



Understanding the Cyber Market

Your Risks, Insurance Coverages and Best Practices

Palm Beach County RIMS

September 2022

Agenda

I.	Introductions	3-4
II.	Threat Landscape	6-11
III.	Market Conditions	13-14
IV.	Underwriting Considerations	16-19
V.	How to Prepare for Coverage Placement	21-22
VII.	Questions & Contact Information	23



Charles Leonard

Senior Vice President – WTW Broking

Southeast Cyber Team co-leader at WTW based in Atlanta, Georgia. Charles is responsible for the consulting, broking, negotiations, and development of Cyber and Professional Liability insurance risk transfer placements in the Southeast and Mid-Atlantic regions. Charles serves WTW's public entity clients and large governmental organizations, among other industries.



Asa Long

Senior Vice President – WTW Broking

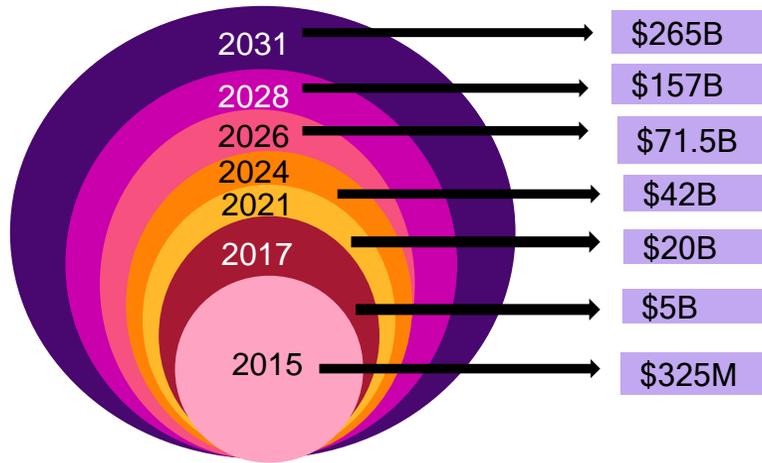
Senior Broker for the WTW Southeast Cyber team based out of Atlanta, Georgia. Asa has over a decade of experience underwriting, analyzing exposures, and assessing risks for cyber liability. Asa focuses on manufacturers, financial institutions, and healthcare clients for WTW specializing in large and complex risks.

Threat Landscape

September 2022

The ransomware crisis

Estimated & Projected Global Costs



Trends

- 130%** Increase in average ransom payment from 3rd quarter of 2021*
- 63%** Increase in median ransom payment from 3rd quarter of 2021*
- 34%** Decrease in average ransom payment from 4th quarter of 2021*
- 37%** Decrease in median ransom payment from 4th quarter of 2021*

*Source: Coveware

Other Key Statistics

Ransomware cost the world **\$20 billion in 2021**, which is 57X more than it was in 2015. That number is expected to rise to **\$265 billion by 2031**.



In 2021, **37 percent of all businesses and organizations** were hit by ransomware.^{Sophos}



Recovering from a ransomware attack cost businesses **\$1.85 million on average in 2021**.^{Sophos}



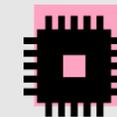
Ransomware is expected to attack a business, consumer or device every 2 seconds by 2031, up from every 11 seconds in 2021.



Out of all ransomware victims, **32 percent pay the ransom**, but they only **get 65 percent of their data back**.^{Sophos}



Of attacks in 2021 only **57 percent** of businesses were successful in recovering their data using backups



50% more cyberattacks per week in 2022 so far compared to 2021



Source: Sonic Wall Cyber Threat Report 2022

Current cyber risk threat landscape: The statistics

623.3 million attacks observed globally in 2021, a 105% increase over 2020 and more than triple the number seen in 2019. Sonic Wall Cyber Threat Report 2022



In 2021, **37 percent of all businesses and organizations** were hit by ransomware. Sophos



Only **57 percent of businesses** are successful in recovering their data using a backup. Sophos



