Gallagher Re

Cyber IQ

Are ransomware claims causing over-reserving?

Introduction

The cyber threat landscape is constantly evolving and maturing, yet over recent years there has been one unavoidable trend: The rise of ransomware. The continued growth in **frequency, severity and sophistication of attacks** creates an additional level of uncertainty when projecting ultimate loss ratios in an already volatile class of business.

This paper outlines some of the **challenges** when considering development patterns for ransomware claims to **avoid over-reserving or suboptimal business planning and reinsurance purchasing**.

Ransomware Proportion of Incurred Losses by YoA

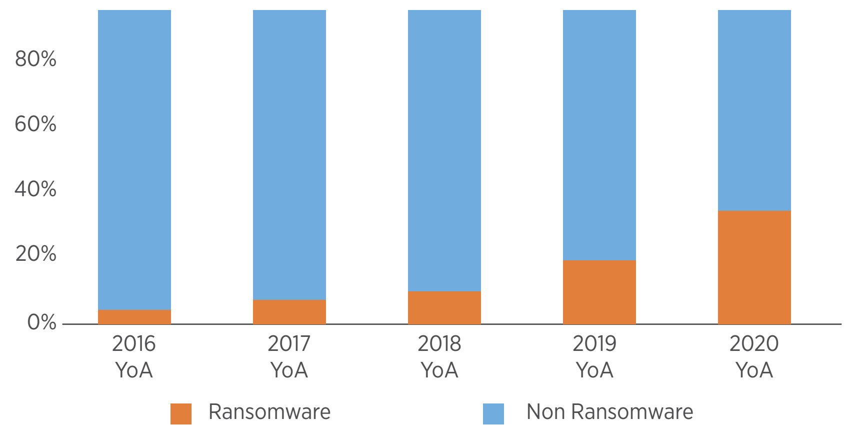


Figure 1 Based on consolidated claims experience from Gallagher Re clients.

Year of Account - Incurred Loss Ratio (Inc/ GrossNet Ultimate Premium)

