CyberNat: Cyber risks caused by Natural Catastrophes

Keywoong Bae

1 Introduction

Natural Catastrophes (NatCat) are inherently uncontrollable and often insurmountable, necessitating a focus on preventive measures (Zhao Zhengtang, 2011). The increasing frequency and severity of NatCat due to recent climate change underscore the imperative for preparedness strategies to mitigate associated risks. Beyond the direct physical damages caused by NatCat, there is a growing recognition of the indirect ramifications in the Cyber domain, leading to an increase in Cyber risks. While the physical destruction from NatCat results in immediate costs and damages, the Cyber risks emanating from such events are indirect in nature.

Direct costs encompass the tangible losses, damages, and suffering directly experienced by the victims of a particular incident. In contrast, indirect costs represent the broader losses and opportunity costs borne by society as a consequence of the incident (Aldasoro, Gambacorta et al 2022). Indirect costs, being more challenging to predict and quantify compared to direct costs (Faria, Vale, Facin, De Carvalho et al 2020), often involve potentialities, presenting a complex challenge for the insurance industry in addressing secondary damages arising from specific events.

This paper aims to shed light on the indirect Cyber risks stemming from natural disasters, elucidating the understanding of the interplay between the indirect costs incurred by natural disasters and their correlation with the cyber domain.

The research begins by defining various risks, including Cyber risk, Natural Catastrophes risk

(NatCat), indirect Cyber risk induced by natural disasters (referred to as CyberNat risk), and general operational risk. Subsequently, a Generalized Linear Model (GLM) regression analysis is employed to scrutinize the factors influencing Cyber and NatCat risks. The estimation of distributions for loss frequency and loss severity is crucial in defining the connection functions used in this analysis.

From the perspective of the extracted variables, the study observes how the physical destruction caused by NatCat affects the infrastructure of entities such as businesses, governments, and institutions, leading to the emergence of Cyber risks. Following this, an in-depth analysis of the Cyber risks arising from such indirect damages is conducted. Through scenario analysis, the paper aims to formulate preventive strategies for instances where NatCat lead to indirect Cyber risks.

This research contributes to a deeper understanding of the essence of indirect Cyber risks arising from NatCat and strives to provide insights into effective responses and preventive measures within the cyber domain. Ultimately, the paper enhances awareness regarding how the indirect costs stemming from the physical destruction caused by NatCat influence the cyber domain and aims to assist in formulating robust strategies for Cyber risk.

The paper is organized as follows: Section 2 delves into data and methodology, Section 3 introduces risk definitions from relevant literature, Section 4 presents statistical results, Section 5 concludes the discussion point of this paper.

2 Data and Methodology

2.1 Dataset

Although cyber risk is a crucial topic for the economy and society and is reported in the media every day, it has been the subject of very limited academic research (Eling,Wirfs 2019;

Aldasoro, Gambacorta et al 2022). This is most likely due to the absence of reliable data. In addition, many literatures of cyber risk is limited to the field of IT and information and the consideration of the number of records lost in a data breach (Eling,Wirfs 2019). Based on Cebular and Young (2010), who defined cyber risk as "operational risks to information and technology assets that have consequences affecting the confidentiality, availability or integrity of information or information systems", we linked cyber risk to operational risk.

We used SAS OpRisk Global data, which is the world's largest collection of publicly reported operational losses. There are numerous academic papers using this database (De Fontnouve-lle, DejesusRueff, Jordan & Rosengren, 2006; Hess 2011;). This database includes 37,653 observations from March 1971 to April 2021. Since it is based on operational risks, it consists of various sectors and types of risks. One of the most powerful characteristics of this database is that it only deals with losses in excess of US$100,000, so we can observe the risk based on the impactful risks.

From this dataset, we extracted three cases of risk: (i) Cyber risk, (ii) Natural catastrophes, and (iii) CyberNat, which is the collection of cases of cyber risks caused by natural catastrophes. For classifying them, we used keyword based classification. Details are on Appendix A.

Through these methods, we extracted 2,852 cyber risks, 384 NatCat risks, 13 CyberNat risks, and 34,429 operational risks from 37652 cases from SAS OpRisk database.

2.2 Loss Distribution Approach

In this paper, Loss Distribution Approach (LDA), which is the most common method for actuarial modeling (Eling,Wirfs 2019), was used and loss data were separated from the perspectives of frequency and severity. The losses L are described by:

$$L = \sum_{i=1}^{N} X_i \qquad (1)$$

where the frequency N is a discrete random variable and $X_1, \ldots, X_N$ are positive independent and identically distributed random variables.

For the loss frequency distribution, a total of six distributions were utilized. Representative discrete distributions, such as the Poisson distribution, negative binomial distribution, and geometric distribution (Panjer, 2006; Boucher, Denuit, Guillén 2008; Liu & Pitt 2017), were used to depict random and independent events. Additionally, zero-inflated distributions were applied to the aforementioned three distributions, resulting in a total of six discrete probability distributions considered as candidates for the frequency distribution estimation. Zero-inflated models are commonly used in count data analysis, such as the number of emergency room visits by a patient in one year or the number of fish caught in one day in a lake (Bilder, Loughin 2014). These models accommodate observations with frequent zero values, indicating a mixture of two distributions. The first distribution generates zeros, while the second, which may be a Poisson distribution, negative binomial distribution, or other count distribution, generates counts, some of which may be zeros (Friendly, Meyer 2015).

For the loss severity distribution, three distributions were used: Gamma, Log-normal, and Weibull (Eling 2012). These three distributions are commonly used in actuarial modeling, and through them, we aim to estimate the empirical distribution.

Based on the estimated results, we extracted significant factors using Lasso regression analysis and GLM regression analysis. Lasso regression analysis was used to exclude irrelevant predictor variables. Lasso regression is a type of regularized linear regression that adds constraints to linear regression coefficients, preventing the model from overfitting.

Utilizing the extracted variables from lasso regression, a GLM regression analysis was conducted to analyze significant factors. The GLM extends the traditional linear regression model by incorporating various distributions for the dependent variable, including normal distributions. It expands the linear relationship between the mean of the dependent variable and the linear relationship with independent variables. In GLM, the probability distribution of the dependent variable is extended to an Exponential Family distribution.

$$g(y) = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \cdots + \beta_n x_n \qquad (2)$$

where function g is a link function, which connects the linear predictor and the mean of the dependent variable, depends on the distribution estimated earlier. GLM regression analysis was separately performed for loss frequency and loss severity, aiming to identify factors influencing frequency and severity.