Ransomware attacks cost an average of **\$4.62 million**, more expensive than the average data breach (\$4.24 million). IBM Cost of a Data Breach Report 2021



405% increase in average ransomware payments in the U.S. between 2019 and the 1st quarter of 2021 Coveware



Ransomware volume increased **105%** year over year and is up **232%** since 2019. Sonic Wall Cyber Threat Report 2022



442,151 never-before-seen malware variants identified in 2021, a 65% year-over-year and an average of **1,211 per day**. Sonic Wall Cyber Threat Report 2022



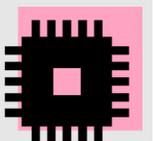
20,136 Common Vulnerabilities and Exposures (CVEs) published in 2021. Sonic Wall Cyber Threat Report 2022



Data breach costs remain highest in the U.S., where the average cost of a data breach in 2021 was **\$9.05 million**, up approximately 5% since 2020. IBM Cost of a Data Breach Report 2021



5.3 trillion intrusion attempts in 2021, up **11%** from 2020. Sonic Wall Cyber Threat Report 2022



Key industry events

SolarWinds Incident

- FireEye first publicized the cyber attack in December of 2020.
- Investigations found the SolarWinds Orion product to be the source of the malware, with malware installed in updates of this software between March and June 2020.
- 18,000 organizations impacted, although approximately 250 had a second type of malware installed that created a back door to allow hackers access to networks.
- Many U.S. government agencies and technology companies affected including Microsoft, VMware, Intel, and Cisco.
- Highly sophisticated supply chain attack the U.S. have attributed attack to Russian state sponsored actors.
- Situation is still developing quickly, and it is likely to continue expanding with additional applications potentially being compromised.

Accellion Incident

- Accellion's File Transfer Application (FTA) was the target of a cyber attack around December 23, 2020.
- The FTA was a 20-year-old product nearing end-of-life when a zero-day vulnerability with a SQL injection flaw was exploited. The file transfer platform was compromised, and data was exfiltrated. Ransom demands were significant.
- 300+ Accellion customers impacted including a government agency, 2 large law firms, a university, a large grocery store chain, but the damage continues to be unveiled.
- The threat actor known as CL0P is believed to be attributed to the Russian state.

Microsoft Exchange Server Incident

- On March 2, 2021, Microsoft disclosed a critical vulnerability impacting on-premises Microsoft Exchange Servers, including 2010, 2013, 2016 and 2019 versions.
- Internet facing servers, such as Outlook Web Access, were particularly at risk of compromise, permitting hackers to gain access to email accounts and the ability to install malware.
- Office 365/Exchange Online mailboxes reportedly unaffected.
- Reportedly carried out by a sophisticated state sponsored actor (Chinese group Hafnium) who infiltrated networks and installed a backdoor to maintain access.
- This vulnerability has led to over 30,000 U.S. governmental and commercial organizations having their emails hacked.

Kaseya

- REvil ransomware group engaged in supply-chain ransomware attack against Kaseya and multiple managed service providers that employ VSA software.
- Kaseya quickly introduced VSA Detection Tool to help MSPs determine if their software had been attacked /compromised.
- Attack spans victims in at least 17 countries, including UK, South Africa, Canada, Argentina, Mexico, Indonesia, New Zealand and Kenya.
- Swedish grocery chain Coop said most of its 800 stores would be closed for a second day on Sunday.
- REvil ransomware gang demanded \$70M in Bitcoin for a tool that can decrypt all affected systems.
- Kaseya on July 21st obtained a decryptor for victims of the ransomware attack but did not disclose whether it had paid the ransomware.