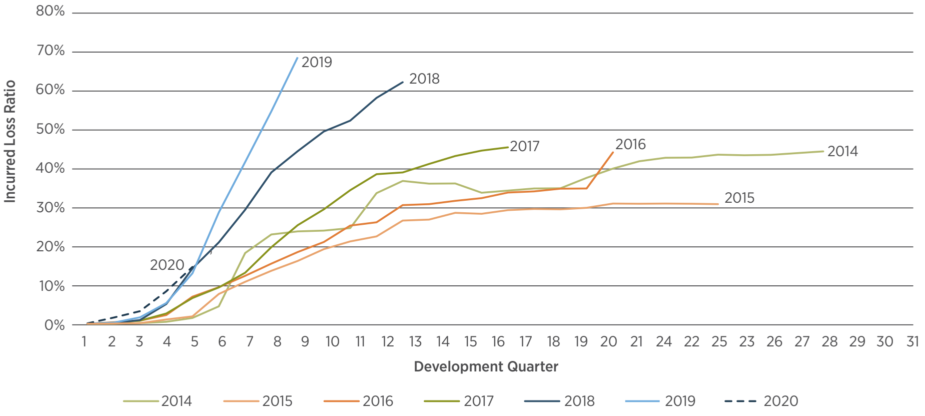


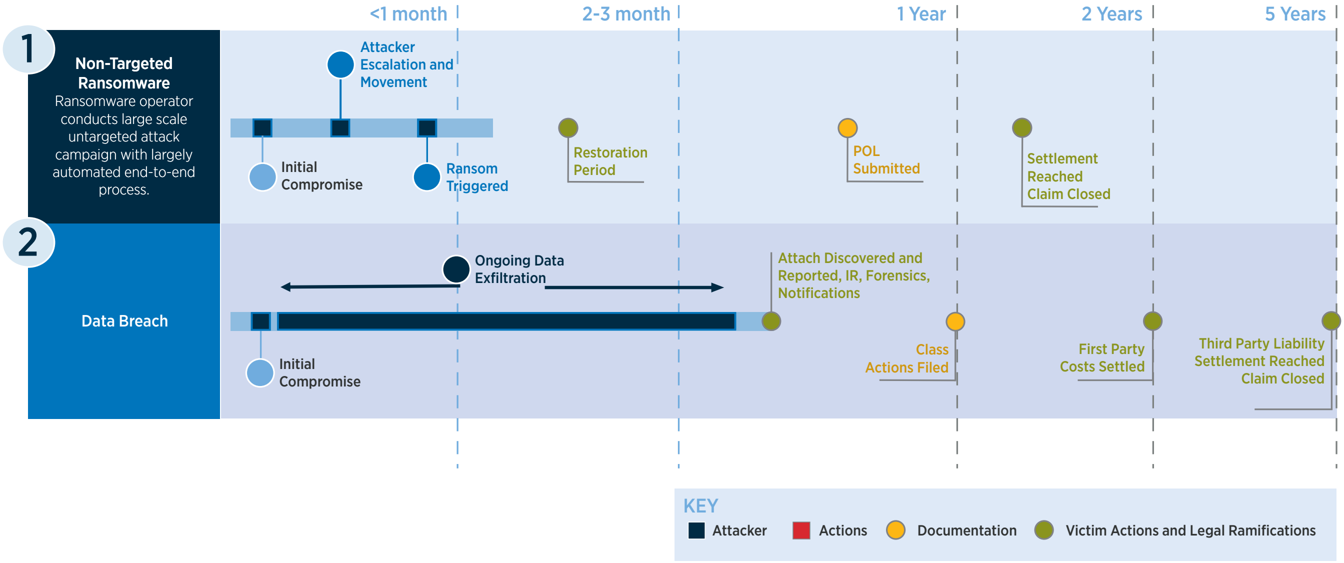
Figure 2 Lloyd's CY Risk Code as at Q2 2021

The type, frequency and severity of cyber losses has developed over the course of the last decade. Whilst privacy breach notification (third party liability) remains a pertinent exposure, the market has observed year on year loss deterioration driven by the proliferation of ransomware, regulatory fines (and the insurability thereof) and Business Interruption (first party). For 2020 YOA, we estimate that ransomware losses make up roughly 35% of the total incurred losses experienced by our clients to date (Figure 1).

Considering, the Lloyd's CY risk code (Figure 2) each year can be seen to be developing to higher loss ratios at the same point in time; however due to the **shift in mix of claims** it is possible that development patterns may be quickening. It is likely that part of this trend is due to **quicker reporting of ransomware claims** rather than simply higher underlying ultimate loss ratios. As such, applying historical patterns with longer tails driven by more traditional third party cyber losses, may be inappropriate for recent years.

Hypothesis: Are ransomware claims speeding up development patterns?

Figure 3 Illustrates an example timeline for two cyber-attacks.



<1 month
2-3 month
1 Year
2 Years
5 Years
1
Non-Targeted Ransomware
Ransomware operator conducts large scale untargeted attack campaign with largely automated end-to-end process.
Attacker Escalation and Movement
Initial Compromise
Ransom Triggered
Restoration Period
POL Submitted
Settlement Reached Claim Closed
2
Data Breach
Ongoing Data Exfiltration
Initial Compromise
Attach Discovered and Reported, IR, Forensics, Notifications
Class Actions Filed
First Party Costs Settled
Third Party Liability Settlement Reached Claim Closed
KEY
■ Attacker
🟥 Actions
● Documentation
● Victim Actions and Legal Ramifications

Ransomware claims are typically discovered, reported, quantified and settled quicker than data breach claims posing the hypothesis: Are ransomware claims speeding up development patterns?

Simple ransomware claims should have a shorter case reserving lifecycle than data breach claims for two reasons. First, they tend to be more rapidly visible to the insured as the attacker demands a ransom soon after initial compromise (usually less than a month compared to six months to a year for data breach claims). Second, the absence of the third party liability element and generally short business interruption phase, renders it easier for claims teams to set a reliable case estimate soon after reporting.

However, we would note that an increasing proportion of ransomware claims have an element of data breach involved due to ongoing data exfiltration and that this may dilute the quickening of reporting patterns.