2.3 Scenario analysis

Scenario analysis refers to "plausible descriptions of how the future may develop based on a coherent and internally consistent set of assumptions" (Nakicenovic and Swart, 2020). It is not merely an analytical tool but rather a methodology employed for strategic planning and decision-making across diverse fields. The scenario development process encompasses five key stages: scenario definition, scenario construction, scenario analysis, scenario assessment, and risk management (Mahmoud et al., 2009). Five essential standard must be met for a scenario to be considered effective: pertinence, coherence, likelihood, importance, and transparency (Durance and Godet, 2010).

3 Risk Definitions from related literatures

In SAS OpRisk Global data, we divided it into four categories: cyber risk events, Natural Catastrophes (NatCat), operational risk, and cyber risks caused by natural catastrophes (CyberNat). In this section, we summarized the definitions and characteristics of cyber risk and NatCat.

3.1 Cyber risk

As cloud systems and artificial intelligence continue to advance, the exposure to and awareness of cyber risks are steadily increasing. Cyber risk refers to the potential risks within an organization, such as financial losses, damage to reputation, and other consequences resulting from the failure of IT systems (Aldasoro, Gambacorta et al 2022). Cebula et al. (2014) operationally defined cyber risk as risks to information and technology assets that impact the confidentiality, availability, or integrity of information or information systems. This definition justifies the diverse and evolving nature of cyber risk due to various and continually emerging causes.

Representative examples of cyber risks include identity theft, business interruption, reputational damage, theft of customer records, and costs associated with data recovery and litigation (European Union Agency for Network and Information Security, 2018; National Association of Insurance Commissioners, 2019;). With the increasing complexity of technology and the integration of infrastructures across sectors such as energy, telecommunications, and banking, the impact and influence of cyber risks are on the rise. The growing interdependency among sectors results in cascading effects of cyber risks, transcending national and sectoral boundaries, ultimately leading to catastrophic consequences for critical infrastructure (Pescaroli and Alexander, 2016; Zio, 2016;).

3.2 Natural Catastrophes Risk

Natural Catastrophes (NatCat) represent risks arising from natural disasters, encompassing physical damages caused by events such as hurricanes, floods, wildfires, and tsunamis. NatCat poses a significant potential threat to entire regions or countries, giving rise to human casualties, extensive losses, and widespread impacts (Donatella Porrini, 2016;).

NatCat is difficult to manage in the insurance field because it is difficult to predict its occurrence and the losses when it occurs are very large. In Zhao Zhengtang 2010, compared to traditional standards, NatCat has the following three characteristics: Fat tails, Tail dependence, and Microcorrelations.

Firstly, NatCat exhibits a Fat tail, deviating from the thin-tailed distribution commonly observed in most loss distributions. This implies a higher likelihood of encountering extreme values (infrequent but significantly impactful cases). Unlike the typical scenario, NatCat predominantly follows a fat-tailed distribution, indicating a higher probability of discovering extreme values (Yuri M. Ermoliev, Tatiana Ermolieva, et al., 2000). NatCat risks can be considered as extreme events, with the probability of such events declining slowly relative to their severity. Consequently, NatCat risk manifests with fat tails, challenging conventional methods of analysis.

Secondly, NatCat demonstrates Tail dependence, signifying a high dependence between two random variables concentrating in extreme high values (Zhao Zhengtang, 2010). This implies a high probability of simultaneous occurrence of severe losses due to the high interdependence of natural disasters. For instance, a strong earthquake may lead to landslides or avalanches, and even wildfires or hurricanes can result in both flooding and wind damage. Failing to account for such tail dependence poses a risk for insurance companies, potentially underestimating exposure and facing significant losses.

Lastly, NatCat exhibits micro-correlations, indicating correlations between variables that may be at or below the detection threshold, even with substantial data. These correlations may not be readily apparent, and while individual variables may seem insignificant, the presence of correlations can pose significant risks. Therefore, NatCat risks, with these distinctive features, demand considerable attention in the insurance sector, presenting various challenges that need to be addressed.

4 Statistical Results

4.1 Empirical Estimation and goodness of fit

Based on the 2,852 cyber risk cases and 383 natural catastrophes cases extracted from SAS OpRisk database, we estimated the distributions on loss frequency and loss severity. In loss frequency, we used three discrete distributions, poisson, negative-binomial distribution, and geometric distribution. We also tested the zero-inflated versions of three discrete distributions above.

In loss frequency of cyber risk, the negative-binomial distribution provides better fit than other ones, and zero-inflated distributions do not show a better fit than the negative-binomial distribution. In loss frequency of natural catastrophes, as a same with cyber risk, the negative-binomial distribution also provided best fit on loss frequency.

Table 1 Goodness-of-fit analysis - frequency

Model	Category	Chi-square p-value	Chi-square-test	AIC	BIC
Panel A: Cyber risk (N=2852)					
Poisson	Basic	0	6494.578	2208.341	2211.886
Poisson	Zero-inflated	1.405694e-168	810.1257	2137.739	2144.829
Negative-binomial	Basic	**0.0042164**	**24.05419**	**1685.127**	**1692.217**
Negative-binomial	Zero-inflated	4.375224e-158	756.7123	2125.177	2135.812
Geometric	Basic	8.320835e-14	83.97248	1749.131	1752.676
Geometric	Zero-inflated	8.3158e-14	83.97381	1749.131	1752.676
Panel B: Natural Catastrophes (N=384)					
Poisson	Basic	5.22708e-115	532.1159	1383.137	1387.015

Poisson	Zero-inflated	0	Inf	14032.11	14039.86
Negative-binomial	Basic	**0.6678481**	**0.8073891**	**957.9549**	**965.7104**
Negative-binomial	Zero-inflated	0	Inf	154681.4	154681.4
Geometric	Basic	5.553635e-14	64.79328	1030.885	1034.762
Geometric	Zero-inflated	5.553634e-14	64.79328	1030.885	1034.762

