ Uncertainties	Cyber Attacks/ Data Breach	Cash Flow/ Liquidity Risk	Technology Failure/ System Failure	Third Party Liability	Physical Damage
10	Failure to Innovate/ Meet Customer Needs	Regulatory/ Legislative Changes	Third Party Liability (inc. E&O)	Property Damage	Political Risk/ Uncertainties	Cash Flow/ Liquidity Risk	Failure to Attract or Retain Top Talent	Merger/Acquisition/ Restructuring

AON

How Prepared Are Various Industries?

Construction	Manufacturing
2.2	2.2
Energy/Utilities	**Life Sciences**
2.4	2.4
Retail	**Professional Services**
2.4	2.5
Technology	**Financial Institutions**
2.5	2.7



CyQu Scoring

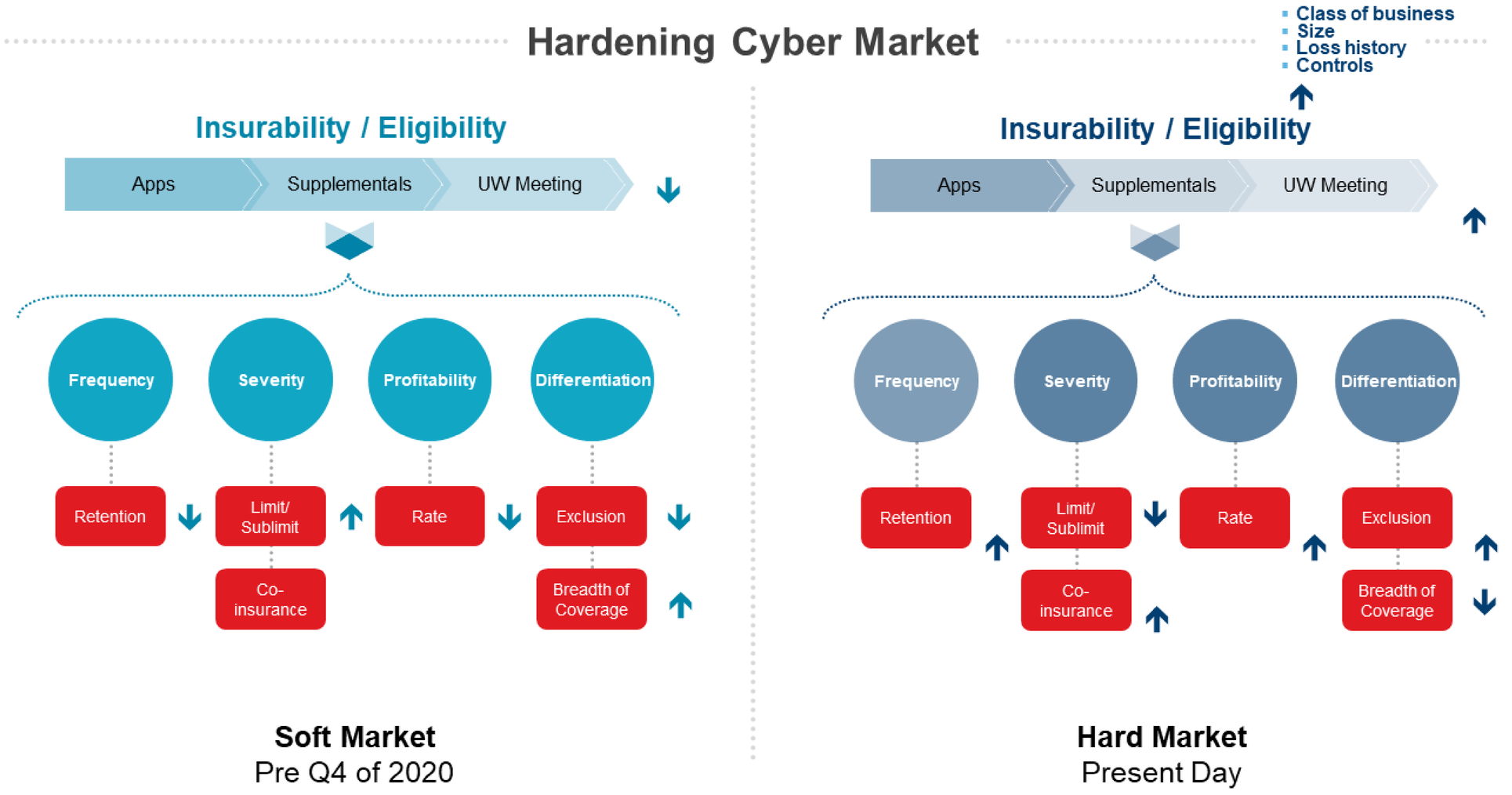
Initial	1 - 1.9	Organizational cyber security risk management practices are not performed
Basic	2 - 2.5	Organizational cyber security risk management practices and technologies are not formalised
Managed	2.6 - 3.4	Risk management practices and technologies are performed and established throughout the majority of the organization
Advanced	3.5 - 4	Adopts an organization-wide approach to manage cyber security risk and regularly update cyber security practices

