Time dynamics of cyber risk

Martin Eling[1], Rustam Ibragimov [2], and Dingchen Ning[1]

[1]Institute of Insurance Economics, University of St Gallen, Girtannerstrasse 6, 9010 St. Gallen, Switzerland

[2]Imperial College Business School, Tanaka Building, South Kensington Campus, London SW7 2AZ, UK

June 2022

ABSTRACT

This is the first paper to jointly analyze the three main cyber loss datasets (Advisen, SAS OpRisk and PRC), yielding the most comprehensive cyber loss data yet considered in the literature. We first study the problem of report delay bias by applying a two-stage model specific to the unique data where more than one point in the timeline of the cyber event is observed. The results show a faster rate of increase for cyber risk frequency compared with the original data. Based on these results, we then focus on the dynamics of cyber risk frequency and severity, where we separately study the properties of full distribution and tail of loss severity. We show the existence of change points over time in each dimension and the extremely heavy-tailed nature of cyber risk. Our results are important for cyber risk management and understanding the insurability of cyber risk.

JEL classification: C15, G22, G32.

I. Introduction

In 2007, an American department store chain, TJX, was hacked and nearly 94 million credit cards information have been exposed (ABC 2007). This was the largest recorded data breach incident at the time, but just several years later, more and more data breach incidents exceeding this magnitude occur. Among them, Yahoo's incident in 2013 was the largest, involving nearly 3 billion user accounts (Reuters 2017). Not only the extreme cyber events are becoming more and more frequent, the overall frequency and severity are also changing quickly. For example, FBI (2020) reports 300% increase in reported cybercrimes during the COVID-19 period. The recent report of McAfee (2020) estimates the cost of global cybercrime at $1 trillion, a more than 50% increase from the 2018 estimate ($600 billion). Also, recent academic research (e.g., Jamilov, Rey & Tahoun 2021) emphasizes that cyber risks have increased significantly globally.

Although all these examples clearly illustrate the huge and increasing importance for businesses and societies, the existing knowledge on the empirical properties of cyber risk is relatively limited. The theoretical work on cyber risk has begun as early as the beginning of this century (e.g., Gordon & Loeb 2002), but due to the limit of data, the empirical work is at least one decade lagging behind with Maillart & Sornette (2010) among the earliest works to use data breach loss information[1]. Still today most empirical works rely heavily on the data breach dataset provided by the Privacy Rights Clearinghouse (e.g., Kamiya, Kang, Kim, Milidonis & Stulz 2021; Farkas, Lopez & Thomas 2021; and Bessy-Roland, Boumezoued & Hillairet 2021), which does not provide information on the financial loss of incidents and thus limits the use for risk management. This study intends to utilize three different datasets to overcome the drawbacks of each database and enable us to get more comprehensive information on cyber risk than what the literature has shown so far, including the number of events, financial losses, accounts affected and number of records breached.

Our work relates to the literature that study statistical properties of cyber risk[2]. Various studies focus on modeling cyber risk, showing the heavy-tailed property of cyber risk severity such as Wheatley, Maillart & Sornette (2016), Eling & Wirfs (2019) and Farkas et al. (2021) with different frameworks. For the comprehensive review of the work on cyber risk, we refer to Eling, McShane & Nguyen (2021) and Woods & Böhme (2021). Considering the existing empirical work, there is little consensus about the dynamics of cyber risk. With data period from 2000 to 2008, Maillart & Sornette (2010) show there is a strong non-stationary growth culminating in July 2006 followed by a stable period afterwards. Edwards, Hofmeyr & Forrest (2016) find no evidence of increasing trend for size and frequency of data breaches for data from 2005 to 2015. However, Romanosky (2016) indicates an increasing trend for the number of cyber events in the same period. Wheatley, Hofmann & Sornette (2021) also observe an increasing trend for both frequency and

[1] We acknowledge that information security has been an evergreen IT topic before this century, but few of them are based on the economic (and risk management) perspective. Therefore, we refer Gordon & Loeb (2002) as one of the earliest papers in this area. We also acknowledge earlier empirical works considering stock prices, but not loss information, especially Campbell, Gordon, Loeb & Zhou (2003). See also Anderson & Moore (2006) for an earlier review on the economics of information security.

[2] We summarize the works on cyber risk in the Appendix.

severity in the similar time period, but only specific to hack type events. More recently, Jung (2021) shows a break point in 2014 for loss severity data with stable trend before 2014 and rapid growth afterwards. Overall, the results appear to be rather inconsistent and the difference might be largely driven by different datasets and different methodologies. This motivates us to reconsider the empirical properties over a long time period with the combination of three main cyber databases which have never been jointly analyzed. We also note that none of the above studies tries to incorporate the bias problems, which are inherent to all these datasets.

