GuyCarpenter

CYBER LANDSCAPE & ANALYTICS

AICT Seminar

September 9, 2021

Chris Shafer, VP, GC Cyber Center of Excellence
Jess Fung, MD, GC North American Cyber Analytics Lead

1. The New Global Landscape of Cyber Risk
2. Impact of Evolving Market on Cyber (Re)Insurance
3. Quantifying Cyber Risk

Agenda

1

The New Global Landscape of Cyber Risk

Rising Cyber Claims Trigger Enhanced Underwriting & Investment

Market Changes Taking Hold in 2021

Cyber Insurance Growing Despite Recent Challenges

- Fitch estimates the U.S. cyber market grew by 22% to 2.7B USD in 2020. This represents written premium for cyber standalone and package policies.
- Ransomware events driving loss activity
- Higher propensity of cyber incidents in recent years prompting shifts in underwriting and pricing strategies

Claims Development Revisited

- Change in claim activity as the sophistication of phishing emails, data theft and ransomware continues to mature
- Loss development assumptions for this product line are again being revisited in 2021 to account for the increased data credibility

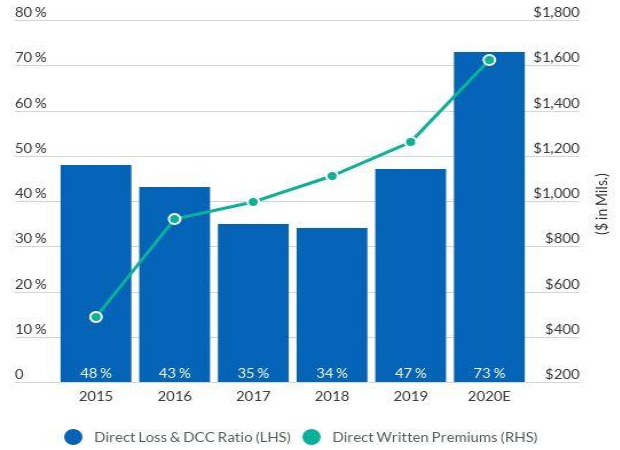
A Call to Arms for Underwriters

- According to the mid-year 2021 Fitch cyber report, the cyber industry direct loss ratio rose to 73% in 2020 from 47% in 2019
- AM Best reported loss ratios increased to 67.8% in 2020 up from 44.8% in 2019
- Portfolio performance varies greatly across various cyber writers
- Across Guy Carpenter's client base, non-cat development increased 15-20% from 2019 to 2020 after previous deterioration of 12-15% in 2018 / 2019

Insurers will have to achieve both significant premium rate increases and tighter coverage terms in order to stage a recovery in underwriting performance over the medium term

P/C Industry Aggregate Standalone Cyber Risk

2020E Direct Loss & DCC Ratios Rose to 73% vs. 47% in 2019



DCC - Defense and cost containment incurred.
Source: Fitch Ratings, S&P Global Market Intelligence.

FitchRatings

Facing pressure on cyber market profitability, the industry has responded by reassessing historical underwriting approaches