AON

The Cyber Insurance 101 & State of the Market

AON

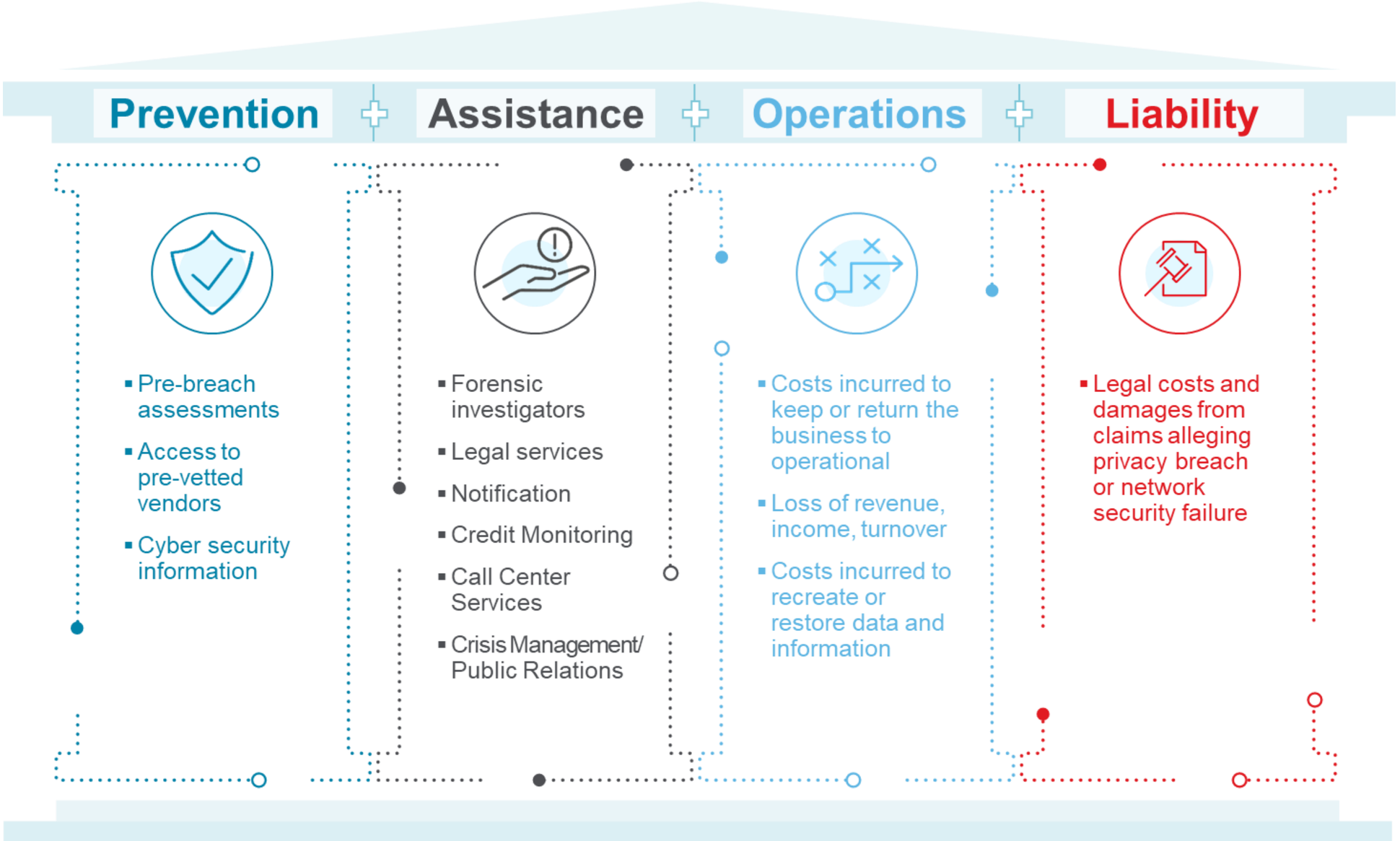
Current State of the Cyber Insurance Market



Soft Market
Pre Q4 of 2020

Hard Market
Present Day

How Does Cyber Insurance Help Protect an Organization?



AON

Cyber Insurance – What Does it Cover?

- **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

- **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
- **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.
- **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.