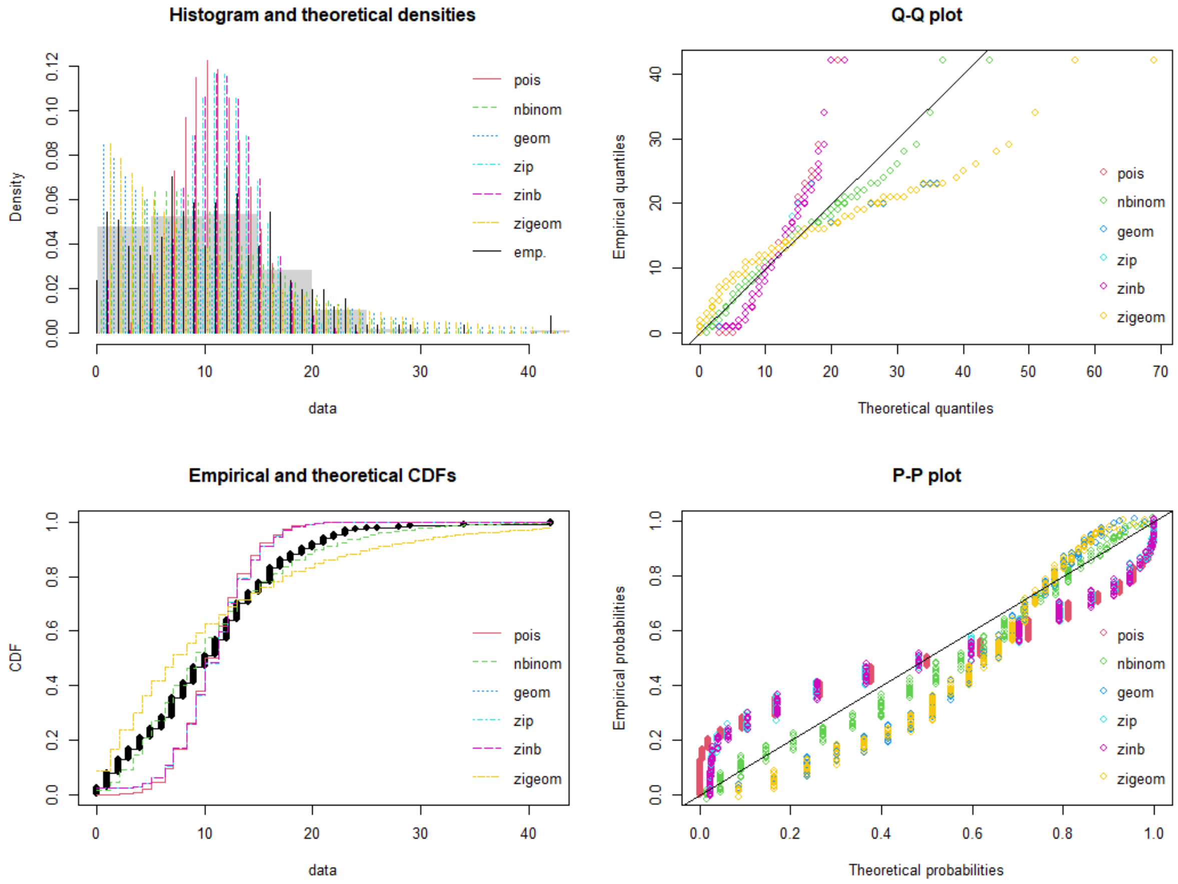

Figure 1 Estimated distribution of Cyber risk’s loss frequency

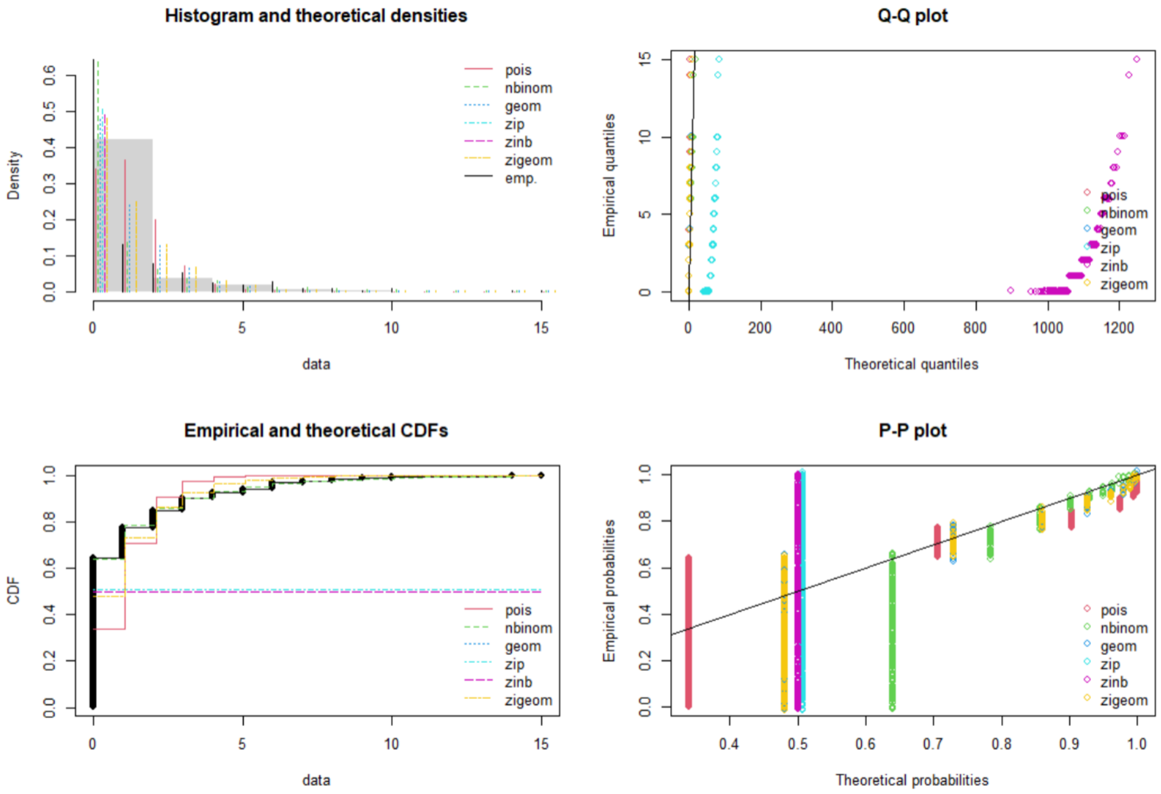

Figure 2 Estimated distribution of NatCat risk's loss frequency

In loss severity, we used three continuous distributions, Gamma, Log-normal, and Weibull distribution.