Key industry events

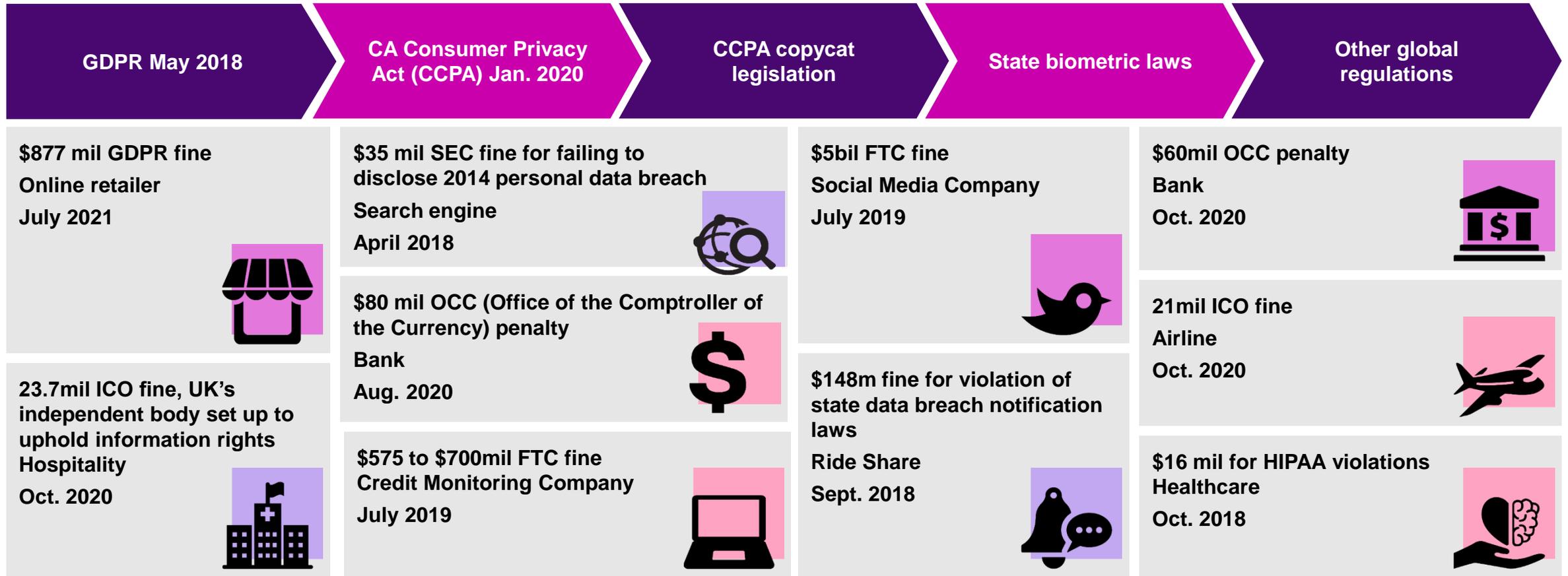
Apache Log4j Incident

- A critical vulnerability in the Apache Log4j utility of the popular application programming language, Java, was exploited by attackers in December 2021.
- The exploit was first seen on sites hosting Minecraft servers, where it was discovered that attackers could trigger the vulnerability by posting chat messages.
- The attack surface is estimated to be sizeable, as some of the components impacted are extremely popular and are utilized by millions of enterprise applications and services.
- Organizations should review their inventory of applications, especially those that are publicly accessible, to determine whether they utilize the Apache Log4j library and need to be patched. Unfortunately, failing to patch actively exploited flaws in a timely manner has resulted in major breaches in the past, an example of which was the 2017 Equifax breach which involved the failure to patch an actively exploited Java Struts2 vulnerability.

Kronos Private Cloud Ransomware Incident

- Kronos Private Cloud, which hosts some of the most heavily utilized applications for time management, payroll processing and other HR-related activities, was hit by a ransomware attack on December 11, 2021.
- Although Kronos is secured using firewalls, multi-factor authentication and encrypted transmission to prevent unauthorized access to these applications, the attackers were able to breach the systems, and likely encrypted servers as part of the attack.
- The immediate impact was that the Kronos Private Cloud applications were rendered unavailable.
- The timing of this attack is not uncommon, as ransomware gangs routinely plan attacks for periods where organizations are short-staffed for the holidays or when they are extremely busy. They do this with the hope that organizations are slow to discover the infiltration and respond, and more likely to pay ransomware demands because of the increased pressure to service customers.