This paper aims at studying the time dynamics of cyber risk by identifying potential change points in time after controlling the bias in data. One issue of data bias that has been studied in both general statistics and actuarial science is report delay, which relates to the structural delay between the event date and observation date. Using the unique information in our data, we are able to correct this bias by developing a two-stage statistical model extending the work of Stoner & Economou (2020). The results show that after accounting for report delay, the trend of frequency is increasing much faster than what we see in raw data.

Building on the results of bias correction, we study the time dynamics of cyber risk frequency, especially at understanding whether there have been fundamental shifts over the years. More specifically, we apply recent statistical methods (e.g., Baranowski, Chen & Fryzlewicz 2019) to detect the unknown number of change points in the time series data of cyber risk.

We also contribute to the analysis of cyber risk severity. Traditionally, the analysis of loss severity focuses on the first moment of the distribution, but this leaves out certain useful information. Following the most recent advances in statistics (Dubey & Müller 2020), we consider the full distribution of cyber risk, which can provide a more comprehensive understanding. The results show that in recent years the distribution of cyber risk shifts to the left, indicating lower loss severity. This might be driven by the increasing number of small losses with the high frequency of cyber risk and strict regulation of information transparency.

Given the extreme nature of cyber risks and manifold discussions around their insurability (e.g., Biener, Eling & Wirfs 2015), the tail of the loss severity distribution requires a deeper look. We apply several non-parametric methods to measure tail risk such as Hill's estimator and OLS log-log rank-size estimator. We show that cyber risk is extremely heavy-tailed with infinite mean and variance in most of the cases. In addition, we exploit the method proposed by de Haan & Zhou (2020) for the trend analysis of tail risk.

The overall contribution of our paper is thus to provide a comprehensive analysis of the time dynamics of cyber risk in different dimensions by analyzing the most comprehensive datasets over a long time period. Utilizing the most recent and advanced statistical methods, we address limitations of existing empirical studies and enhance the knowledge on the dynamics of cyber risk frequency and severity. The results can provide more clarity on the empirical properties of cyber risk and shed light on the ambiguious results in the literature.

Another contribution is to be the first to provide empirical evidence on the problem of cyber data bias and develop a statistical model to control it. In many related studies (Maillart & Sornette

2010, Wheatley et al. 2016, Farkas et al. 2021), the authors have questioned the reliability of data and discussed the potential issues that this can bring about. However, due to the limitation of data, few studies have proposed useful methods for the evaluation of data bias. Together with the more detailed incident-level data, we start by addressing one type of the issues (report delay) and find more convincing evidence on the increasing speed of cyber risk over the years.

The reminder of this paper proceeds as follows. Section II describes the data and methods used for the main analysis of cyber risk. Section III presents the empirical results for the time dynamics of risk frequency and severity. Section IV concludes.

II. Data and methods

A. Data

We have three sources of data for the analysis on cyber risk. The first and major data source is from Advisen[3]. Their database collects information from multiple publicly available sources such as government websites (Securities & Exchange Commission, Federal Trade Commission, Federal Communications Commission, State data breach notification websites, etc.) and other sources including keyword-based alerts, official court and litigation sources and other internet information. The magnitude of the records in the database is over 150,000, while more than 80% of the cases are from U.S. and the rest are from 177 different countries. Since the database creates different records for different kinds of losses arising from one incident such as direct damage and legal costs, we aggregate the original data and result in 111,253 incidents for further analysis. Although the magnitude of cyber events in this database is large, the information on financial loss and accounts affected is more scare. After cleaning the data and using the sample after 2001[4], we have 5,714 records for financial loss and 88,386 records for accounts affected.

The second source we use is SAS OpRisk Global data[5], which is the world's largest database on publicly reported operational losses. This database contains more than 35,000 operational events in excess of US$ 100,000 for different countries and industries. There is no classification for cyber risk and thus we cannot extract cyber events directly from the database. Therefore, we use an approximate method following Eling & Wirfs (2019) which exploits text mining to extract cyber-related events. This results in 2,659 observations for our analysis.

The last source of data is from the non-profit organization Privacy Rights Clearinghouse[6] (PRC), which is the one frequently used in the current literature. It collects information about breach events from government agencies and verifiable news sources starting from 2005. The dataset contains 6,822 records up to the end of 2019. The major difference from the previous two data sources is that this database focuses only on data breach events and does not provide financial loss amount

[3] `https://www.advisenltd.com/data/cyber-loss-data/`.