Source: Fitch Ratings & S&P Global Market Intelligence

Ransomware was the Loss Driver in 2020

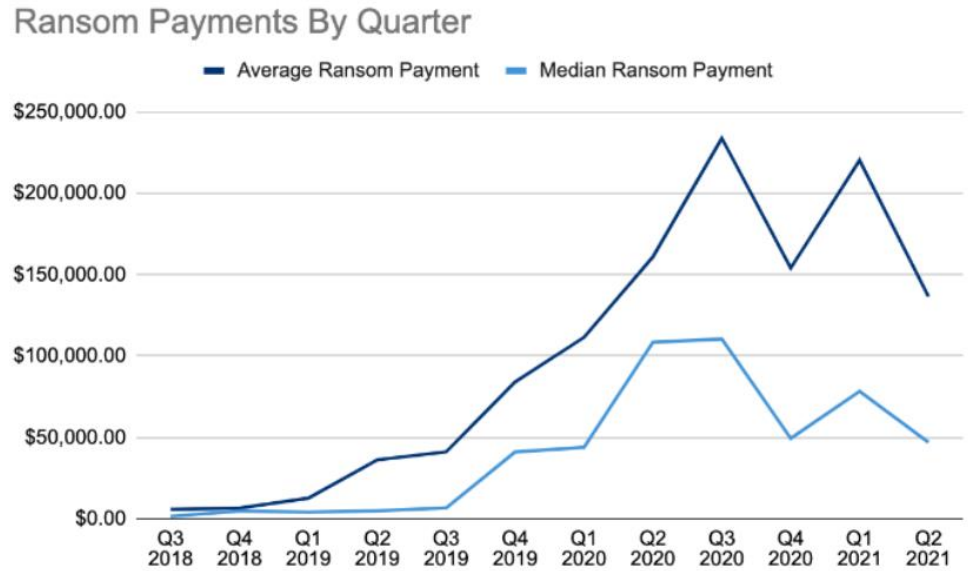
Criminal Business Model Caused Cyber Loss Ratios to Increase

Evolution of Ransomware

- Revenue diversification is less meaningful as ransomware attacks against enterprises forked between big game attacks and an increase in new Ransomware-as-a-service (RaaS) variants targeting small businesses
- Improvements to back up protocols and recovery without ransom payment is muddying the conversation over whether paying the demands is prudent
- High profile attacks on critical infrastructure and supply chains are being viewed as national security threats, applying pressure on governments to take action

Insurance Implications

- To date, ransomware has altered the development of cyber claims. There is faster loss emergence than previously projected due to the 1st party dominance of immediate network downtime, event-related forensics costs and potential extortion payments.
- Recent ransomware loss trends provide more signals to reinsurers in their assessment of risk
- Elevated discussion of how the war exclusion may be invoked
- Industry and public sector collaboration is under way



COVEWARE

Q2 Tides

- New, smaller RaaS pulls down average and median demands
- In 2020, 65% paid their demands. In Q2 2021, that fell to 50%.
- Downtime is 23 days, down from Q1

Public and private changes

- Headline news as a wake up call
- Mobilizing a federal response
- Law enforcement budget and focus
- **Cyber insurance requirements and sharpened underwriting is beginning to force technical acumen**

Ransomware trends are being closely examined across the industry

Source: Coveware Q2 2021 Ransomware Marketplace Report, Marsh statistics

Global Supply Chain Ransom Events

High profile events prompting a more public response

Colonial Pipeline – May 2021

- The extortion event attributed to eastern European group **DarkSide** to whom Colonial paid **USD $4.4m** equivalent ransom demand
- Colonial supplies almost half of the US east coast with fuel and was at least partially shut down for nearly two weeks
- Impact included gas shortages and price hikes, plus criticism over paying the ransom
- DOJ was able to recover at least part of their ransom payment, a detail which is still playing out in terms of insurance impact

JBS Beef – June 2021

- JBS paid a **USD $11m** equivalent ransom demand to Russian group **REvil** in June

Kaseya – July 2021

- **REvil** has claimed responsibility. The FBI described the Kaseya incident as a "supply chain ransomware attack leveraging a vulnerability in Kaseya VSA software against multiple MSPs and their customers."
- **Aggregation Potential**: According to Kaseya, of their 36,000 global customers, 60 on premise MSPs and as many as 1500 downstream customers were impacted.
    - Kaseya has stated publicly they did not pay an extortion demand to obtain keys for customers and downstream entities
    - Insurable impact has been minimal to date

Multiple headline events have prompted the US Government to take action:

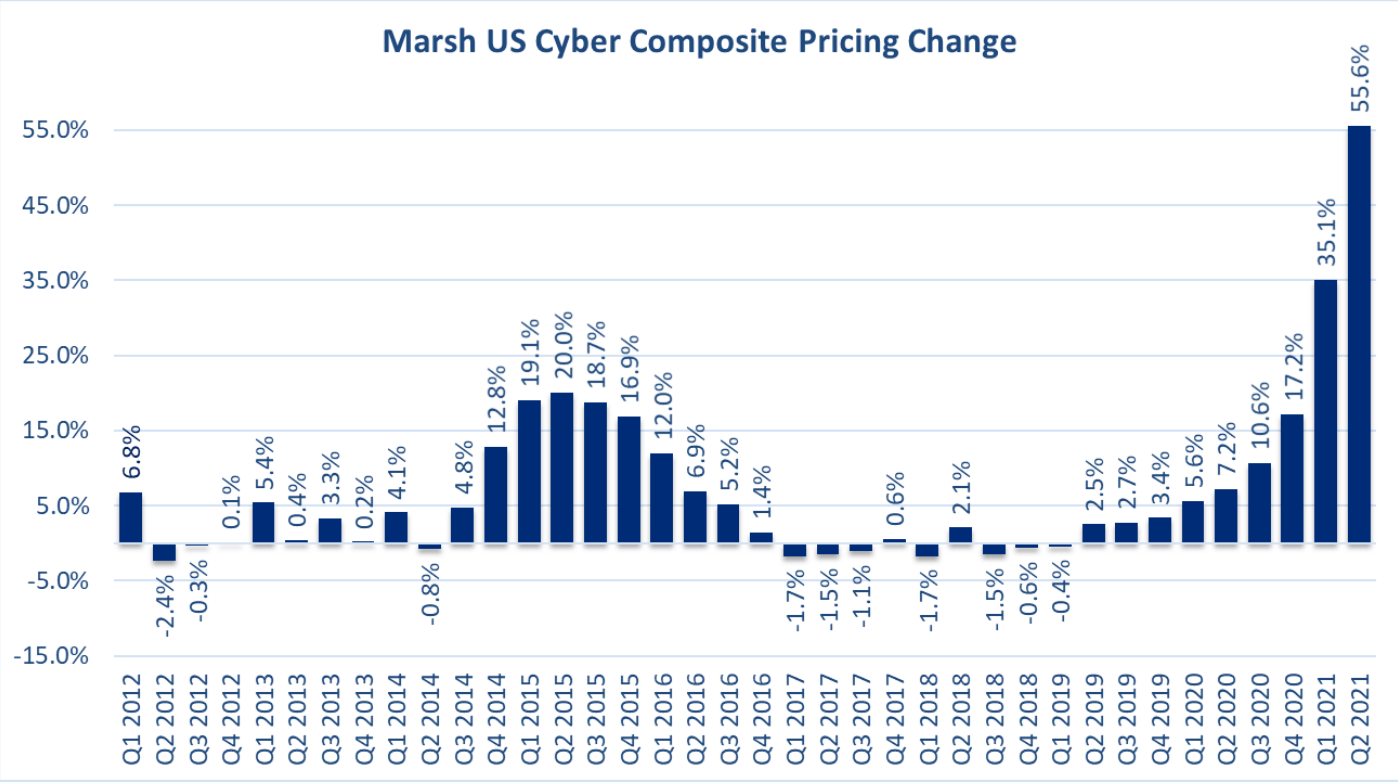
- Formal sanctions against Russia
- DHS laying out cybersecurity regulations specifically for pipelines including reporting incidents
- Exec Order for government agencies and contractors requiring improvements to security controls

Globally, the conversation over "to pay or not to pay" the ransom has been reignited after reports of significant demands and payments.

AXA France has taken a stance on ransom payments. It is unclear if other insurers will follow suit.

Pricing and Terms Offset Development

Cyber US - 1st Q 2012 to 2nd Q 2021



The Marsh Global Insurance Market Index is a proprietary measure of commercial insurance premium pricing change at renewal, representing the world's major insurance markets and comprising nearly 90% of Marsh's premium. The pricing change captures year-over-year pricing movement, measured quarterly. The pricing change metrics are based on a combination of statistical data and surveyed opinions from Marsh placement leaders worldwide. All references to pricing and pricing movements in this report, where stated in terms of percentages, should be considered averages unless otherwise noted.