Cyber regulatory landscape



Ransomware incidents – Based on BlackFog reporting only

Reflecting 2021 ransomware attacks with reported demands/payments

Industry	Event	Financial Impact	Description
Retail	REvil	\$30 million demand, unknown response	Unclear what the impacts were
Automobile	DoppelPaymer	\$20 million demand, unknown response	Unclear what the impacts were – firm denied incident
Technology	REvil	\$50 million demand, unknown response	Data exfiltrated and published partially as proof
Insurance	CryptoLocker	\$40 million paid (not confirmed by firm)	Over 15,000 devices encrypted, remote access impaired
Retail	Conti	\$2 million paid	Data exfiltrated January, company delayed reporting
Technology	Clop	\$12 million demand, then \$24 million demand	Firm has not acknowledged incident
Education	Conti	\$40 million demand, unknown response	Student and teacher data threatened with release
Pharma	REvil	\$25 million demand, then \$50 million demand	Firm advised able to bring attack under control in 24 hrs
Technology	REvil	\$50 million demand	Blueprints to valued tech threatened with release
Energy	DarkSide	\$4.4 million paid	Significant supply disruption, gas shortages
Chemicals	DarkSide	\$4.4 million paid	150Gb of stolen data
Meat packer	Not identified	\$11 million paid	Plants shutdown in US and Australia
Technology	Conti	\$7 million demanded, \$2.6 million paid	Exfiltrated data, contracts and source code
Technology	Revil	\$70 million demand, unknown response	Many downstream firms impacted
Consulting	LockBit	\$50 million demand, unknown response	6 Tb of data allegedly held

Market Conditions

September 2022

Cyber market update – Q2 2022

Pricing Guidance

- 2020 transition to “hard” Cyber market with increases for loss free accounts worsening:
 - **Q1 2020:** +5% to +10%
 - **Q2 2020:** +10% to +20%
 - **Q3 2020:** +15% to + 30%
 - **Q4 2020:** +25% to +50%
 - **Q1-Q4 2021:** +50% to +200%
 - **Q1-Q2 2022: +25% to +150%**
- Ransomware controls impact pricing
- Excess Carriers focused on:
 - rate adequacy
 - resulting in higher increases on excess
- Excess rates: 85%-95% of underlying

Capacity & Coverage

- Global insurers managing capacity to < \$10M for single account
- Insurers exited the cyber market (eg., RLI, TDC, Occam)
- Carriers adjusting coverage for ransomware.
- Carriers applying
 - sub-limits
 - co-insurance
 - broader exclusions
- Challenged industries: Higher education, public entities, managed service providers (MSPs) and airlines.

Underwriting Process

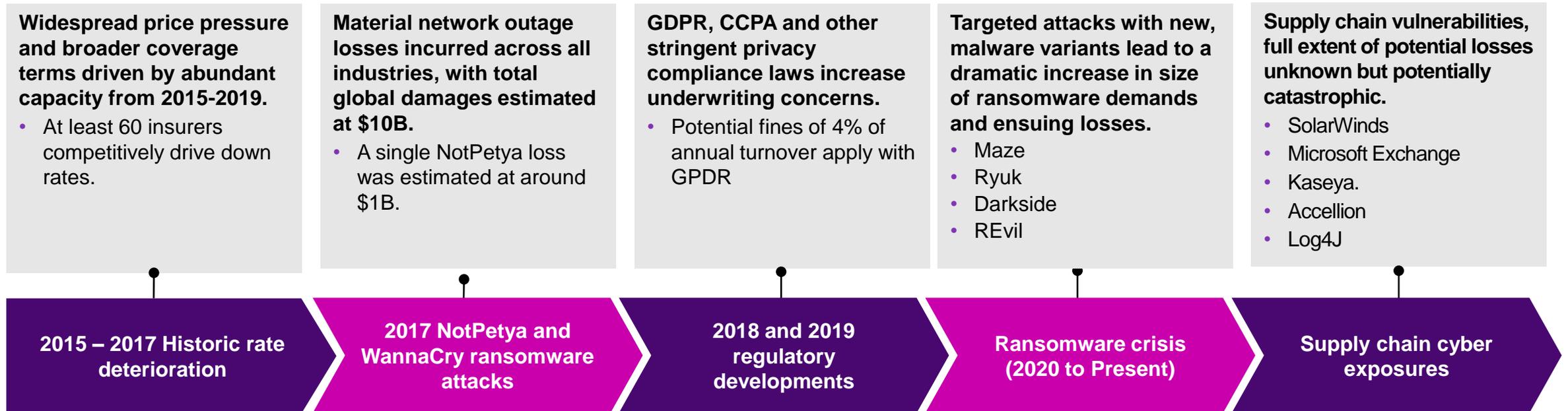
- Ransomware and other applications required by carriers
- Insurers review 3rd party security ratings to supplement underwriting (BitSight, Security Scorecard).
- Systemic exposure now a key underwriting focus (e.g. Blackbaud, SolarWinds).
- Perceived weak controls often result in coverage restrictions or declinations.

