A logo with a black background

Description automatically generated

Ransomware Model: Highlights and Approaches

Version 0.3

August 2024

Éireann Leverett (eleverett@concinnity-risks.com)

Erin Burns (eburns@concinnity-risks.com)



Developed by:



Funded by:

# Document Review History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Notes** | **Author** |
| 0.1 | 16th Jul 2024 | First version | Eireann Leverett (Concinnity Risks) and Erin Burns (Concinnity Risks) |
| 0.2 | 20th Aug 2024 | Full edit, reformat and restructure | Matt Donovan (Oasis LMF) |
| 0.3 | 27th Aug 2024 | Minor additions, clarifications | Eireann Leverett (Concinnity Risks) |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[Document Review History 2](#_Toc175065523)

[1.0 Introduction 4](#_Toc175065524)

[2.0 What Data was Used When Developing the Model? 4](#_Toc175065525)

[3.0 What Does This Model Cover? 4](#_Toc175065526)

[3.1 Peril and Exposure 5](#_Toc175065527)

[3.2 Supported Coverages 5](#_Toc175065528)

[4.0 Important Modelling Assumptions 5](#_Toc175065529)

[4.1 Frequency 6](#_Toc175065530)

[4.2 Number of Victims Correlates to Gross Domestic Product (GDP) 6](#_Toc175065531)

[4.3 Revenue is More Important Than Sector 6](#_Toc175065532)

[4.4 Technographic Factors 7](#_Toc175065533)

[4.5 Severity 7](#_Toc175065534)

[4.6 Negotiated Versus Fixed Price Ransoms 8](#_Toc175065535)

[4.7 Data Alteration 8](#_Toc175065536)

[4.8 Exfiltrated Data and Sector 9](#_Toc175065537)

[4.9 Digital Forensic and Incident Response Costs (DFIR) 9](#_Toc175065538)

[4.10 Regulatory fines 9](#_Toc175065539)

[4.11 Data Restoration 9](#_Toc175065540)

[4.12 Business Interruption (BI) and Contingent Business interruption (CBI) 9](#_Toc175065541)

[5.0 Conclusion 10](#_Toc175065542)

# 1.0 Introduction

This model is for ransomware economic harm, commonly known as an attrition model. It models a portfolio of companies and some of their firmographic information and estimates the economic losses of a given year of ransomware events across that portfolio. It is possible to create a catastrophe model from the data we have available, but the initial focus of this model is on portfolio attritional effects rather than losses from the single largest ransomware event. To produce a catastrophe model, we need better event definitions and community discussion.

Also, this model is more appropriate to analyse a portfolio rather than simulate variations in a single organisation's loss profile. It is designed to provide insight into the losses of a group companies in aggregation, year on year. If you want to simulate the losses of a single company, we recommend you look elsewhere for a model that is better suited to that purpose.

# 2.0 What Data was Used When Developing the Model?

This model has been developed using multiple data sets to understand both the frequency and severity of ransomware.

To understand severity:

* *RansomCoin Dataset* from Concinnity Risks[[1]](#endnote-1)
* *A survey of DFIR hourly/daily costs across service providers*

To understand frequency:

* *Sentinal Data Set* from Microlab.red
* *Data from FIRST.org*
* *IC3 Yearly reports*

Several industry and academic papers have also influenced the modelling choices:

* Cyentia IRIS Ransomware Insights[[2]](#endnote-2)
* Marsh and Mclennan Ransomware[[3]](#endnote-3)
* Sophos Ransomware Report[[4]](#endnote-4)
* Trend Micro[[5]](#endnote-5)
* Cambridge Centre for Risk Studies & Kivu[[6]](#endnote-6)

# 3.0 What Does This Model Cover?

This model estimates the economic impacts of ransomware to a specific list of companies rather than calculating the total economic impact globally or to a specific country. However, it can be used for that, providing the portfolio of companies is large enough. This model cannot calculate the impacts to a specific company although again, it could be used that way. The impacts of ransomware highlight significant variability to specific companies based on their size, sector, employees, security or incident response capabilities.