For

- Discovery and notification of ransomware losses surface **much quicker** than traditional data breach events as insureds are immediately or very soon aware of when they suffer a ransomware event. Under a claims made basis, this would not directly impact development patterns.
- The ransom is typically paid following a **cost benefit analysis** to determine whether it will be cheaper paying the ransom than recovering systems and suffering prolonged business interruption. Where it is paid then a period of restoration is often shorter and therefore the business interruption claim impact will be limited. In this situation, we could expect the claim to close even sooner than the timeline suggests (1.5 years).
- Without data theft, there is limited exposure to long tail third party liability and / or claims which can take years to settle. Under a typical ransomware event, we expect systems to be restored and running within a few months, then there is 180 days to submit the POL, with final negotiations and settlement typically taking a few more months. Overall, we expect **the ransomware loss to be settled** within 1.5 years.

- The impact of double extortion ransomware, where data is exfiltrated and then leaked or sold if the ransom is not paid, will **depend on the industry targeted**. For example, if a manufacturer is targeted and data is stolen, it is more likely that the stolen data will include corporate IP/commercially sensitive information rather than Personally Identifiable Information (PII) / Payment Card Industry (PCI) / Protected Health Information (PHI). However, if the stolen data includes PII/PCI/PHI, it is likely that the manufacturer would need to consider: making notifications to regulators and affected customers; the possibility of exposure to class actions and law suits; and setting up call centres credit monitoring services for affected customers.

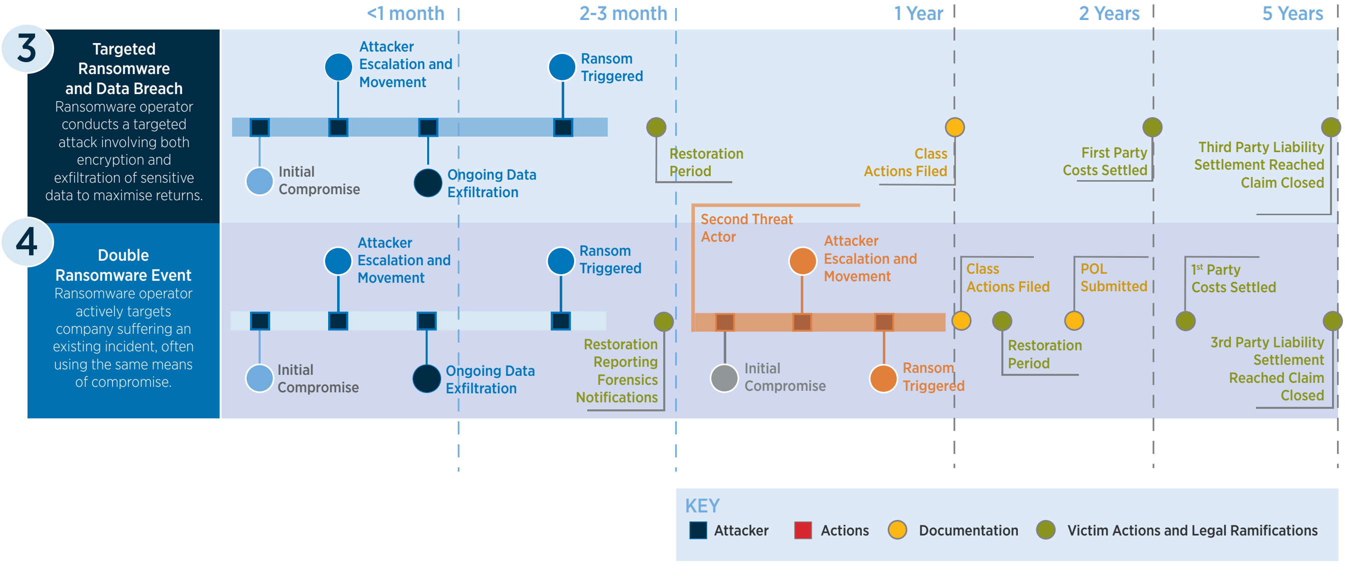
Against

- **Double extortion ransomware**, where the threat actor extorts for data exfiltration in addition to encryption, is observed in 77% of cases as of Q1 2021**, having grown from just 27% in Q3 of 2020.* When **data is exfiltrated during a ransomware event**, then the event could have similar timeline to data breach. The level of third party liability and settlement speed will increase significantly if large volumes of PII/PCI/PHI is stolen. However, in many cases an attacker exfiltrates only the information they can access with ease to trigger the extortion, as opposed to a company's most sensitive or valuable information. This trend in double extortion may not endure as ransom payments for exfiltrated data are less common, owing to limited trust in the criminal appropriately deleting the data as promised and a limited offset of data breach costs incurred.
- **Double ransomware attacks**, where a victim suffers a ransomware event multiple times in a short timeframe, are also increasing in frequency. Although this phenomenon is largely driven by different threat actors exploiting the same vulnerability or compromise in a victim's network, some ransomware crews e.g., Conti have been known to re-infect previous victims. Depending on the threat actors responsible, the timeframes and the tools and methods exploited, this may be classified as one or more claims.