- **Privacy and Network Security Liability –**
  - ✓ **Privacy Liability:** Liability coverage for defence 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
  - ✓ **Network Security Liability –** Liability coverage for defence 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 defence 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

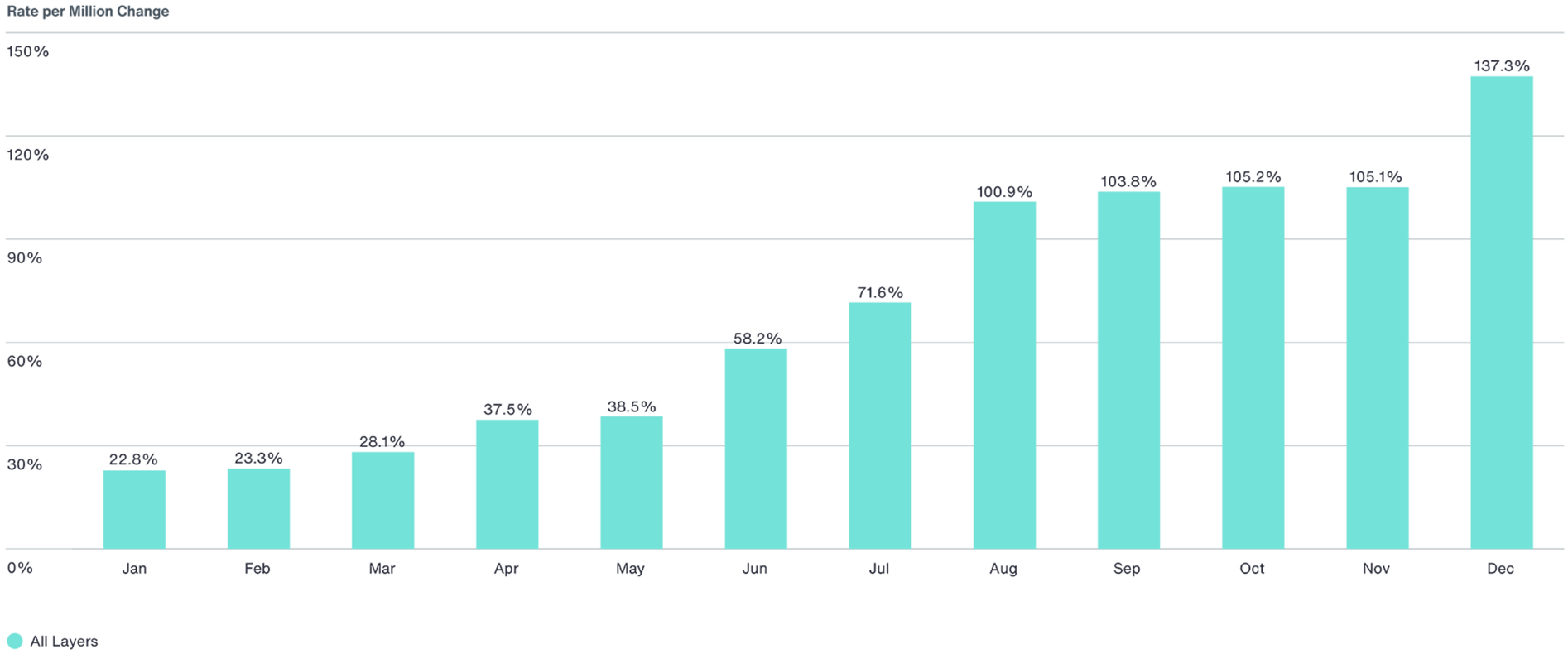
- **Media Liability –** Liability coverage for defence costs and damages suffered by others for content-based injuries such as libel, slander, defamation, copyright infringement, trademark infringement, or invasion of privacy. The scope of covered media is variable and can range from the insured's website 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

AON

Aon Clients Data/Analytics - Pricing Trends

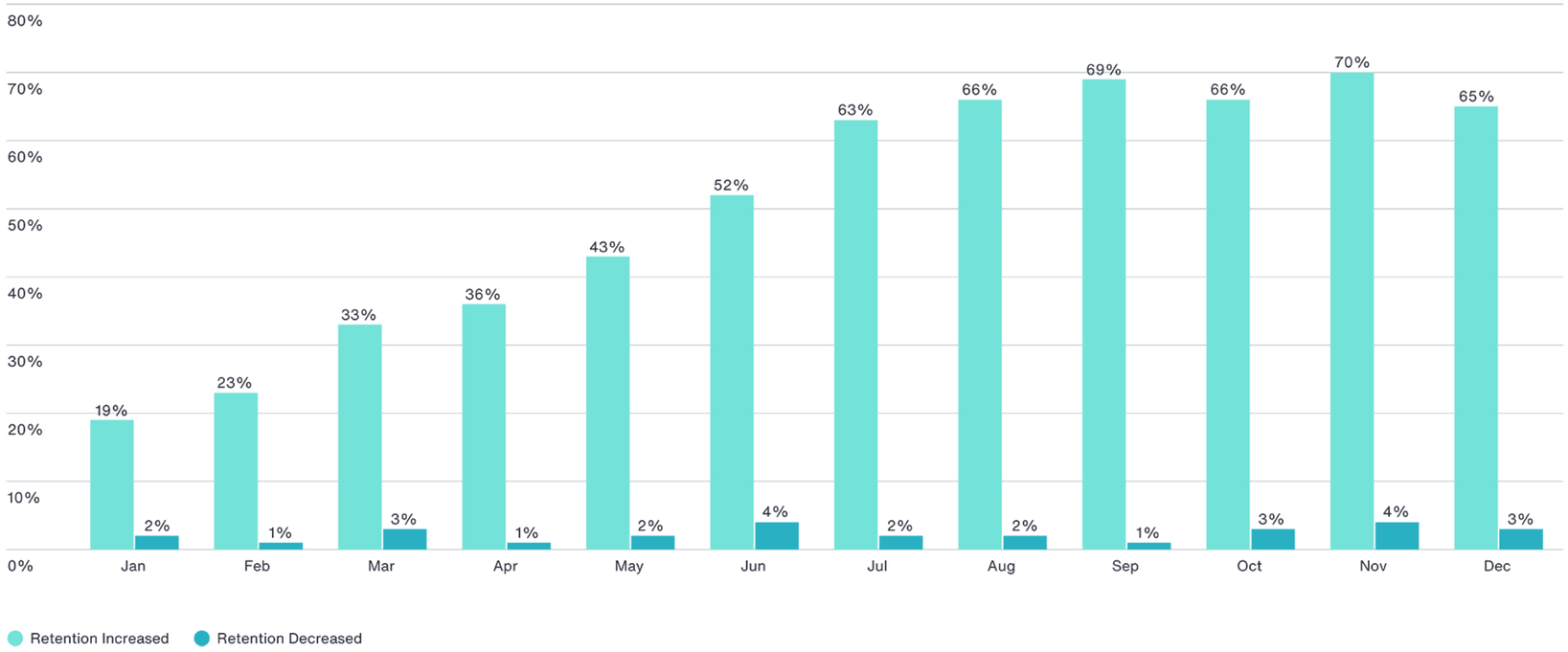
2021 E&O / Cyber Pricing All Layers Average Year-over-Year Change (Same Clients)