In summary, frequency is derived from the collective behaviour of ransomware threat actors, and severity is driven by the victim and how they respond to a ransomware event.

## 3.1 Peril and Exposure

This model focusses on cross border security (CBS) and specifically ransomware. The categorisation of ‘ransomware’ is difficult to define due to how much it has evolved over the last decade. ‘Ransomware’ as a cyber peril can be ambiguous, so it’s important to be explicit and clear as to how the losses are divided between insurance coverages.

This model utilises the Open Exposure Data (OED) standard for cyber to ensure accurate terminology and articulation of the various coverages that need to be understood before a “full” ransomware model can be developed and deployed.

The brackets in the following section reflect the OED Open Data Standards coverages in version 1. They can be found on github[[7]](#endnote-7), and are used to clarify the modelling by being specific about what variance in losses is reflected in different coverage types. While the initial model will only reflect a few of these coverages, we list all the coverages that we aim to reflect in future versions for discussion, and to provide a potential roadmap for development. Those in blue are in scope for version 1 of this model, those in orange are for future versions of the model.

Ransomware economic impacts can reflect:

* Ransom payments (CBS-EXT)
* Digital Forensics and Incident Response costs (CBS-INRE)
* Data Recovery costs [Encryption/Corruption/Deletion] (CBS-DIAS)
* Breach liability [Exfiltration] (CBS-LIAB)
* Breach Regulatory Fees [Exfiltration] (CBS-REG)
* Business Interruption Losses (CBS-BI)
* Contingent Business Interruption Losses (CBS-CBI)

## 3.2 Supported Coverages

The first coverage included within this ransomware model will be ‘extortion’ (OED Coverage code ‘EXT’) which calculates the expected ransom payments. The second phase of development will include *Digital Forensics and Incident Response* (DFIR) followed by *Recovery Costs*. The third phase will focus on Digital Asset Recovery costs DIAS.

Future collaboration with the market and user community will likely identify next steps and define a road map to provide further modelling, which has significant overlaps with a breach model.

## 4.0 Important Modelling Assumptions

Every model developer needs to make difficult decisions regarding assumptions and choices of what to include in their model. Models can drive markets, but they should also initiate discussions, and these discussions are critical to developing the ransomware dialogue. The assumptions made in this model are outlined below.

## 4.1 Frequency

The frequency of ransomware is highly dependent on the number of threat actors perpetrating ransomware attacks. This model was developed by observing the top 45 ransomware groups victimisation approaches. The victim numbers show *pareto* style distributions with the top threat actors making up more than 50% of victims. Therefore, it’s likely that adding substantially more threat actors will have diminishing returns. However, it is a parameter that needs to be monitored and yearly adjustments will be necessary.

Secondly, it’s important to understand that over the last decade, ransomware victimisation has risen (and fallen) by orders of magnitude. In terms of the numbers of ransoms paid, 2014 was the peak year, although the ransoms were very small. The amount of money in ransoms being paid now are substantially larger as threat actors target large companies, but the number of them is reduced compared to 2014 victimisation.

## 4.2 Number of Victims Correlates to Gross Domestic Product (GDP)

The Cybersecurity Centre of Belgium published an insightful paper describing how the number of ransomware victims per country strongly correlates to the GDP of that country[[8]](#endnote-8).

The outcomes of that paper have been considered in this model and used to scale the risk based on the resident country HQ of the insured in the portfolio. Putting it succinctly, our model assigns events to countries in a weighted manner with the highest GDP getting the most incidents. There are notable exceptions to this rule, in that China and Russia are often not victimised, and many ransomware groups have explicitly claimed not to infect systems in these countries.

## 4.3 Revenue is More Important Than Sector

NAICS was used as the industry standard for classifying victims for this analysis. The initial raw number of victims by sector differed significantly, but these differences reduced and become more appropriate once the data was normalised by the number of businesses within a sector. Following further analysis, there was little correlation between sector and numbers of victims. Essentially, more construction companies and hospitals get attacked simply because there are more of them[[9]](#footnote-1).