Double extortion ransomware, where the threat actor extorts for data exfiltration in addition to encryption, is observed in 77% of cases as of Q1 2021**, having grown from just 27% in Q3 of 2020*.

***Source:** Ransomware Payments Decline in Q4 2020 (coveware.com)
****Source:** Ransomware Attack Vectors shift as New Software Vulnerability Exploits Abound (coveware.com)

Figure 4 Highlights example timelines for ransomware events that could have timelines similar to data breach losses.

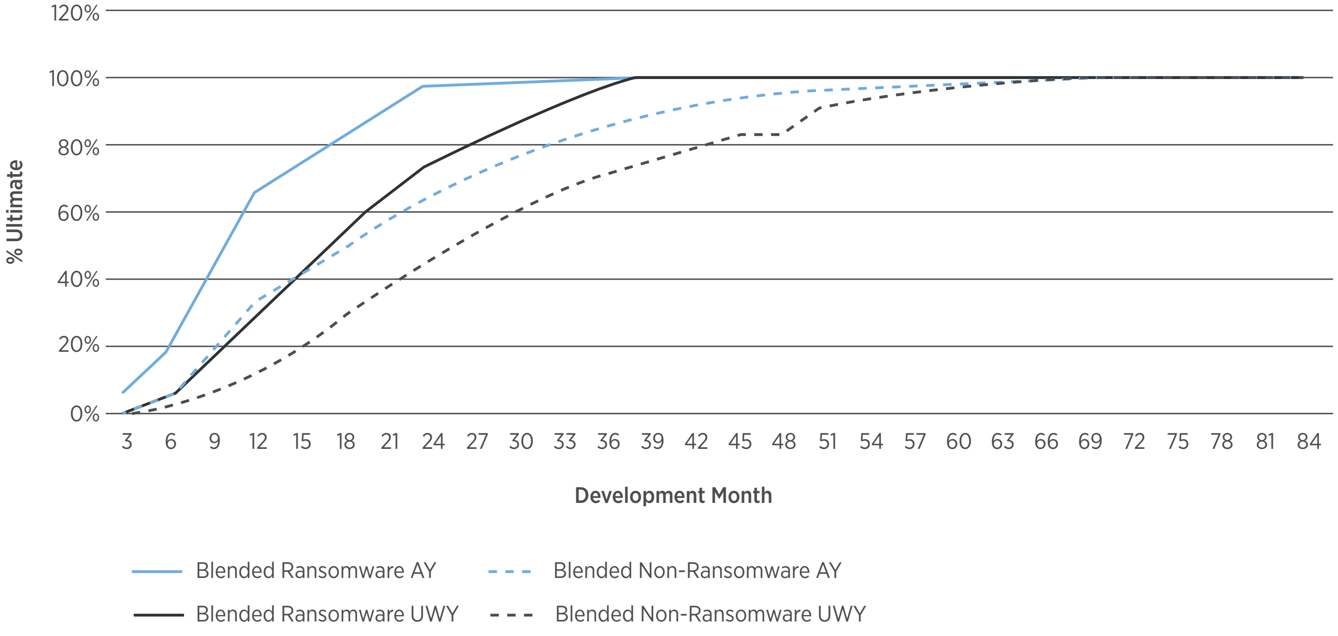

<1 month
2-3 month
1 Year
2 Years
5 Years
3
Targeted Ransomware and Data Breach
Ransomware operator conducts a targeted attack involving both encryption and exfiltration of sensitive data to maximise returns.
Attacker Escalation and Movement
Ransom Triggered
Initial Compromise
Ongoing Data Exfiltration
Restoration Period
Class Actions Filed
First Party Costs Settled
Third Party Liability Settlement Reached Claim Closed
4
Double Ransomware Event
Ransomware operator actively targets company suffering an existing incident, often using the same means of compromise.
Attacker Escalation and Movement
Ransom Triggered
Initial Compromise
Ongoing Data Exfiltration
Restoration Reporting Forensics Notifications
Second Threat Actor
Attacker Escalation and Movement
Initial Compromise
Ransom Triggered
Class Actions Filed
POL Submitted
Restoration Period
1st Party Costs Settled
3rd Party Liability Settlement Reached Claim Closed
KEY
■ Attacker
■ Actions
● Documentation
● Victim Actions and Legal Ramifications