Prognosis

- Rate increases in the second half of 2022 are expected to be less pronounced than the first half with some market stabilization expected in 2023.

Historical review: How did we get to the current crisis?

Timeline of factors affecting rate (2015 to the present)



Underwriting Considerations

September 2022

Cyber insurance overview

Liability coverage

Security & Privacy Liability Insurance	Liability associated with your inability to protect personally identifiable information or corporate confidential information of third parties. The information can be in any format and breached intentionally or negligently by any person, <u>including third party service providers to which you have outsourced information. Third party service providers include, but are not limited to, IT service providers.</u> Coverage also extends to liability associated with your inability to prevent a computer attack against your computer systems or alleged responsibility for transmission of malicious code to a third party.
Media Content Insurance	Tort liability associated with content you create, distribute or is created and distributed on your behalf , including social media content.
Regulatory Fines & Legal Expense	Fines assessed by a regulatory body following a cyber incident, and legal defense costs. Actual fines and penalties can only be covered where insurable by law.
PCI Loss	PCI fines, penalties and assessments following a data breach and alleged non-compliance with PCI standards.

Direct (Loss mitigation coverage)

Data Breach Expense	Direct costs expended to mitigate a privacy breach. Costs typically include public relations expenses, notification, legal compliance, identity theft restoration, credit monitoring services and forensic/remediation expenses. Coverage also extends to the costs to restore or re-create data.
----------------------------	---

Direct (First party coverage)

Network BI & Dependent BI	Income loss/extra expense associated with your inability to prevent a disruption to your computer network caused by introduction of malicious code or any unintentional or unplanned outage. Coverage also extends to disruptions of IT vendors and other entities the Insured is critically dependent on to conduct business.
Cyber Extortion Insurance	Costs incurred by the Insured to hire a third party to assist with managing an extortion and demand and costs for the actual extortion payment, including payments made in Bitcoin or other cryptocurrency.
Reputation Guard and Lost Income	Coverage for costs to mitigate or respond to an alleged cyber incident and lost income following damage to the Insured's reputation following a cyber incident.
Dependent Business Income Loss	Income loss/extra expense due to a network outage or disruption that originates from a security/privacy incident at a dependent third party provider, leaving your operations with a disruption.

Key coverage enhancements

Product Recall	Coverage for 1 st and/or 3 rd party recall losses arising from negligent performance of a technology product or impaired product
Property Damage & Physical Business Interruption	Affirmative coverage for property damage arising from a cyber incident, providing coverage for risks that are not traditionally found in the property marketplace
Voluntary Shutdown	Coverage for network business interruption arising from a voluntary shutdown of systems by the Insured.
GDPR & CCPA Non-Compliance	Coverage for non-compliance with privacy and data collection laws and regulations.
Business Interruption Trigger & Indemnity Period	Expanded triggers on first party to account for interruptions of the <i>business</i> , versus computer system. For example, ADI has coverage for outage less than 10 hours, if it is followed by business interruption that is more.
Cyber Terrorism	Coverage for acts of terrorism
Social Engineering	Filling the gap in Cyber and computer crime policies for social engineering risks. No call back provision.
Covered Business Interruption Costs	Coverage for continuing operating expenses (including payroll) and forensics costs incurred to appraise for the business interruption loss.
Reputational Harm	Providing coverage for loss of net income following adverse publicity of a cyber incident.
Betterment	Coverage for costs to improve software and systems following a loss.