Market Commentary

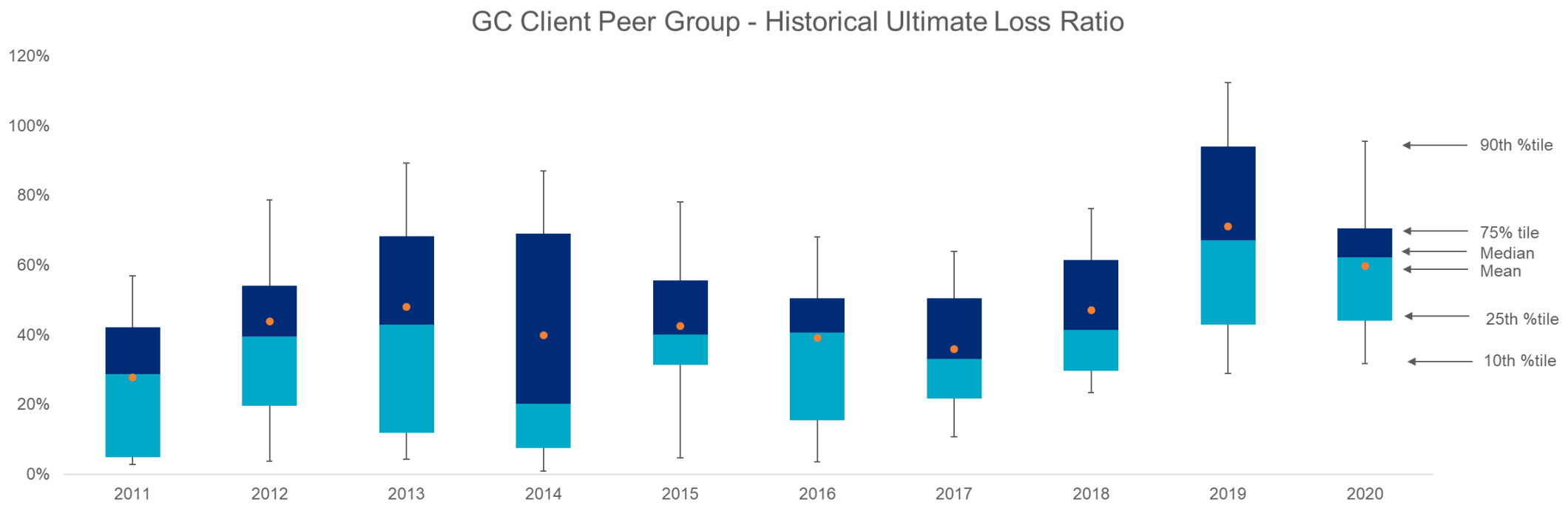
Cyber pricing increased 55% in the 2nd Quarter, significantly higher than the prior quarter.

- Cyber pricing increased every month of quarter i.e. April: 40%; May: 47% and June 2021: 74%.
- While this exhibit captures Marsh's US client base, pricing is reflective of market change globally.
- Rate change shown evidenced here has not been risk adjusted. Therefore, increases would be higher if contemplating the contracted coverage.
- Most insurers scaled back limit deployment to a maximum of USD5 million to USD10 million for any one risk, and narrowed coverage for ransomware-related losses.
- Many insurers have declined to quote risks in certain industry classes or without certain controls. They are also often imposing higher retentions and co-insurance provisions for the risk they do support.

Source: Marsh

Client Peer Analysis and Benchmarking

Carrier Industry Performance



Results vary by year as shown in the chart due to carriers' underlying composition of business, limits & attachment points

The GC Cyber Analytics team can assist in interpreting global carrier market cyber trends

2

Impact of Evolving Market on Cyber (Re)Insurance

The Industry's Response to Ransomware is Fluid

Keeping Our Clients Differentiated In Performance Is Vital

Ongoing Issue - Guy Carpenter's extensive global client base allows us insight into how cyber peers are shifting underwriting strategy to address ransomware risk and its portfolio performance impacts.