Gallagher Re client study

Gallagher Re has consolidated claims experience from five clients to investigate and understand potential patterns in developing ransomware and non-ransomware losses independently.

Benchmark Non/Ransomware Development Patterns

Figure 5 shows blended benchmark patterns on both a Underwriting Year (UWY) and Accident Year (AY) basis. The clients are predominantly US focused and write a mixture primary/excess, various industries and revenue segments.



Examining the graph, it is clear that there is a difference in the development of cyber claims:

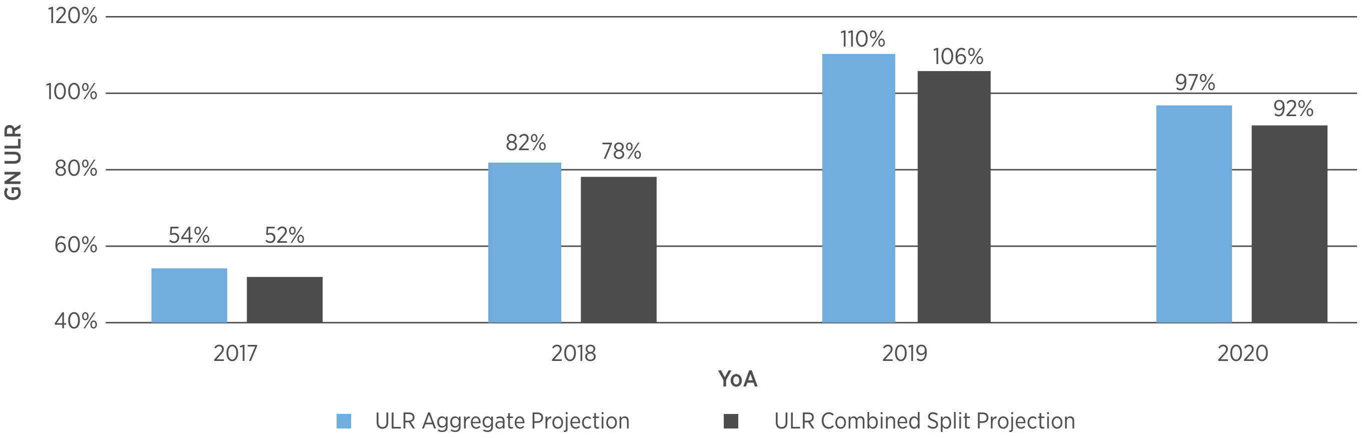
- Ransomware development patterns are on average significantly quicker than non-ransomware, however, we note one of the five clients did not observe this trend.
- The blended patterns in Figure 5 are made up of the underlying clients' ransomware patterns noting that there are significant differences between the clients' patterns driven by a combination of the portfolio makeup, underwriting standards and claims handling.

Headline consequences are:

- The material difference in the ransomware and non-ransomware development patterns suggest it may be beneficial to carry out reserve analysis at a **more granular level** or, at least, apply appropriate adjustment factors for increasing proportions of ransomware claims. Aggregate analyses may **materially overstate the ULRs** in more recent years where the proportion of ransomware losses is higher than previously observed.

Figure 6 demonstrates the potential difference in ULRs between an aggregate projection and a granular combined split ransomware and non-ransomware projection.

Lloyd's CY ULR - Aggregate V Combined Split Projections



- It may also help for claims systems to develop more complex tagging of loss types (e.g., ransomware vs ransomware with data exfiltration vs double ransomware).
- While cyber risk continues to evolve, the industry experiences challenges when applying traditional reserving techniques which fundamentally assume that historical experience is a good guide for future trends. As this class matures, we should also **closely monitor softer factors** that are not always easily captured in the data: evolving threat landscape, hackers' motivations, coverage changes, exclusions, peril sublimits, increasing excess points, claims inflation and trends, and more recently increasing rates leading to higher premiums.
- The mix of the insured base may also give insights into vulnerability to the growing types or frequency of new cyber claims in the market which should be reflected in the business planning process.
- We note it is important to classify claims appropriately and continue to monitor loss experience to identify and allow for emerging loss trends.