Table 2 Goodness-of-fit analysis - severity

Model	Kolomogorov-Smirnov-test	Anderson-Darling-test	AIC
Panel A: Cyber risk (N=2852)			
Gamma	0.2107	Inf	293529.2
Log-normal	**0.04022**	**87.6649**	**266499.0**
Weibull	0.10331	789.298	276119.0
Panel B: Natural Catastrophes (N=384)			
Gamma	0.1732938	20.71557	4065.805
Log-normal	**0.026864**	**0.262326**	**3865.712**

Weibull	0.07131	4.75675734	3933.814

In conclusion, it was confirmed that both Cyber risk and NatCat risk exhibit a negative binomial distribution for loss frequency and a log-normal distribution for loss severity. The estimated parameters for each distribution are summarized in Table 3.

Table 3 Conclusion of goodness-of-fit and parameters of estimated distributions

Estimated parameters		
Cyber risk		
Loss frequency	Negative-binomial	$size = 2.536, \mu = 10.66$
Loss severity	Log-normal	$\mu = 1.664, \sigma = 2.106$
Natural Catastrophes		
Loss frequency	Negative-binomial	$size = 0.283, \mu = 1.081$
Loss severity	Log-normal	$\mu = 2.883, \sigma = 2.012$

4.2 Factor analysis with GLM

In this section, a Generalized Linear Model (GLM) analysis was conducted utilizing information derived from the estimated distribution. The objective is to extract and validate factors influencing each respective risk (Cyber risk, NatCat risk).

Prior to identifying key factors, variable selection was carried out through Lasso regression. The findings indicated that, in the case of Cyber risk, subcategorical risks such as disasters, thefts, manufacturing, and employee-related components, along with the European region within the regional category, and the manufacturing sector within the sector category, were deemed irrelevant. For NatCat risk, it was determined that the systems subcategorical risk and the manufacturing sector were unrelated.

$$
\begin{aligned}
g\left(y_{Cyber\ loss}\right) = \ & \beta_0 \\
& + \sum_{i=1}^{7} \beta_i X_i^{Dummy-Subcategories} \\
& + \beta_8 X^{legal\ liability} + \beta_9 X^{assets} \\
& + \sum_{i=1}^{6} \beta_{9+i} X^{Dummy-Sector} \\
& + \sum_{i=1}^{1} \beta_{15\_i} X^{Dummy-Region}
\end{aligned}
\tag{3}
$$

$$
\begin{aligned}
g\left(y_{NatCat\ loss}\right) & \\
= \ & \beta_0 + \beta_1 X^{legal\ liability} \\
& + \sum_{i=1}^{4} \beta_{1+i} X^{Dummy-Sector} \\
& + \sum_{i=1}^{1} \beta_{5\_i} X^{Dummy-Region}
\end{aligned}
\tag{4}
$$

Utilizing the selected variables, significant factors were identified through GLM analysis. Table 4 summarizes the key factors influencing Cyber risk and NatCat risk.

Table 4 The drivers of Cyber risk and NatCat risk.

Dependent variable: Log(cost)		
	Cyber risk	NatCat risk
Panel A: Numerical variables		
Legal liability	0.0045 ***	0.01067 .

Assets	0.00000162 *	-
Panel B: Subcategories		
Improper Business or Market Practices	1.1016 ***	-
Suitability, Disclosure & Fiduciary	1.029 ***	-
Systems	1.218 ***	-
Disasters and Other Events	1.263 **	-
Product Flaws	1.478 **	-
System Security	0.289 *	-
Transaction Capture, Execution & Maintenance	0.422 *	-
Panel C: Sector		
Financial Services	-1.501 ***	-0.989 .
Information	-0.749 ***	-0.9245 .
Utilities	-1.008 **	-
Mining	-1.217 *	-
Other Services (except Public administration)	-3.507 .	-
Real Estate, Rental and Leasing	-1.589 .	-
Retail Trade	-	-3.109 .
Agriculture, Forestry, Fishing and Hunting	-	-2.165 *
Panel D: Region of domicile		
North America	-0.299 **	0.656 .

5 CyberNat Scenarios

5.1 CyberNats in SAS Oprisk Database

CyberNat risk is the case of Cyber risks caused by Natural Catastrophes. In SAS OpRisk databases, there are 13 CyberNat cases. In Table 5, we summarized cases of CyberNat based on the selected variables from GLM analysis.

Table 5 Cases of CyberNat risk

No	Natural Disaster	Loss ($M)	Legal Liability ($M)	Assets ($M)	Sub-categorical Risk	Sector	Region
1	Storms	6.93	0.0	10848.20	Disasters	Information	Asia
2	Floods	3.83	0.0	10080.10	Disasters	Information	Africa
3	Floods	5.07	0.0	28741.00	Disasters	Information	Europe
4	Floods	2.73	0.0	110058.30	Disasters	Information	Asia
5	Floods	49.83	0.0	33179.50	Disasters	Information	Other
6	Earthquake	1293.38	0.0	202686.80	Disasters	Information	Asia
7	Solar outburst	200.00	0.0	59550.00	Disasters	Information	North America
8	Winter storms	6.26	0.0	18762.00	Disasters	Information	Asia
9	Typhoon	6.19	0.0	2518.20	Disasters	Information	Asia
10	Floods	29.00	0.0	2641.70	Disasters	Information	Asia
11	Floods	9.49	0.0	17765.90	Disasters	Information	Asia
12	Floods	3.32	0.0	7511.82	Disasters	Information	Asia
13	Hurricane	4.80	4.8	75361.30	Systems	Utilities	Europe

5.2 CyberNat Scenarios

Risk can be analyzed by distinguishing between frequency and severity. In the context of Natural Catastrophes Risk, cases with both high frequency and high severity are rare. Therefore, high-frequency disasters with high severity significantly impact Cyber Risk. A prominent example of a high-frequency disaster influencing Cyber Risk is flooding. Flooding occurred 132 times over approximately 600 months, making it the second most frequent disaster according to Appendix A, following storms. Such cases represent high frequency and low severity, with risk retention and loss control strategies being exemplary risk management approaches. Employing control techniques focused on loss control, individuals or entities practicing risk retention based on loss control techniques calculate and accumulate appropriate funds regularly to cover cyber risks arising from flooding.