PRICING
Push rate as answer

- Cyber is a developing market seeking product adoption. Many in the industry are not willing to exclude or modify coverage despite uptick in ransomware claims for fear of making the product less relevant
- Rate was taken as an immediate action, but there was recognition this alone would not solve the problem for impacted portfolios
- Ransomware driving quicker loss emergence within portfolios, particularly since 2017

RESEARCH
Better understanding of the issue

- Many (re)insurers conducted analyses to determine the affected portfolio segments, industry classes and coverages most triggered
- Refinements included the development of underwriting strategies, pricing correlations and underwriting questionnaires
- The intent was to determine which controls best mitigated ransomware risk
- This includes extensive and ongoing work to understand and diagnose the data and events

TOOLS
Leverage analysis/ data to build tools

- Some analysis led to the introduction of stronger risk selection criteria and tools
- Impacted portfolios invested in partnerships with strategic vendors to aid in data capture and cybersecurity offerings
- We saw a marrying of these partner insights with an updated underwriting application to create a multi-disciplined underwriting view

FUTURE
Where are things going?

- After 12-18 months of debating the effectiveness of coverage amendments, the industry is now executing on new underwriting strategies (excluding extortion payouts, sublimiting ransomware events, limits reductions, coinsurance clauses) and/or security requirements.
- OFAC/DOJ may help to pave the way for change given heightened discussion around criminal actors
- Rate push continues

Managing Cyber Risk

Leveraging Updated Underwriting Techniques

Cybersecurity partnerships augmenting risk selection

Ongoing monitoring/feedback of security postures throughout policy term

Defined affirmative offering, cross-sell strategy with consistent usage of underwriting guidelines and pricing methodologies

Cross LOB underwriting/ risk engineering/ claims collaboration, view of risk

Continuous underwriting training, particularly on privacy regulation globally

Renewed emphasis on limits management strategies

Defined ransomware strategy to include considerations for:

- Laser specific underwriting questions around common entry points (RDP ports, blocking malicious traffic) and ability to avoid payment though backup protocols
- Sublimit approach, separate retention, and/or coinsurance utilization for ransomware events
- Prescribed metrics for portfolio management
- Analysis of ransomware performance by industry, coverage type
- Clearly defined tiers by risk profiles, link to underwriting approach
- Excess/follow form strategy in place for amended lower layers
- View of preferred attachment
- Regional differentiation as needed (i.e. no extortion payment)
- Combined view of risk merging updated questionnaires and 3rd party risk scoring
- Re-evaluation of waiting period adequacy
- Segment analysis to determine if revenue appetite shifts are needed

Newly introduced strategies are influenced by tower purchased, broker preferences and commercial viability

Cyber is Top of Mind for Rating Agencies

The agencies specifically look at the way insurers are managing and planning for aggregation.

S&P Global Ratings

- Aggressively called for insurers to accelerate the development of the standalone cyber product space rather than packaged
- Critical of silent cyber risk on other policies. They call for insurer centers of excellence to the benefit of reinsurance buying strategies
- Apprehensive of balance sheet accumulation risk for aggressively growing insurers

Moody's

- Encouraged by insurers who are well capitalized writing cyber
- Sees agg modeling as difficult to nail down since the risk can shift faster and evolves differently than other lines
- Recently launched a JV called Team 8 to focus on outside/in assessments and seeks to create a cyber risk rating

FitchRatings

- Views increased buying habits driven by customer demand and strategies to clarify ambiguous or silent language
- The velocity of ransom attacks prohibits the insurance industry from addressing claims trend in the short term
- Cyber is uniquely difficult to apply traditional diversification, industry, and geography accumulation strategies