Cyber underwriting criteria

Focus areas for underwriters

Remote Desktop Protocol

RDP is a dominant attack vector for ransomware.

Recommendations to secure

RDP include:

- VPN
- Encryption
- RDP Gateway
- Complex passwords



Multifactor Authentication

In addition to securing RDP, insurers are looking for insureds to utilize MFA to secure:

- Email
- Network Access
- Privileged User Accounts
- Virtual Desktop Instances (VDI)
- Cloud resources including Office365



Additional Safeguards

- Placement within the Network
- Network Level Authentication (NLA)
- Endpoint Detection Protection and Response
- Limit Domain Administrator Account Access and regularly audit Administrator Accounts and monitoring of Admin Accounts
- Regular cybersecurity awareness and phishing training
- If using O365, O365 Advanced Threat Protection add-on and Defender
- Email security – SPF (Sender Policy Framework), DKIM (Domain Keys Identified Mail), DMARC (Domain-based Message Authentication Reporting and Conformance)
- Business Continuity Plans & Incident Response Plans that are tested on at least annually
- Use of account-naming convention that does not reveal organizational information
- 24/7 SOC or MSSP solution
- PAM Tool



Back-up Policies

Property secured back-ups reduce the severity of Ransomware losses.

Recommendations include:

- Encrypting backups
- Segregating backups; physically stored offsite and offline
- Regular testing backups for data integrity and restorability
- Regularly performing full and incremental backups of data
- Regular testing of Incident Response/Business Continuity Plan including ransomware events
- 3-2-1 backup strategy



Segregation of Networks/Assets

- Segregate operational technology and information technology networks
- Ability to test updates in a sandbox environment prior to deployment

Risk transfer strategies

Higher retention

- Consider in order to address Insurer concern with frequency of losses – if aligned with your risk tolerance.
- Can also use captive to infill higher SIR.



Risk sharing

- Quota Share participation in lieu of single participant layers – Claims control would need to be codified.
- Co-Insurance – consider primary only vs excess only vs entire tower (to address concern with frequency and/or severity).
- Can also use captive for retained risk.



Accept sub-limits for lower priority coverages

- Some coverages, based on your risk profile, may not be equally important.



Risk engineering | mid term credit or coverage

- Agreement to implement certain recommended actions within the policy term resulting in a credit to be applied on renewal, or removal of any sub limits.
- Most effective if specific controls are of underwriter concern.



Captive

- Introduce captive as “quota share” or full layer capacity on select attachments.
- Use captive capacity as leverage in market negotiations and as replacement capacity as needed.
- Leverage captive for any new retained risk – higher SIR, reduced limits, etc.



Alternative risk transfer: integrated risk

- Combine program with other lines of coverage such as property, crime or D&O.
- Potential for integrated structure on primary only, excess only, or both.
- Various retentions could apply