Aon Clients Data/Analytics : Retention

Clients continue to evaluate program structure in some instances due to limited options from the market. The number of clients increasing their retention climbed throughout 2021. Clients have experienced pressure to increase waiting periods for business interruption (BI)-related coverage agreements

Retention Change Year-over-Year (2021)



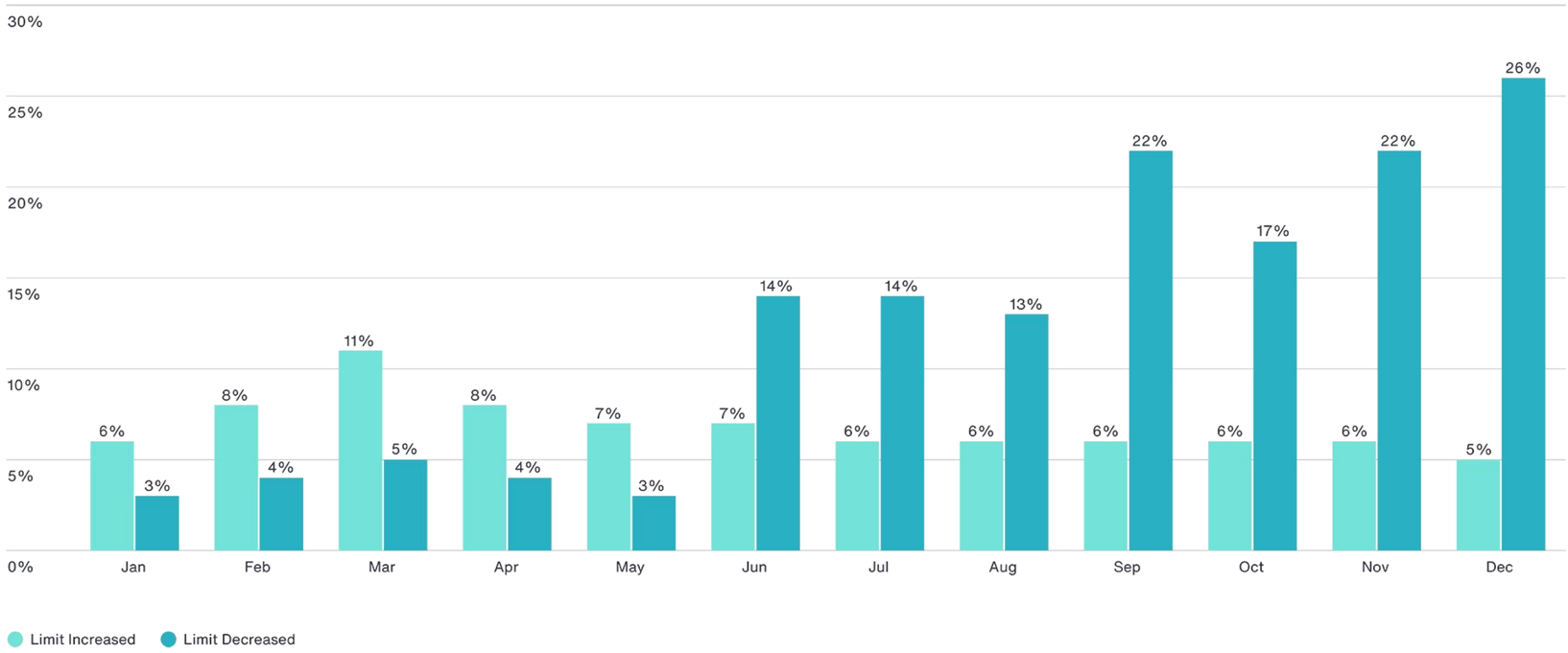
Key observations

- 60-70% of clients renewing in Q4 2021 saw an increase in retention.
- Retention increases were exponentially more common in the Middle Market segment.
- Aon expects continued pressure from the market to increase retention levels.