AM BEST SINCE 1899

- Having a well-defined risk identification process that can quantify an insurer's exposure the cyber risk is essential. Stress testing, external models, regular reporting/review
- Called for insurers to be regularly reassessing risk management plans especially in a high growth market. Seeks a balance between increased policy count and limits with critical underwriting

Common themes:

Want to see clarity ability to adequately underwrite small and mid size risks

Precision on where cyber is offered or excluded

Insurers' evolving underwriting strategies to keep up with growing threat and increased digitization

Bullish on regulation and legislation. Want to see more prescriptive global coordination

Coordination Between Industries

DarkWeb IQ is recently formed and coming out of stealth

- Early stage start up aiming to coordinate public-private fight against ransomware
- Assessed RaaS activity and works with law enforcement and insurers to enable remediation before a network is breached

CyberAcuView announced their launch in June 2021

- New company created by investment from 7 major cyber insurance carriers to provide certain data.
- Outcome forecasted to be industry wide mitigation, cyber risk resilience, and foster a competitive cyber insurance marketplace.

Ransomware Task Force released their first report out in April 2021

- Public-private collaboration of experts in cybersecurity, government, law enforcement, civil groups, and internationals orgs
- Wrote and released a ransomware framework of 48 preventative and mitigation recommendations

Verisk Cyber Data Exchange aggregates cyber insurance policy exposure and claims

- Provide summarized metrics via interactive dashboards to participating companies updated quarterly
- Data reported to regulatory agencies by ISO on behalf of insurance companies Will provide account level cybersecurity data back to contributors for portfolios uploaded

Reinsurance Market Response

Having an Accurate Pulse on This Rapidly Changing Market Is Critical for Success

Reinsurance Strategies

- Group risk tolerances for cyber have decreased causing more demand for reinsurance capacity
- Given heightened demand, reinsurance support is driven by deep engagement and confidence in underwriting strategy
- Leverage broader placements to achieve Cyber placement economics
- Movement toward ground-up quota shares rather than VQS/QQS structures
- New aggregate placements supplementing sideways proportional protection for global cyber writers

Pricing

- Pricing on all structures has increased due to diminished profitability and increased uncertainty
  - Aggregate Programs:
    - Risk-adjusted rate increases continue
    - Limited pricing consensus in the cyber reinsurance market
  - Pro-rata structures:
    - Ceding commission reductions on top of prior year reductions
    - Pricing pressure correlated to level of loss ratio cap

Hard Market Dynamics

Capacity

- Remains finite and not increasing:
  - Uncertain market slowing new traditional market entrants
  - Existing markets limiting available capacity
  - Timing to market is critical to minimize placement benchmarking
- Key considerations for capacity deployment:
  - Portfolio performance against peers
  - Depth and timeliness of data provided
  - Impact of ransomware on performance and strategic response
  - Quarterly update on claims development

Terms

- War exclusion: certain markets require broader language that is more expansive than a kinetic war exclusion
  - Guy Carpenter is successful in having reinsurers follow the fortunes wording with war to ensure coverage alignment
- Reinsurers are looking to increase attachment points for agg XOLs to maintain a similar likelihood of attachment going forward
  - Loss ratio attachment preferred over monetary attachment