Gallagher Re's embedded cyber analytics team have built a ransomware model, Gh0st, to help our clients and markets quantify diverse and realistic ransomware scenarios, and optimise their portfolios.

Conclusion

We hope this article encourages market participants to consider the impact of ransomware claims on their cyber reserving methodology and challenges traditional approaches that aggregate all cyber claims in a single triangle.

How can we help?

Business Planning and Reserving

- Benchmarking and enhancing your ransomware and non-ransomware patterns. Gallagher Re can develop benchmark patterns that align with the characteristics (region, revenue target, primary/excess, industry mix) of your cyber portfolio.
- Peer reviewing your projected ultimate loss ratios and assistance with annual business planning (including inputs for capital modelling).

Capital Modelling

- Cognizant of ransomware's impact, Gallagher Re's embedded cyber analytics team built a ransomware model, Gh0st. The proprietary model was created to help our clients and markets quantify diverse and realistic ransomware scenarios, and optimise their portfolios in a rapidly changing and challenging cyber claims environment.
- Provide output from external third party models to quantify the systemic nature of this risk and its overall impact on your portfolio.

Pricing

- Advising the market about the toolkit available to support them in attempting to limit the likelihood and severity of ransomware incidents suffered by insureds. This ranges from providing insureds with advice around cyber hygiene and good practice, to leveraging external scanning data and identifying potential vulnerabilities. Gallagher Re are currently working to better understand the ability of externally scanning data to anticipate cyber-attacks. This is relevant for ransomware as insecure Remote Desktop Protocol (RDP), which is largely scanable from the outside, is estimated to be responsible for over 50% of ransomware events in Q1 2021**.

**Source: Ransomware Attack Vectors shift as New Software Vulnerability Exploits Abound (coveware.com)

Would you like to talk?

Justyna Pikinska
Head of Specialty Analytics

T: +44 (0)207 234 4301

E: Justyna_Pikinska@gallagherre.com

Emily Chillingworth
Analytics Team Leader

T: +44 (0)203 425 3434

E: Emily_Chillingworth@gallagherre.com

Patrick Brooke
Actuary

T: +44 (0)777 432 4922

E: Patrick_Brooke@gallagherre.com

CONDITIONS AND LIMITATIONS

The opinions and views expressed in this bulletin are those of the authors only and are for guidance purposes only. The authors disclaim any liability for reliance upon those opinions and would encourage readers to rely upon more than one source before making a decision based on the information.

This information is not intended to constitute provide legal, financial or risk management advice and and, accordingly, it should not be relied upon for such. It should not be regarded as a comprehensive statement of the law and/or market practice in this area. In preparing this bulletin we have relied on information sourced from third parties and we make no claims as to the completeness or accuracy of the information contained herein. No liability can be attributable to Gallagher Re for any errors in the underlying information nor for any losses which arise from a recipient's reliance upon this bulletin. Recipients should not act upon information in this bulletin nor determine not to act, without first seeking specific legal and/or specialist advice. This bulletin reflects our understanding as at 10/08/21, but you will recognise that matters concerning ransomware and cyber risk liability are fast changing across the world. Gallagher Re make no warranties, express or implied, as to the accuracy, reliability or correctness of the information provided. Neither Gallagher Re nor its r officers, employees or agents or affiliates shall be responsible for any loss whatsoever arising from the recipient's reliance upon any information provided in this bulletin. Gallagher Re shall retain any and/all copyright and other forms of intellectual property or other proprietary rights subsisting anywhere in the world (together, "Intellectual Property Rights") in any and/all works; developments (including but not limited to any ideas, know-how, techniques, documentation, software and reports) and materials (including but not limited to any design, specification, instruction, software, information, data and documents) used or produced by Gallagher Re whether individually or in conjunction with others in connection with this document. Recipients do not acquire any right or license in relation to any Intellectual Property Rights owned or used by Gallagher Re by virtue of this document being provided to them.

www.gallagherre.com

Gallagher Re