Next, remarkable cases of high severity disasters influencing Cyber Risk include earthquakes and cases resulting from Solar Outbursts. While these occurrences may not happen frequently, when they do occur, they cause significant damage. In such cases, a risk transfer strategy, such as introducing financial techniques like insurance, is necessary. This involves managing risk through the adoption of financial techniques, specifically insurance, to transfer the risk associated with high-severity disasters.

6 Discussion

In this study, we have undertaken an exploration of the inherent indirect cyber risks stemming from natural catastrophes and have presented effective preventive measures within the cyber domain. The novelty of this topic lies in its unprecedented nature, considering the current significance of researching secondary damages in the cyber domain resulting from natural disasters.

However, throughout the research process, three noteworthy points for discussion have come to light. Firstly, there was a notable prevalence of redundant cases within the dataset. Notably, instances 2 through 5 in Appendix B, while distinct, shared commonalities such as all being flood-related and possessing highly similar descriptive content. Numerous other cases exhibited duplications, necessitating the formulation of strategies to address this issue.

Secondly, a notable limitation surfaced during the factor analysis stage, indicating that the model lacked robustness. The correlation coefficients varied depending on the choice of variables for factor analysis. While this affords the advantage of a multidimensional perspective on relationships between diverse variables, it also introduces the drawback of generating non-robust results contingent on the selected variables.

Lastly, an oversight emerged regarding the temporal characteristics of risk. While natural catastrophe risks are minimally influenced by temporal factors, cyber risks arising from the advancement of IT services are significantly temporally contingent. Cyber risks are presently more sensitive than in the past, and the future is expected to be even more sensitive. Unfortunately, the methodology employed for factor analysis in this paper failed to consider such temporal nuances.

While temporal constraints limited an in-depth exploration in this study, future research building upon this topic should address these discussion points for enhancement, thereby contributing to a more meaningful and comprehensive investigation.

References

Zhengtang, Z. (2011). Natural catastrophe risk, insurance and economic development. *Energy Procedia*, *5*, 2340-2345.

Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2022). The drivers of cyber risk. *Journal of Financial Stability*, *60*, 100989.

Faria, B. C., Vale, J. W. S. P. D., Facin, A. L. F., & De Carvalho, M. M. (2020). Main challenges in the identification and measurement of indirect costs in projects: a multiple case study.

Gestão & Produção, *27*, e4913.

Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk events?. *European Journal of Operational Research*, *272*(3), 1109-1119.

Cebula, J. J., & Young, L. R. (2010). A taxonomy of operational cyber security risks. *Software Engineering Institute, Carnegie Mellon University*.

De Fontnouvelle, P., Dejesus-Rueff, V., Jordan, J. S., & Rosengren, E. S. (2006). Capital and risk: New evidence on implications of large operational losses.

Journal of Money, Credit and Banking, 1819-1846.

Hess, M., Sczyrba, A., Egan, R., Kim, T. W., Chokhawala, H., Schroth, G., ... & Rubin, E. M. (2011). Metagenomic discovery of biomass-degrading genes and genomes from cow rumen.

Science, *331*(6016), 463-467.

Panjer, H. H. (2006). *Operational risk: modeling analytics* (Vol. 620). John Wiley & Sons.

Boucher, J. P., Denuit, M., & Guillén, M. (2008). Models of insurance claim counts with time dependence based on generalization of Poisson and negative binomial distributions.

Variance, *2*(1), 135-162.

Huo, D., Hu, H., Rhie, S. K., Gamazon, E. R., Cherniack, A. D., Liu, J., ... & Olopade, O. I. (2017). Comparison of breast cancer molecular features and survival by African and European ancestry in The Cancer Genome Atlas.

JAMA oncology, *3*(12), 1654-1662.

Bilder, C. R., & Loughin, T. M. (2014).

Analysis of categorical data with R. CRC Press.

Friendly, M., & Meyer, D. (2015).

Discrete data analysis with R: visualization and modeling techniques for categorical and count data (Vol. 120). CRC Press.

Eling, M. (2012). Fitting insurance claims to skewed distributions: Are the skew-normal and skew-student good models?.

Insurance: Mathematics and Economics, *51*(2), 239-248.

Nakicenovic, N., Alcamo, J., Davis, G., Vries, B. D., Fenhann, J., Gaffin, S., ... & Zhou, D. (2000). Special report on emissions scenarios.

Tabor, C., Murali, R., Mahmoud, M., & El-Sayed, M. A. (2009). On the use of plasmonic nanoparticle pairs as a plasmon ruler: the dependence of the near-field dipole plasmon coupling on nanoparticle size and shape.

The Journal of Physical Chemistry A, *113*(10), 1946-1953.

Durance, P., & Godet, M. (2010). Scenario building: Uses and abuses.

Technological forecasting and social change, *77*(9), 1488-1492.

Goto, Y., Panea, C., Nakato, G., Cebula, A., Lee, C., Diez, M. G., ... & Ivanov, I. I. (2014). Segmented filamentous bacteria antigens presented by intestinal dendritic cells drive mucosal Th17 cell differentiation.

Immunity, *40*(4), 594-607.

Remac, M. (2017). The European Union Agency for Network and Information Security (ENISA)-Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA).

McDonald Hulen, M., Hodgson, B., & Jorgensen, D. (2019). Department of Insurance.

California Regulatory Law Reporter, *25*(1), 18.

Pescaroli, G., & Alexander, D. (2016). Critical infrastructure, panarchies and the vulnerability paths of cascading disasters.

Natural Hazards, *82*, 175-192.

Zio, E. (2016). Challenges in the vulnerability and risk analysis of critical infrastructures.

Reliability Engineering & System Safety, *152*, 137-150.

Porrini, D. (2016). Risk classification in natural catastrophe insurance: The case of Italy.

International Journal of Financial Research, *7*(1), 39-49.

Ermoliev, Y. M., Ermolieva, T. Y., MacDonald, G. J., Norkin, V. I., & Amendola, A. (2000). A system approach to management of catastrophic risks.

European Journal of Operational Research, *122*(2), 452-460.