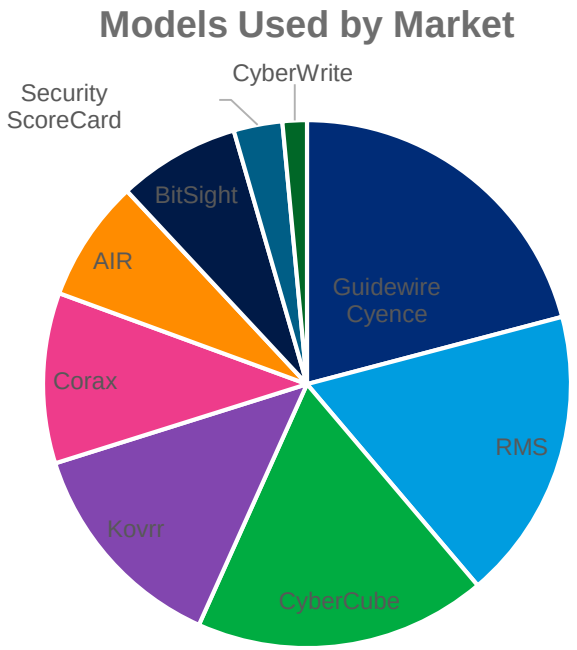
3

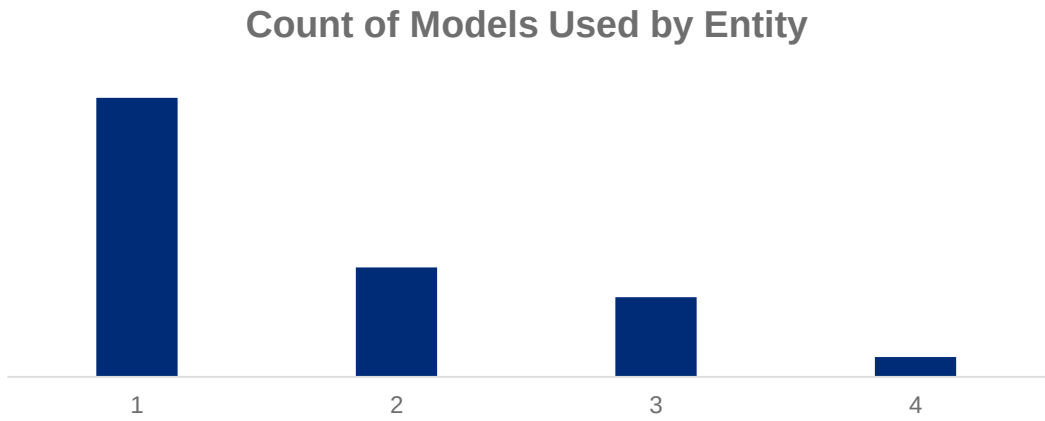
Quantifying Cyber Risk

Vendor Engagement and the Modelling Landscape

Vendor Market Penetration

- **Model market shares**
  - The chart below sets out our derived market shares for some of the key cyber models
  - This is based on our best our discussions with clients relating to individual vendors, however the **picture is changing** rapidly with many choosing to go through vendor assessments and RFPs





- **Count of vendors by entity**
  - The chart above sets out known counts of vendors based on GC Cyber Analytics' market intelligence
  - There is likely a reporting bias **towards** those with some usage of vendor models, but **possibly the understates** the full total in some cases
  - What is clear is that entities are increasingly leveraging multiple views, in addition to their own view of cyber risk

GC Stress Test: WannaCry / NotPetya What-if

Silent Cyber Stress Test

Actual Event

Responsible parties: Russian nation state attack
Incident: Critical shipping and distribution downtime, ransom, data loss
Technical: Spread using a Ukrainian tax software to exploit an unpatched Windows vulnerability called EternalBlue
Revealed: June 27, 2017
Incident size: 300,000 potential victims
Intent: Significant disruption

Stress Scenario & Cascading Impact

Primary stressors: amplifying ransom demand + prolonged disruption during holiday season

- Data exfiltration prior to encryption, with progressively and exponentially increasing ransom demand over time
- Cost of ransom, forensics, legal fees, data breach regulatory fines
- Pipeline shutdown → gas shortages, price hikes, impact on commercial travel
- Logistics tracking software inaccessible → global distribution delay of consumer & healthcare goods, esp. during holiday season
- Data loss with no back up → lost or diminished value of hardware
- Reduction in revenue guidance to financial markets → stock drops
- Breaches of contracts to downstream customers → consumer confidence loss, reputational damage