Aon Clients Data/Analytics : Limits

Some clients have opted to purchase lower aggregate limits throughout the second quarter, which may correlate with the acceleration of rate increases and its pressure on budgeting. For larger insurance programs, some limit reductions were due to lack of capacity offered by the market.

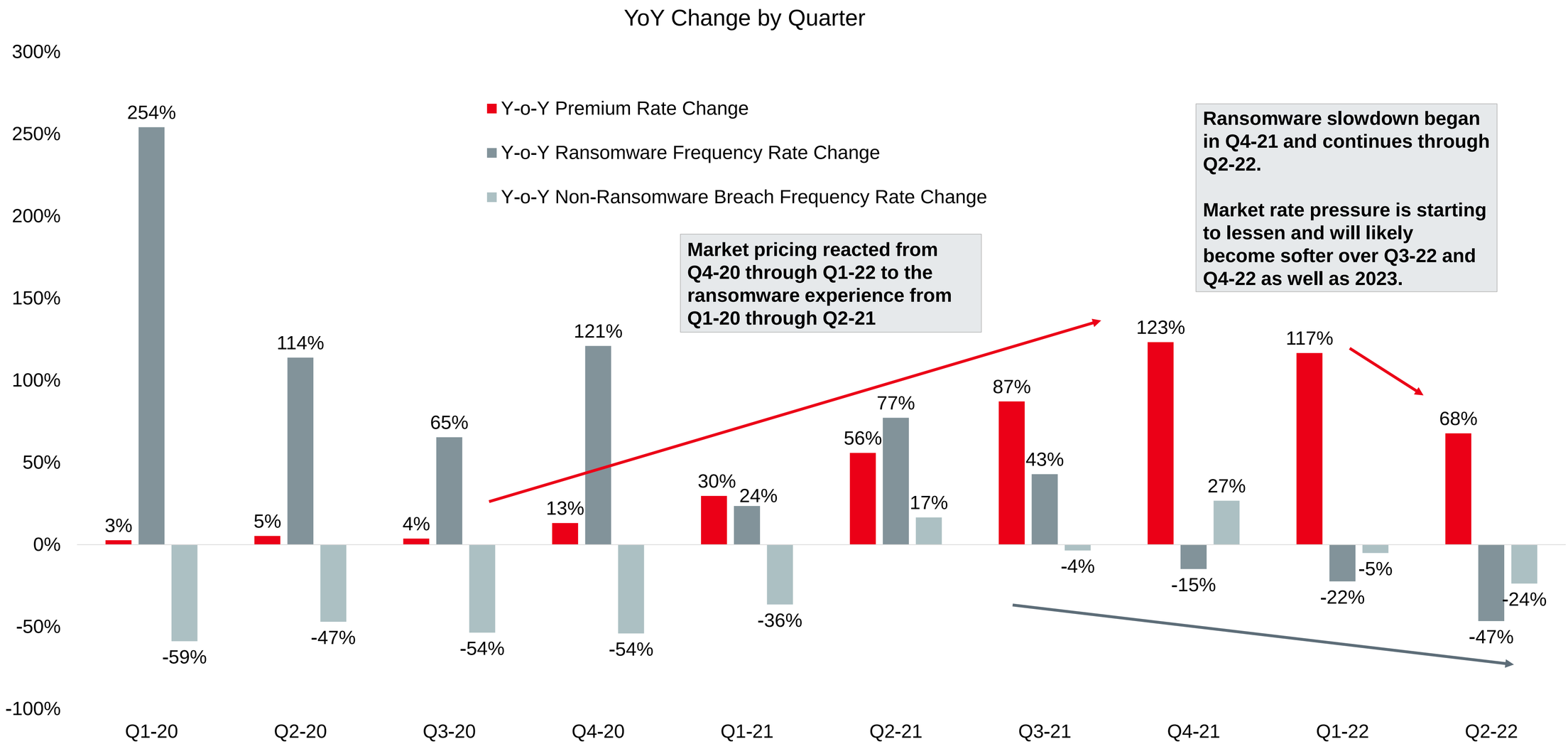
Limit Change Year-over-Year (2021)



Key observations

- There has been an uptick in Q4 2021 in the number of clients reducing overall limits, due to market capacity limitations or the cost of insurance increasing.