We found that the impact of revenue was a much stronger predictor of ransomware victimisation frequency. Therefore, this model has focussed on revenue rather than sector, but the sector is still supported in the model, and can be used in future versions of the model.

The model support revenue, sector and country variation in frequency, and severity.

## 4.4 Technographic Factors

While technographic factors can have significant impacts on the ransomware risk, they are not included in this first version of the model for three main reasons:

1. Its’ still uncertain within the insurance and security community which factors have what impact on the frequency or severity.
2. Although it’s understood that patching, email security and an incident response team will reduce the risk, the quantification and uncertainty around this reduction in risk are still inconclusive.
3. Many insurers do not capture enough of this data to sufficiently model it.[[10]](#footnote-2).

## 4.5 Severity

While the severity of the ransom is usually proportional to the revenue, the severity of the other impacts (or coverages) can be influenced by either the sector, number of employees, customers, data records, legal or regulatory liability. Therefore, when developing the severity within the model, there has been less focus on revenue (except for ransoms themselves).

A ransomware claim can be identified using the following descriptions:

* Encrypted/Corrupted/Deleted data
* Leaked data
* Distributed Denial of Service
* A mixture of the above

It’s important to understand these distinctions when describing claims. For example, a manufacturing company may care less about leaked data, as the data may have come from factories that are not considered under any regulatory liability. However, encrypted/deleted/corrupted data may impact their BI significantly. A hospital is an example where both encrypted and leaked data may cause losses, where a law firm is likely more focussed on the leaking of the data than the deletion of it (except for cases in progress). The attackers will know what will have the most impact on the companies and will change tactics (and this will reflect as shifting coverages) based on what is most likely to get the ransom paid.

A challenge when developing the model is to accurately reflect the severity around these different forms or attack and capture them in the correct coverage category.

An additional key factor in the severity of a ransomware incidents is whether the ransom was paid or not. Some presume that paying the ransom negates the other costs, but research suggests this only happens in very few cases. In fact, most of the other costs of a ransomware incident are still incurred and some research even suggests paying the ransom simply increases the cost of the incident.

If insurance policies exclude ‘extortion’, the model user can choose to accept or decline ransom payments in a rule-based manner, however, as the model will be primarily used by the re/insurance industry, the approach has been taken to focus on the behaviour of the insured rather than the businesses.

Based on the most recent report from *Marsh and McLennon*, this model includes the calculation of not paying a ransom (i.e. EXT = 0) as .75 (75% of insureds do not pay ransoms[[11]](#footnote-3)). This is based on figure 7 of the report, and although it states 77% of ransoms were not paid in 2023, a slightly more conservative approach was taken using a value between the 2022 and 2023 data.

## 4.6 Negotiated Versus Fixed Price Ransoms

Some ransomware groups or campaigns such as *Wannacry and Deadbolt* charge a fixed price. Others such as *Clop and LockBit3* negotiate on price[[12]](#footnote-4). This highlights the difficulty when assigning absolute or relative damage bins to each group in the model. Although the proportionality of this may change over time, best efforts have been made to capture the reality of the 2023 ransomware year.

## 4.7 Data Alteration

There are three main ways to alter data; *deletion, corruption,* and *encryption* and when developing a view of the economic severity, these will generally get considered under the banner of *digital assets* (OED coverage code ‘DIAS’). Data alteration can impact each sector differently, but this has not been considered in the first version of the model. This is primarily due to the lack of evidence and academic maturity to support this modelling, though we do believe it to be true.

Each sector in the model is thus agnostic and will be developed in future versions.

## 4.8 Exfiltrated Data and Sector

Like data alteration, data *exfiltration* (data theft or covert transfer of data) affects different sectors and countries economically. This is largely reflected in differences of regulation and liability (OED coverage codes ‘REG’ and ‘LIAB’ respectively).

As mentioned previously, the model is sector agnostic and the ‘severity by sector’ will need further research before being encoded into a model.