Alternative risk transfer: Second loss/structured risk

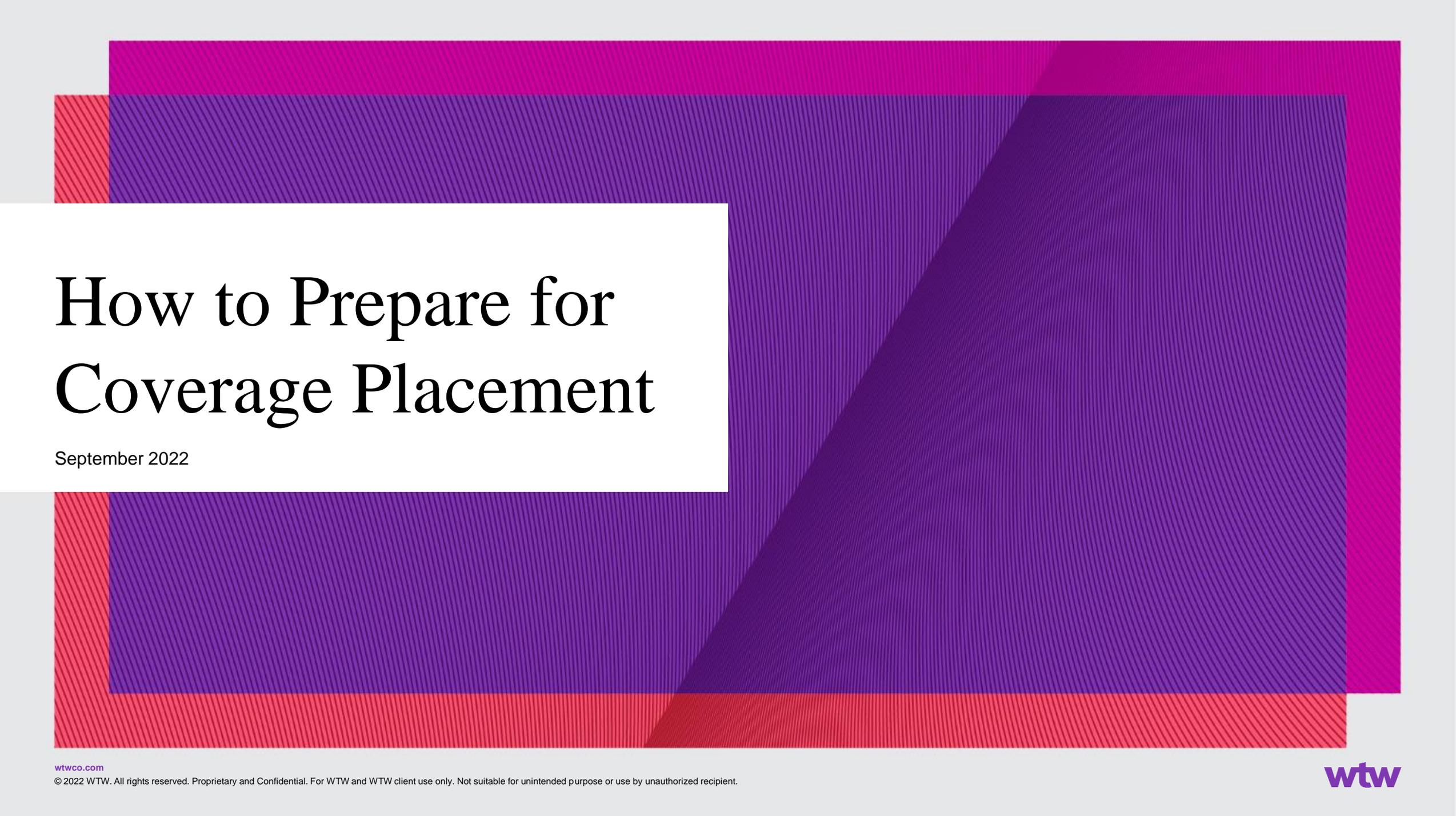
- Second Loss: first loss on the tower is self-insured; policy responds to second loss.
- Structured Risk: Multiyear stop loss program – ultimate cost of program varies depending on the loss costs.



Limit reduction

- Re-examine limits against highest priority exposures and their corresponding impacts.