WannaCry / NotPetya What-if

Parallel Timelines

Actual Event

June 27	June 28	July 5	July 15	+45 days
In the weeks following WannaCry and Petya, a similar more dangerous ransomware strain emerges out of Ukraine. NotPetya is spread without user requirements. It exploits an unpatched vulnerability on certain Windows devices.	Operations are halt at huge multinational corporations including Mondelez, Merck, and AP Moller-Maersk	Multiple impacted organizations are still nearly fully shut down. Scope broadens to potentially all hardware running on Windows. Ransom demands appear but are not the motivations for the attack	Operations begin again though using multiple manual processes Damage to hardware including bricked servers is assessed Significant shipping and distribution delays	Legal process attempts to determine whether NotPetya is an act of war Significant revenue decreases from impacted orgs Multiple insurance policies are triggered highlighting scope of a cyber event
Discovery	**Scope**	**Limited recovery**	**Patching**	**Assessing damage**
Dec 1	**Dec 2**	**Dec 9**	**Dec 19**	**+45 days**
Multiple multi national organizations report widespread outages and no access to critical software and files. Determined to be a Zero Day attack	Scale estimated to be 500,000 potentially vulnerable orgs. Dozens of pipeline, gas distributors, and shipping orgs voluntarily shut down. Goal is determined to be financial and 6 digit USD ransom demands emerge	The vendor exploit patches are sent to customers but require testing and deployment. Impacted orgs' forensic teams determine data has been exfiltrated and deleted.	Unpaid ransom demands begin increasing 10x. Paid ransoms regain some access to their systems. Actors begin requesting second ransom payment under threat of publishing data publicly	Without backups some data is lost; some confidential data is published Threat of other zero-days Ensuing financial loss and liability

Stress Scenario

GC Stress Test: SolarWinds What-if

Affirmative Cyber Stress Test

Actual Event

Responsible parties: Most likely APT29 (Cozy Bear/Russian SVR)
Incident: Targeted software supply-chain attack
Technical: Compromised software updates used to install backdoor access
Revealed: December 13, 2020
Incident size: 18,000 SolarWinds' customers downloaded the malicious update
Intent: Espionage

Stress Scenario & Cascading Impact

Primary stressors: financially motivated attack beyond espionage; extortion / ransomware on non-FI + fraudulent transactions for FI

- Impact of downtime from all of Top 10 Telecom and 425 of Fortune 500 companies crosses multiple industries
- Widespread data exfiltration, ranging from login credentials to financial information to trade secrets
- Multiple backdoors created at initial compromise stage for future exploits → extensive claims development period
- Disproportionately higher impact on medium-to-large risks that purchase standalone cyber policies

SolarWinds What-if

Parallel Timelines

Actual Event

Dec 13, 2020	Dec 14, 2020	Dec 31, 2020	Jan 5, 2021	Jan 27-29	Feb 24
Discovery	**Announcement**	**Impact**	**Gov Response**	**Announcement 2**	**Impact 2**
Investigating their own unrelated breach, FireEye discovers and tweets about a backdoor in a SolarWinds product attackers manipulated to deploy malicious code to SolarWinds customers	SolarWinds publicly discloses the vulnerability and issues 2 hot fixes	Potentially 18,000 customers may have downloaded the vulnerability. MSFT attributes the attack to Russia, likely c Oct '19. No reports of ransom demands or data exfiltration emerge	Multiple US agencies call the attack by Russia an Advanced Persistent Threat. Calls it an intelligence gathering event on gov. and non gov't bodies.	CISA and Solarwinds each issue advisories about the event	MSFT and FireEye testify in congress that likely 1000+ skilled engineers worked on this exploit The event is deemed the most sophisticated of its kind in history

Stress Scenario

Discovery via huge ransom demands on thousands of companies, stolen privileged credentials at FIs, moving money to offshore accounts	Compromised network monitoring and creds could mean hot fixes and patches (which can be issued immediately) will not be a viable solution	Customers include Top 10 US Telecom and 425/500 F500 companies	Private and government, financial, IP, and privileged data is exfiltrated on a massive scale. Attack could include second ransoms		Undetected backdoors created and a new cascade of attacks follows weeks later

Questions