## 4.9 Digital Forensic and Incident Response Costs (INRE)

*Digital Forensic and Incident Response* costs are usually in a per hour, per diem, or per incident pricing structure. The price does not typically vary much across the different sectors, countries or revenues. Therefore, the cost variability coded within the model follows that found in the 2023 cyber incident response market. The prices in our industry surveys of the market range from a low of 200 per hour to a high of 500 per hour. The number of hours worked per incident is obviously correlated to the size of the company, but equally seems to be correlated to the threat actor (some ransomware groups are more damaging than others).

## 4.10 Regulatory fines

Regulatory fines are heavily dependent on the jurisdiction of the victim or its customers. For example, General Data Protection Regulation (US/EU) breach fines differ substantially from the breach fines issued by the Federal Trade Commision’s (US).

To model this we would need to look at the fines imposed in many different countries in the world and model them. Initially that might be the USA and GDPR, slowly expanding outward from there but for now this is out of scope in the first version of the model.

## 4.11 Data Restoration

Data restoration costs are largely unrelated to sector, revenue, country, or employees. The intention is that this sub-peril within the model will reflect the variation of global prices in 2023.

Feedback and advice are encouraged on this from the cyber insurance community.

## 4.12 Business Interruption (BI) and Contingent Business interruption (CBI)

BI and CBI are the two coverages most sensitive to all the firmographic factors. The impact of ransomware is economically very different for a hospital than for a lumber mill and this level of detail is not included in the first version of the model and will be developed in the future with collaboration from various parties.

# 5.0 Conclusion

This is a first version of the ransomware model where only the *extortion* and incident response coverages will be supported. Beta testing will be required where further discussion and feedback is encouraged to include the digital asset recovery coverages. The aim of this model is to be fit for purpose for commercial practitioners in the cyber re/insurance space and so development will continue.

As more coverages are supported, ransomware insurance can become much less capital intensive. Although there is a lot more to be considered, this simple model should still bring significant value to the market.

1. <https://docs.apwg.org/ecrimeresearch/2020/22_Averages_don_t_characterise_the_heavy_tails_of_ransoms.pdf> [↑](#endnote-ref-1)
2. <https://www.cyentia.com/ransomwares-heavy-toll/> [↑](#endnote-ref-2)
3. <https://www.marsh.com/en/services/cyber-risk/insights/ransomware-a-persistent-challenge-in-cyber-insurance-claims.html> [↑](#endnote-ref-3)
4. <https://www.sophos.com/en-us/whitepaper/cyber-insurance-and-defenses> [↑](#endnote-ref-4)
5. <https://documents.trendmicro.com/assets/white_papers/wp-what-decision-makers-need-to-know-about-ransomware-risk.pdf> [↑](#endnote-ref-5)
6. <https://www.jbs.cam.ac.uk/wp-content/uploads/2022/12/2022-risk-kivu-mitigating-ransomware-risk-report.pdf> [↑](#endnote-ref-6)
7. <https://github.com/OasisLMF/ODS_OpenExposureData/blob/master/OpenExposureData/Cyber/Docs/OED_Cyber_Data_Spec_v1.0.0.xlsx> [↑](#endnote-ref-7)
8. <https://ccb.belgium.be/sites/default/files/RansomwareResearchReport_GDP%26targeting_2024-02-01.pdf> [↑](#endnote-ref-8)
9. Please note this is ONLY an assessment of **frequency**, severity of impact does vary widely by sector. [↑](#footnote-ref-1)
10. This underscores the importance of the OED Cyber Data Standards work led by Oasis LMF team. [↑](#footnote-ref-2)
11. <https://www.marsh.com/en/services/cyber-risk/insights/ransomware-a-persistent-challenge-in-cyber-insurance-claims.html> [↑](#footnote-ref-3)
12. An academic paper on this subject can be provided on request from the author. It will be published thanks to this project, and funding from Lighthill Risk Network. [↑](#footnote-ref-4)