Appendix A. Method of Data Classification

Table 6 Keywords of Natural Disasters

Keyword	Count
Avalanche	4
Blizzard	5
Cyclone	21
Drought	3
Earthquake	71
Flood	132
Hail	16
Hurricane	95
Ice	37
Landslide	8
Snow	37
Storm	197
Tornado	12
Tsunami	33
Typhoon	8
Wind	71

Appendix B. CyberNat cases in details

No	Natural Disaster	Loss ($M)	Legal Liability ($M)	Assets ($M)	Sub-categorical Risk	Sector	Region
1	Storms	6.93	0.0	10848.20	Disasters	Information	Asia

In August 2010, Multinet Pakistan Pvt Ltd, a Pakistani telecommunications company and subsidiary of Axiata Group Bhd, reported **that it lost an estimated $6.93M (600M PKR) due to flooding**. Heavy monsoon rains led to severe flooding of Pakistan's Indus River basin in July and August 2010. The floods killed at least 1,600 people and left millions homeless. The country's infrastructure, including the landline and cellular telecommunications networks, was heavily damaged by the floods. Landline telecommunications companies reported damaged switches, route cable networks, aerial optics, fiber optics, and buildings. Cellular telecommunications companies reported collapsed boundary walls and towers, as well as Business Support Systems (BTS) and DC Power Systems that accumulated water during the storms. The Ministry of Information Technology and Telecommunication (MoITT) conducted a preliminary report to evaluate the losses in the telecommunications sector. The report estimated that Pakistan's telecommunications companies lost $26.57M (2.3B PKR) due to the flooding. The preliminary estimates did not include some repair and damage costs, and the losses were expected to rise after the flood waters receded. The telecommunications companies were increasing efforts to restore service in affected regions. The MoITT would conduct another assessment to ascertain the final damages to the telecommunications infrastructure. The affected telecommunications companies included the state-owned Special Communication Organization, National Telecom, Pakistan Telecommunication Co Ltd (PTCL), Multinet Pakistan, Telenor Pakistan, Pakistan Mobile Communications Ltd (Mobilink), China Mobile Pakistan (CMPak), Warid, and Pakistan Telecom Mobile Ltd (Ufone). Multinet Pakistan reported that a 350-kilometer fiber optic cable was damaged in Dera Ismail Khan. **The damages amounted to $6.93M.**

No	Natural Disaster	Loss ($M)	Legal Liability ($M)	Assets ($M)	Sub-categorical Risk	Sector	Region
2	Floods	3.83	0.0	10080.10	Disasters	Information	Africa

In August 2010, Pakistan Mobile Communications Ltd, a Pakistani telecommunications company and subsidiary of Orascom Telecom Holdings, **reported that it lost an estimated $3.83M (331.5M PKR) due to flooding**. Heavy monsoon rains led to severe flooding of Pakistan's Indus River basin in July and August 2010. The floods killed at least 1,600 people and left millions homeless. The country's infrastructure, including the landline and cellular telecommunications networks, was heavily damaged by the floods. Landline telecommunications companies reported damaged switches, route cable networks, aerial optics, fiber optics, and buildings. Cellular telecommunications companies reported collapsed boundary walls and towers, as well as Business Support Systems and DC Power Systems that accumulated water during the storms. The Ministry of Information Technology and Telecommunication (MoITT) conducted a preliminary report to evaluate the losses in the telecommunications sector. The report estimated that Pakistan's telecommunications companies lost $26.57M (2.3B PKR) due to the flooding. The preliminary estimates did not include some repair and damage costs, and the losses were expected to rise after the flood waters receded. The telecommunications companies were increasing efforts to restore service in affected regions. The MoITT would conduct another assessment to ascertain the final damages to the telecommunications infrastructure. The affected telecommunications companies included the state-owned Special Communication Organization, National Telecom, Pakistan Telecommunication Co Ltd (PTCL), Multinet Pakistan, Telenor Pakistan, Pakistan Mobile Communications Ltd (Mobilink), China Mobile Pakistan (CMPak), Warid, and Pakistan Telecom Mobile Ltd (Ufone). Mobilink reported that 65 of its Business Support Systems sustained damage **worth an estimated $3.83M**.

No	Natural Disaster	Loss ($M)	Legal Liability ($M)	Assets ($M)	Sub-categorical Risk	Sector	Region
3	Floods	5.07	0.0	28741.00	Disasters	Information	Europe

In August 2010, Telenor Pakistan, a Pakistani telecommunications company and subsidiary of Telenor ASA, reported **that it lost an estimated $5.07M (438.6M PKR) due to flooding**. Heavy monsoon rains led to severe flooding of Pakistan's Indus River basin in July and August 2010. The floods killed at least 1,600 people and left millions homeless. The country's infrastructure, including the landline and cellular telecommunications networks, was heavily damaged by the floods. Landline telecommunications companies reported damaged switches, route cable networks, aerial optics, fiber optics, and buildings. Cellular telecommunications companies reported collapsed boundary walls and towers, as well as Business Support Systems and DC Power Systems that accumulated water during the storms. The Ministry of Information Technology and Telecommunication (MoITT) conducted a preliminary report to evaluate the losses in the telecommunications sector. The report estimated that Pakistan's telecommunications companies lost $26.57M (2.3B PKR) due to the flooding. The preliminary estimates did not include some repair and damage costs, and the losses were expected to rise after the flood waters receded. The telecommunications companies were increasing efforts to restore service in affected regions.