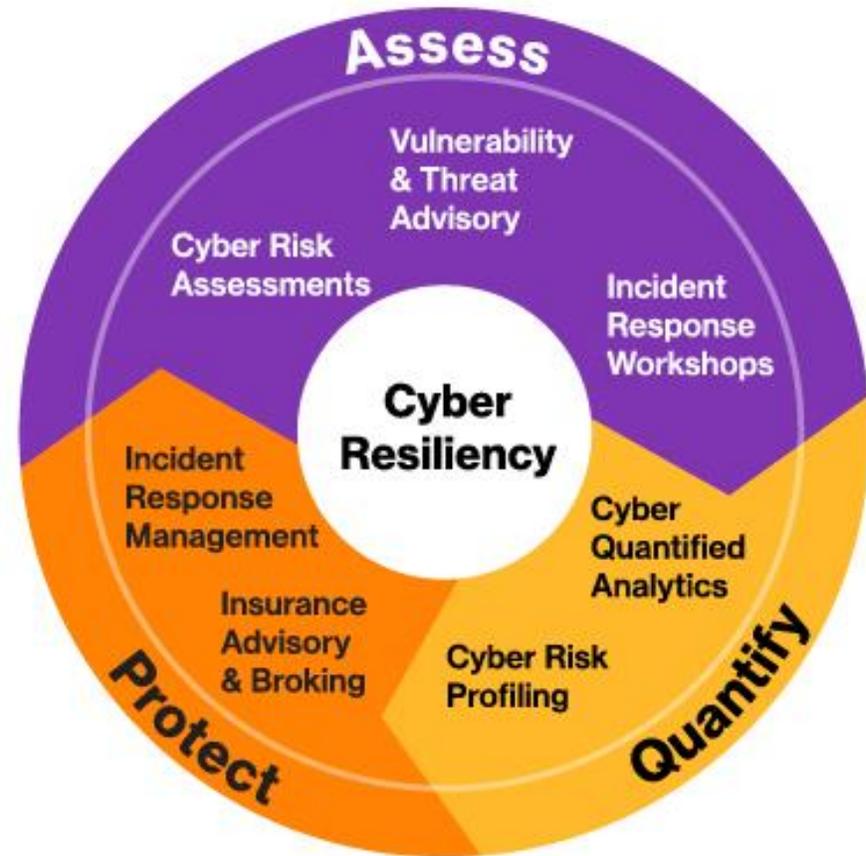




How to Prepare for Coverage Placement

September 2022

Keys to Coverage Placement



Keys to Placement

- **Address Prior Year Deficiencies**
 - Throughout the year address any deficiencies identified during the prior years placement, these can result in increased premiums and sublimits.
- **Provide application at least 60 days in advance**
 - This allows time for new markets to review your risk and allows time for any questions to be answered via email or an underwriting call.
- **Involve Necessary Staff**
 - Leverage CISO, IT Director, or any personnel that can assist in clarification of any unique aspects to your network controls/procedures not outlined on application.
- **Prepare for underwriting call**
 - To assist with the marketing and involvement of new markets be prepared to participate in underwriting call to provide additional information about network security and procedures
- **Prepare roadmap of improvements**
 - Have a plan to prioritize ongoing projects to improve your network security.
- **Claim preparation**
 - In the event of an open claim be prepared to discuss the status of the matter, and if threat actor or malicious code is still on the network. If the matter(s) are closed prepare to discuss what happened and what steps have been taken to prevent losses from a similar attack vector/vulnerability.
- **Review regulatory environment**
 - Review the type of data you hold and where that data comes from and compare it to any new regulatory/statutory filings that could apply to your data.

Cyber risk

Execution in the cyber marketplace

Phase	Assessment	Analytics & Quantification	Mitigation & Strategies	Selection & Protection
Tools	1. Cyber & Ransomware Application	1. Benchmarking	1. Risk Tolerance Evaluation	1. Strategy Evaluation
	2. Cyber Risk Profile Diagnostic	2. Historical Claims Analysis	2. Mitigating Actions	2. Strategy Selection
	3. Workforce Cyber Culture Assessment	3. Cyber Exposure Analysis	3. Action Evaluation	3. Implementation & Cyber Risk Reevaluation
Output	Vulnerabilities, Threats, Risk Scenarios	Benchmarking Cyber Risk Exposure	Risk Tolerance & Mitigation Strategies	Strategy Selection Demonstrable value of Risk Transfer

Questions?

Charles Leonard – charles.leonard2@wtwco.com
Asa Long – asa.long@wtwco.com