The Lag Between Cyber Attacks and Insurance Reaction



, Aon’s Guidance - Key Areas of Underwriting Focus

Key Areas of Underwriting Focus

Multi-Factor Authentication (MFA)	Endpoint Protection and Response (EDR)	Phishing Exercise/Cyber Awareness Training
Patch Management	Secure RDP/VPN	Incident Response Plan
Previous Incidents and Containment	Disaster Recovery/ Backups	Email Filtering

Aon’s List of Critical Network Security Controls

1. Multi-factor authentication (MFA) for:
   Email, privileged accounts, all remote access
2. Security & phishing awareness training
3. Properly configured URL filtering and email attachment sandboxing
4. Advanced endpoint detection and response (EDR) solution
5. Advanced malware detection tool that inspects network traffic
6. 16+ character service account and domain admin passwords
7. Lateral Movement Detection Tools
8. Properly configured security information and event management (SIEM) platform
9. Continuous security monitoring function
10. Business Resilience
11. Disabling accessibility of remote desktop directly from Internet

AON

Staying Ahead of the Market

1

FOCUS ON: Preparing a Collaborative Underwriting Submission, early….

- Collaborate with your broker during the information gathering stage. While the underwriting requirements from 2021 provide a relevant base for 2022 renewals, the required details and applications have evolved. Gathering the appropriate information and completing the current versions of applications can help prevent a “stale” submission which often delays the process.
- Brokers can also help identify pain points underwriters may have based on preliminary responses. In some instances, it may be possible to bolster the context around a particular risk management decision; in others, it may be possible to help clients explore ways to improve control. Without time, it will not be possible to improve the perceived risk posture before a policy expiration or renewal date. We recommend clients start the process as early as 150 days prior to the placement date.

2

FOCUS ON: Cyber Security, and not just Cyber Insurance!

- The marriage between cyber insurance and cyber security is the strongest it has ever been. Organizations need to maintain a healthy balance and investment in both, too much investment in either is not going to be a long term fix.
- Ten years from now, E&O and cyber exposures will likely still pose material risk to companies. We believe companies will continue to buy more insurance, transferring a portion of their risk to insurers. While insurance is an important aspect of an organization’s cyber risk mitigation plan, it NEEDS to be coupled with an investment in security controls.

Staying Ahead of the Market

3 FOCUS ON: Ransomware and Business Interruption

The topic of ransomware isn't going away quickly, if ever. Insurers will continue to focus on key controls they perceive will limit the probability of a ransomware event and the severity of the event. Topics such as access control, business continuity planning, and patch management remain relevant and will continue to develop. Being prepared for that discussion with underwriters is key.

Additionally, we've seen claims friction across two common fronts:

1. **First**, we continue to see misalignment of vendors or counsel used in response to an event, with insurer vendor panels. At least annually (and more often as incident response playbooks are revised) the client's preferred incident response vendors should be discussed in the context of the insurance policy to ensure alignment with the insurers' requirements for pre-approval and/or panel usage.
2. **Second**, as business interruption and extra expense claims progress through the adjustment process, clients should have a plan in place to document information needed for cyber business interruption claims and should have a forensic accounting team – with cyber expertise - selected to help expedite the proof of loss process and maximize the potential recovery.

4 FOCUS ON: Creativity

- The most valuable brokers are the ones who are the most creative. We know the market will continue to be challenging; it's important for clients to work closely with their broker, think about various ways to develop an optimal program, and for the insured to be a part of the process.

Thank You!

We are Here to Support…

Questions?

Ady Sharma | Vice President, Cyber Growth Leader
Aon | Cyber Solutions Canada
20 Bay Street | Toronto, ON M5J 2N9
T: 416.263.7876 M: 647.391.4121
ady.sharma@aon.ca

Appendix

Aon Cyber Solutions – Full Services Menu

Seek

We help you understand and quantify your risk.

- Assessments
  - > Security Risk Assessment
  - > Cyber Quotient Evaluation (CyQu)
  - > Cyber Impact Analysis: Financial Quantification
  - > Incident Response Readiness Assessment
  - > Privacy Compliance Assessment
  - > Insider Risk Assessment
  - > Individual Vulnerability Assessment
  - > CyberScan
  - > Corporate Threat Intelligence Assessment
- Cyber Security Testing
  - > Red Team & Social Engineering Testing
  - > Application & Mobile Security Testing
  - > Network & Cloud Penetration Testing
  - > Cloud & Host Configuration Review
  - > Automotive & IoT Security Testing
  - > Source Code Security Review
  - > Security Architecture Assessment
  - > Developer Application Security Training
  - > Secure Development Training
  - > Threat Hunting
- Due Diligence & Background Investigations

Shield

We know how to protect your organization and its critical assets.

- Cyber Insurance
- Cyber Risk Financing
- Incident Response Planning & Playbook Development
- Cyber Threat Simulation/Tabletop
- Security Architecture & Design
- Security Policies & Standards Development
- Security Strategy Development
- Security Controls Optimization
- Third Party Cyber Risk Management
- Insider Risk Program Development
- M&A Cyber Due Diligence
- Secure Software Development Lifecycle
- SOC Optimization
- CISO Advisory
- Board Advisory
- Errors & Omissions Insurance
- Rapid Response Planning
- Threat Intelligence Monitoring
- Data Privacy Analysis
- Data and Workflow Mapping

Solve

We search for the truth and help you recover quickly.