The MoITT would conduct another assessment to ascertain the final damages to the telecommunications infrastructure. The affected telecommunications companies included the state-owned Special Communication Organization, National Telecom, Pakistan Telecommunication Co Ltd (PTCL), Multinet Pakistan, Telenor Pakistan, Pakistan Mobile Communications Ltd (Mobilink), China Mobile Pakistan (CMPak), Warid, and Pakistan Telecom Mobile Ltd (Ufone). Telenor Pakistan reported that 86 of its Business Support Systems sustained damage **worth an estimated $5.07M.**

No	Natural Disaster	Loss ($M)	Legal Liability ($M)	Assets ($M)	Sub-categorical Risk	Sector	Region
4	Floods	2.73	0.0	110058.30	Disasters	Information	Asia

In August 2010, China Mobile Pakistan, a Pakistani telecommunications company and subsidiary of China Mobile Ltd, reported **that it lost an estimated $2.73M (236.3M PKR) due to flooding**. Heavy monsoon rains led to severe flooding of Pakistan's Indus River basin in July and August 2010. The floods killed at least 1,600 people and left millions homeless. The country's infrastructure, including the landline and cellular telecommunications networks, was heavily damaged by the floods. Landline telecommunications companies reported damaged switches, route cable networks, aerial optics, fiber optics, and buildings. Cellular telecommunications companies reported collapsed boundary walls and towers, as well as Business Support Systems and DC Power Systems that accumulated water during the storms. The Ministry of Information Technology and Telecommunication (MoITT) conducted a preliminary report to evaluate the losses in the telecommunications sector. The report estimated that Pakistan's telecommunications companies lost $26.57M (2.3B PKR) due to the flooding. The preliminary estimates did not include some repair and damage costs, and the losses were expected to rise after the flood waters receded. The telecommunications companies were increasing efforts to restore service in affected regions. The MoITT would conduct another assessment to ascertain the final damages to the telecommunications infrastructure. The affected telecommunications companies included the state-owned Special Communication Organization, National Telecom, Pakistan Telecommunication Co Ltd (PTCL), Multinet Pakistan, Telenor Pakistan, Pakistan Mobile Communications Ltd (Mobilink), China Mobile Pakistan (CMPak), Warid, and Pakistan Telecom Mobile Ltd (Ufone). CMPak, also known by its brand name ZONG, reported that 96 of its Business Support Systems sustained damage **worth an estimated $2.73M.**

No	Natural Disaster	Loss ($M)	Legal Liability ($M)	Assets ($M)	Sub-categorical Risk	Sector	Region
5	Floods	49.83	0.0	33179.50	Disasters	Information	Other

In January 2011, Telstra Corp Ltd, an Australian telecommunications company, reported that it would lose an **estimated $49.83M (50M AUD) due to flood damage.** A series of devastating floods struck Queensland, Australia in December 2010 to January 2011. The Queensland floods inflicted major damage to infrastructure in the densely populated areas of Brisbane and other cities. At least 15 people died in the Brisbane and Toowoomba floods, with many more still missing. The recovery efforts in Brisbane were expected to cost at least $4.98M (5B AUD). More than .02M Telstra customers were without telecommunications service at the height of the flooding. Once the floods began to recede, the inaccessibility of many sites continued to hinder the recovery process. In mid-January 2011, Telstra stated that 262 telephony stations were still inaccessible to Telstra employees. The company's goal was to establish short-term service to customers in a matter of days. The company also aimed to establish temporary networks by mid-February and to finish rebuilding its infrastructure by late April. While Telstra did not want to estimate its total repair costs, analysts put the cost at approximately $49.83M.

No	Natural Disaster	Loss ($M)	Legal Liability ($M)	Assets ($M)	Sub-categorical Risk	Sector	Region
6	Earthquake	1293.38	0.0	202686.80	Disasters	Information	Asia

In April 2011, Nippon Telegraph and Telephone Corp, a Japanese telecommunications company, reported that it lost an estimated $1.29B (106B JPY) due to a natural disaster. On March 11, 2011, **a magnitude-9.0 earthquake triggered tsunami waves along the northeast coast of Japan**. The earthquake and tsunami caused extensive damage to Nippon Telegraph and Telephone Corp's (NTT Corp) infrastructure. Forty-one buildings were flooded, almost .07M electric poles were disabled, and the company's cellular phone base stations and optical cables were damaged. NTT Docomo, NTT Corp's mobile subsidiary, sustained an estimated $73.21M (6B JPY) in damages, and the firm expected to lose another $122.02M (10B JPY) over the next year due to the catastrophic event. NTT East, another NTT Corp subsidiary, lost an estimated $244.03M (20B JPY) and would lose another estimated $244.03M in the next fiscal year. NTT Corp also reported that it would need $610.08M (50B JPY) in capital investments to rebuild facilities and restore services. The company expected to resume operations in its exchange office buildings and mobile base stations by the end of April 2011. NTT Corp would also try to restore services as soon as possible to customers who lived in heavily affected areas. The company planned to develop networks and procedures to help it recover more quickly from natural disasters in the future.

No	Natural Disaster	Loss ($M)	Legal Liability ($M)	Assets ($M)	Sub-categorical Risk	Sector	Region
7	Solar outburst	200.00	0.0	59550.00	Disasters	Information	North America

In January 1998, American Telephone & Telegraph Co, a US communications and networking company, reported that **it had realized a loss of $200M** when one of its television relay satellites, Telstar 401, s**uffered a massive power failure due to a violent solar outburst.** The satellite was rendered completely inoperable. Scientists and investigators concluded that the anomaly might have been triggered by an isolated but intense magnetic substorm, which in turn was caused by a coronal mass ejection, a magnetically charged cloud of hydrogen and helium that was spewed from the Sun's outer atmosphere on January 6. The cloud sped toward the Earth at a speed of one million mph, mushrooming to a width of more than 30 million miles by the time it smashed into the earth's protective magnetic field on January 10, delivering an electrical charge of 1 million amps. Robert Hoffman, a NASA scientist, reported that Telstar 401 had been orbiting in an affected area of the magnetosphere, which is the Earth's magnetic field. The $200M spacecraft, which had been built by Lockheed Martin Astro Space and was launched in late 1993, was designed to operate for 12 years. Of the total loss, $145M was to be covered by insurance.

No	Natural Disaster	Loss ($M)	Legal Liability ($M)	Assets ($M)	Sub-categorical Risk	Sector	Region
8	Winter storms	6.26	0.0	18762.00	Disasters	Information	Asia

In February 2008, China Unicom Ltd, a Chinese wireless communications company, reported that **it lost $6.26M (45M CNY) due to damages to telephone lines from severe winter storms**. The winter snowstorms, which hit China in January 2008, caused damage to crops, intrastate and local businesses. China Unicom announced that the network damage to much of its property during the storm caused outages to portions of its wireless network. The damages to the networks would take weeks of repair work before services could be fully restored.

No	Natural Disaster	Loss ($M)	Legal Liability ($M)	Assets ($M)	Sub-categorical Risk	Sector	Region
9	Typhoon	6.19	0.0	2518.20	Disasters	Information	Asia

In October 2009, Globe Telecom Inc, a Philippines telecommunications company, reported that **it lost an estimated $6.19M (288.2M PHP) due to typhoon damage.** The typhoons Ondoy and Pepeng brought storms and severe flooding to the Philippines in late September and early October 2009. Globe Telecom (Globe) stated that Ondoy had impacted about 200 of its service sites in south Luzon and greater Manila. The company also encountered difficulties in restoring services due to flooding at a major service site in Pasig. As of mid-October 2009, the company had resumed 99 percent of its wireless services and 92 percent of its broadband services. The company stated that it would spend approximately $3.18M (148M PHP) on repairs to its mobile and broadband networks. The company would also spend approximately $2.89M (134.5M PHP) on rebates, equipment, and other offers to broadband subscribers and mobile customers who lived in high-flood areas. In addition, the company would provide assistance to Globe distributors in Rizal and Marikina and would provide temporary phone and internet stations in North Luzon and metro Manila at an estimated cost of $.12M (5.7M PHP). The company planned to relocate damaged facilities to higher ground in order to avoid future flood damage.

No	Natural Disaster	Loss ($M)	Legal Liability ($M)	Assets ($M)	Sub-categorical Risk	Sector	Region
10	Floods	29.00	0.0	2641.70	Disasters	Information	Asia

In August 2010, Pakistan Telecommunication Co Ltd, a Pakistani telecommunication company, reported that it lost an estimated **$29M (2.5B PKR) due to flooding.** Heavy monsoon rains led to severe flooding of Pakistan's Indus River basin in August 2010. The floods killed 1,600 people and left 2M people homeless. Pakistan Telecommunication Co Ltd (PTCL) reported that the floods had damaged .15M connections and more than 150 exchanges in the Peshawar, Dera Ismail Khan and Federally Administered Tribal Areas (FATA) regions. In Peshawar, a total of 101 exchanges were damaged and 38 of these were not yet restored as of mid-August 2010. The buildings that housed 12 exchanges collapsed entirely, and two exchanges remained underwater. In Dera Ismail Khan, 45 exchanges were still undergoing repairs, and the networks of nine exchanges would need to be replaced. Repair work was hindered by the destruction of roads and bridges and a lack of fuel. In the FATA region, unrest made repair work impossible without security forces. PTCL stated that it had lost approximately

$29M due to the floods, and that the company and its employees had donated another $.62M (53.5M PKR) to victims of the floods.

No	Natural Disaster	Loss ($M)	Legal Liability ($M)	Assets ($M)	Sub-categorical Risk	Sector	Region
11	Floods	9.49	0.0	17765.90	Disasters	Information	Asia

In September 2010, Bharat Sanchar Nigam Ltd, an Indian telecommunications company, reported that it lost an estimated **$9.49M (450M INR) due to flooding.** On August 6, 2010, heavy rains caused flooding and mudslides in the city of Leh in Jammu and Kashmir, killing at least 125 people. The disaster caused heavy damage to the telecommunications infrastructure of Bharat Sanchar Nigam Ltd (BSNL), including the destruction of company offices. As of mid-September 2010, BSNL had restored service to 45,000 mobile phones and 11,000 landlines. BSNL expected to spend $9.49M rebuilding and expanding its telecommunications services in Leh, including $4.85M (230M INR) for new buildings, $2.74M (130M INR) for improved mobile and transmission networks, and $1.9M (90M INR) for expanded broadband and landline service. The Minister of State for Communications and IT also ordered BSNL to install satellite towers in remote parts of the country in order to better deal with any future disasters.

No	Natural Disaster	Loss ($M)	Legal Liability ($M)	Assets ($M)	Sub-categorical Risk	Sector	Region
12	Floods	3.32	0.0	7511.82	Disasters	Information	Asia

In November 2010, TOT Corp PCL, a Thai telecommunications company, reported that it lost an estimated **$3.32M (100M THB) due to flood damage.** In October and November 2010, heavy rains caused rivers to flood across Thailand. The floods affected an estimated 7M people and caused more than 200 deaths. The floods caused damage to the country's telecommunications infrastructure, including base stations, fiber-optic cables and telephone booths. In November 2010, TOT stated that its total property damage due to the floods would reach a maximum of $3.32M. The company's initial assessment showed damages of at least $.66M (20M THB) in the northeast and approximately $1M (30M THB) in the south. The company stated that it could not report the exact amount of damages until floodwaters receded. TOT stated that it would use its emergency reserves to pay for the repairs. As of November 2010, TOT reported that conditions in Hat Yai province had returned to normal and that it would now focus its repair efforts on the Chumphon and Surat Thani provinces.

No	Natural Disaster	Loss ($M)	Legal Liability ($M)	Assets ($M)	Sub-categorical Risk	Sector	Region
13	Hurricane	4.80	4.8	75361.30	Systems	Utilities	Europe

In September 2013, National Grid PLC, a UK electric and gas utility, **reported that it would pay $4.8M (3M GBP)** to hourly employees for improperly compensating them for work performed. The work by hourly employees was performed between November 1, 2012 and March 31, 2013. Approximately 6,500 New York workers were hired by National Grid to help repair utility lines after Hurricane Sandy hit the east coast of the United States. **Hurricane Sandy hit the state of Florida on October 25, 2012, before slowly moving up the east coast of the US**. Although the storm was downgraded to a post-tropical cyclone before it slammed into the Northeastern US on October 29, it still produced hurricane-force winds and a storm surge of over 14 feet. The storm affected at least 24 states, but New York and New Jersey were hit especially hard. The state investigation found over .03M incidents in which employees working for National Grid failed to be fully paid or were provided inaccurate wage statements. National Grid blamed the errors on computer glitches in its system due to a conversion to new computer systems within the company that changed the way it performed time keeping and payroll functions. The state found that employees were left unable to pay rent, repair their homes or pay for basic necessities when their paychecks failed to arrive. As part of its agreement with the state, National Grid would provide an account summarizing each employees unpaid wages and the reason for those payment problems. The company stated that it had already fixed the errors that caused the glitch. The company agreed to pay up to $4.8M to over 6,500 New York workers who were working during the time period in question. National Grid faced several lawsuits in the state of New York over the unpaid wages. Any settlements reached in those lawsuits would be credited to the obligations it agreed to with the state.