- Incident Response
- Digital Forensics
- Deep and Dark Web Scan
- eDiscovery
- Expert Witness Testimony
- Incident Response Retainer
- Complex Cyber Claims Preparation
- Cyber Claims Advocacy
- Fraud & Financial Loss Investigations
- Workplace Misconduct Investigations
- Digital Evidence Preservation
- Asset Searches
- Insider Leak Investigations
- Identity Attribution
- Social Media Exploitation
- PHI/PII Data Mining for Risk/Compliance

Notable Data Breach / Privacy Commercial Impacts

Organization	Approximate Disclosure Date	Commercial Impact	Financial Components	Source
British Airways	10/25/2018	£20 million	ICO Fine	ICO Enforcement
Capital One	07/29/2019	$127 million $80 million	Gross Expenses to Date excl. OCC OCC Civil Penalty	Q3 2020 Earnings OCC Consent Order
Desjardins Group	06/20/2019	CA$108 million	Gross Expenses	Q4 2019 Earnings
Equifax	09/07/2017	$1.956 billion £500,000	Gross Expenses to Date ICO Fine (DPA 1998)	Q3 2020 Earnings ICO Notice
Facebook	03/16/2018	$5 billion $100 million £500,000	FTC Civil Penalty SEC Settlement ICO Fine (DPA 1998)	FTC Press Release SEC Press Release ICO Notice
Marriott	11/30/2018	$159 million	Gross Expenses Includes £18.4 million ICO Fine	Q3 2020 Earnings Q2 2020 Earnings Q1 2020 Earnings 10-K Filing 2019 10-K Filing 2018
Target Corporation	12/18/2013	$292 million	Gross Expenses	10-K Filing 2016
Yahoo! Inc. (Altaba Inc.)	09/22/2016 12/14/2016	$350 million $117.5 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

Disclosed Data Breach / Privacy *Cyber* Insurance Recoveries

Organization	Approximate Disclosure Date	Recoveries Received / Accrued	Total Cyber Insurance Limits	Source
Capital One	07/29/2019	$67 million	$400 million	Q3 2020 Earnings Press Release
Equifax	09/07/2017	$125 million	$125 million	Q2 2019 Earnings ICO Notice
Global Payments	03/30/2012	$27 million	Unknown	10-K Filing 2015
Heartland Payment Systems	01/20/2009	$31.2 million	Unknown	10-K Filing 2013
Home Depot	09/02/2014	$100 million	$100 million	10-K Filing 2016
Marriott	11/30/2018	$133 million	Unknown	Q3 2020 Earnings Q2 2020 Earnings Q1 2020 Earnings 10-K Filing 2019 10-K Filing 2018
Target Corporation	12/18/2013	$107 million	Unknown	10-K Filing 2016 10-K Filing 2019

All of the values above were derived from published financial statements and/or company press releases.

AON

Notable Data Breach / Privacy Information Released

Organization	Approximate Disclosure Date	Individuals Impacted	Information Stolen	Source
British Airways	10/25/2018	500,000 PII/PCI	Log in, payment card, and travel booking details as well name and address information	ICO Notice
Capital One	07/29/2019	106 million PII	Personal information relating to people who had applied for credit card products and credit card customers; 100 million US; 6 million Canada No credit card account numbers or log-in credentials were compromised and over 99 percent of Social Security numbers were not compromised	Press Release
Equifax	09/07/2017	147 million PII	PII of approx. 145.5 million U.S. consumers, approx. 19,000 Canadian consumers, and approx. 860,000 U.K. consumers.	10-K Filing 2018
Marriott	11/30/2018	339 million PII 9.1 million PCI	Names, mailing addresses, phone numbers, email addresses, passport numbers, payment card numbers and expiration dates, Starwood Preferred Guest account information, dates of birth, gender, arrival and departure information, reservation dates, and communication preferences.	10-K Filing 2018 ICO Notice
Target Corporation	12/18/2013	70 million PII 40 million PCI	Payment card data from up to approx. 40 million credit and debit card accounts of guests; guest information, including names, mailing addresses, phone numbers or email addresses, for up to 70 million individuals.	10-K Filing 2014
Yahoo! Inc. (Altaba Inc.)	09/22/2016 12/14/2016	3 billion 500 million	500 million (2014 breach) and 3 billion user accounts (2013 breach) were impacted as part of two separate data breaches	U.S. District Court

AON

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

The NotPetya event began propagating on 6/27/2017; all of the organizations above have an approximate disclosure date of 6/27/2017.

AON

Notable Business Interruption Commercial Impacts

Organization	Approximate Disclosure Date	Commercial Impact	Financial Components	Source
Cognizant	04/20/2020	$36 million $24 million	Q2 Revenue Impact (90 BPS) Q2 Additional Expense	Q2 2020 Financials
Demant A/S	09/03/2019	~$95-103 million ~$84.6 million ~$11 million	2019 and 2020 EBIT Reduction 2019 Sales Reduction 2019 Direct Costs	2019 Annual Report
Eurofins	06/02/2019	€75 million €69 million	2019 EBITDA Reduction 2019 Revenue Reduction	2019 Annual Report
Norsk Hydro (LockerGoga)	03/19/2019	~$68-79 million	Lost Output, Margin, & IT Costs	Q4 2019 Earnings Release
Pitney Bowes (Ryuk)	10/12/2019	$18 million $0.08 / share $29 million	Revenue Reduction EPS Impact Free Cash Flow Reduction	Q4 2019 Earnings Release
Sopra Steria (Ryuk)	10/21/2020	~€40-50 million	Operating Margin Reduction	Press Release
Travelex	01/02/2020	£25 million	EBITDA	Press Release
TSB (IT System Failure)	04/24/2018	£33.5 million £125.2 million £49.1 million £122.4 million	Sales Reduction Customer Redress & Rectification Fraud & Operational Additional Resource & Advisory	Q4 2018 Earnings Release
TSMC (Malware)	08/03/2018	$85 million	Cost of Revenue	TSMC Press Release 2018 20F

AON

Disclosed Business Interruption *Cyber* Insurance Recoveries

Organization	Approximate Disclosure Date	Recoveries Received / Accrued	Total Cyber Insurance Limits	Source
A.P. Moller – Maersk*	06/27/2017	N/A	*No* Cyber Insurance in Place	Q4 2017 Financials
FedEx* (TNT Express)	06/27/2017	N/A	*No* Cyber Insurance in Place	Q4 2018 Financials
Mondelez International*	06/27/2017	TBD	$100 million (Property Insurance)	Circuit Court of Illinois
Demant A/S	09/03/2019	~$15 million	~$15 million	2019 Annual Report Press Release
Eurofins	06/02/2019	€19.8 million	Unknown	Q2 2020 Financials
Norsk Hydro (LockerGoga)	03/19/2019	~$23.2 million NOK 190 million	Cyber Insurance in Place	Q3 2019 Financials Q4 2019 Earnings Q2 2020 Earnings

All of the values above were derived from published financial statements and/or company press releases.

*These entities were all impacted by the NotPetya event, which began propagating on 06/27/2017.

AON

Real Manufacturing Company Cyber Incident – Aon Client

Mid-size Canadian manufacturer, supplier and distributor

- The organization was a target of a ransomware attack, with a demand of $2.7M CAD in Bitcoin.
- The organization attempted to negotiate with the hacker through legal counsel while assessing impact on their systems. All 300 file servers had been encrypted, and email/phone systems were down.
- Recovery took 6 weeks from date of incident, at which point the insured was still operational at only 75%.
- Insured had to undertake efforts to recover its intellectual property, consisting primarily of product drawings and plans. These items had to first be located on the servers, and then assessed to ensure they could be recovered to a usable state.

AON

Real Manufacturing Company Cyber Incident – Aon Client

Table 1

Summary of Loss

Description	Per MDD
Business Interruption	
Hourly Production Staff - Labour Inefficiencies	$ 1,109,692
[redacted]	183,706
Salaried Staff - Continuing Payroll and Overhead Expenses	3,123,182
[redacted] - Continuing Payroll Expenses	49,825
Loss on [redacted]	
Lost [redacted] Revenue	97,273
Loss on [redacted]	18,272
Total - Business Interruption	4,581,949
Extra Expenses	
External Consultant and Other Costs	35,348
Meals, Travel and Other	52,409
Total - Extra Expenses	87,757
Other	
Cyber Incident Response Costs	388,888
Digital Data Recovery Costs	260,158
Total - Other	649,046
Total	5,318,752
Less: Retention	(50,000)
Net Loss	**$ 5,268,752**
Policy Limit	**$ 5,000,000**
Claim Preparation Fees - Estimate	**$ 25,000**

Amount to be determined.

Recent Cyber Insurance Losses

Large national construction client, generally best in class controls – poor MFA controls

An Aon Insured suffered a Ryuk ransomware attack shortly before the Christmas holidays. The Insured did not have a significant number of Personally Identifiable Information of their employees or customers, but they did have a substantial amount of sensitive information on third-party corporate confidential information – including information from federal governments and military entities. The initial ransom demand was $5M, which was negotiated down to $1M by their Insurer. Forensic and legal services were engaged to help remediate the breach for a total of $950K. **The total amount paid out under the Insured's cyber policy, including credit monitoring and all extra expenses, was $2.45M.**

Large national manufacturing client, generally mediocre controls – security awareness training missing

An Aon Insured fell victim to a ransomware event due to a phishing email sent to an employee's personal email which on the organization's VPN. The phishing email delivered a batch file while installed malicious software on the user's system. The bad actor gained access to an old app server and domain controllers, continuing to compromise a privileged account. The Insured was able to continue their revenue generating operations, but sensitive data was exposed and encrypted. The sensitive data included C-suite and employee T4s and confidential customer contracts. The bad actor demanded an extortion amount of $5M which was negotiated down to $2M and paid. **Total amount paid to rectify the incident was around 2.5M.**

AON