[4] We restrict the sample to time period from 2001 since cyber risk only becomes a serious issue in the 21st century and the data in the last century are very sparse. This also applies to other data sources

[5] `https://www.sas.com/content/dam/SAS/en_us/doc/productbrief/sas-oprisk-global-data-101187.pdf`.

[6] `https://privacyrights.org/data-breaches`.

for each case. Therefore, we will use this database for the analysis of risk frequency and number of records breached.

Table I summarizes the basic statistics of our datasets over time. Although we present the results in the same period for each database, it is important to note that PRC data range only from 2005 to 2019, which explains the lower number of events in the first and last period. In addition, the number of events in the last period for all datasets is not significantly higher than the previous periods, which is very likely related to report delay bias that we will study in more detail.

We see an increasing trend of loss severity (and the standard deviation of it) for all databases, except for certain anomalies[7], again documenting the increasing relevance of cyber risk events. Also, the difference between mean and median value is substantial, indicating the highly skewed distribution of cyber risk.

B. Methodology

B.1. Bias correction

Reliable data are crucial for the analysis of cyber risk, but the current databases are not comprehensive (such as PRC data that only focus on data breach) and/or potentially biased (such as the database of Advisen and other commercial databases). Hence, empirical studies without bias correction may only lead to partial or even incorrect conclusions about cyber risk.

We aim to apply recent methods from the field of statistics to identify and correct the potential bias in the current data before conducting further statistical analysis. One main problem is report delay, which is the case where the total observable count will only be available after a period of time since the actual date that an event occurs. Therefore, before the total count becomes available, we can only observe incomplete data. This can be detrimental for the analysis of time dynamics and lead to misinterpretation of the actual number of events. For the case of cyber risk, this problem is common since many events are noticed and made public after a long time. Also, the delay may occur when the database cannot update the data in time due to various reasons such as labor shortages.

To model report delay, we follow the work of Stoner & Economou (2020) and extend their framework to include two stages that are unique in the Advisen dataset. The Advisen dataset is the main focus in this part since it has the detailed timeline of each incident, from the event date to the date of first notice, until the date of entry into database. This unique feature allows us to capture two delay mechanisms.[8].

The reason we choose the method from Stoner & Economou (2020) is that it provides higher

[7]The frequency in 2001-2005 is significantly lower while the severity is higher than other periods. This is likely driven by data bias issues such as less cyber events are made public in the early years and thus mostly extreme events are collected. In addition, the particularly high total loss amount in this period for SAS data is related to several extreme events including the case of money laundering for Bank of China in 2005 which resulted in more than $10 Billion loss.

[8]SAS OpRisk database only has the date of occurrence and the date of entry, while PRC database contains only the date of occurrence. Therefore, they are not very suitable for report delay analysis.

Table I Summary statistics of three databases

	Loss amount-SAS	Loss amount-Advisen	Accounts affected-Advisen	Records breached-PRC
Whole sample				
Number	2659	5714	88386	6822
Total loss	101216.22	90758.94	80141.28	10387.40
Mean loss	38.07	15.88	0.91	1.52
Median loss	1.64	0.13	0.00	0.00
Standard deviation	368.13	224.36	42.09	41.96
2001-2005				
Number	311	496	1185	117
Total loss	41415.24	7404.79	2809.94	55.10
Mean loss	133.17	14.93	2.37	0.47
Median loss	3.40	0.48	0.00	0.02
Standard deviation	1027.93	96.88	47.47	3.71
2006-2010				
Number	837	1776	11330	1774
Total loss	18370.36	19028.43	3651.94	741.99
Mean loss	21.95	10.71	0.32	0.42
Median loss	1.30	0.04	0.00	0.00
Standard deviation	116.07	126.11	6.66	5.41
2011-2015				
Number	643	2105	39290	2884
Total loss	18647.70	31028.54	21048.62	1543.45
Mean loss	29.00	14.74	0.54	0.54
Median loss	1.46	0.14	0.00	0.00
Standard deviation	108.45	181.03	26.67	7.39
2016-2021				
Number	868	1337	36581	2047
Total loss	22782.92	33297.19	52630.78	8046.85
Mean loss	26.25	24.90	1.44	3.93
Median loss	1.83	0.22	0.00	0.00
Standard deviation	110.79	372.71	58.57	75.89

Note:
The monetary loss value is presented in $Million (adjusted to 2021 dollar value), and the accounts or records breached are presented in Million.

accuracy by jointly modeling the delay mechanism and the total count number. Traditionally, the task of correcting the delayed reporting has been separated from the task of forecasting but this ignores the joint uncertainty in the incidence of total count and the presence of delay. For example, a low number of cyber cases in month t may be resulted from a temporal decreasing trend or a low reported number in this period, or both. Therefore, it is important to jointly model these two mechanisms.

Three models are considered in this paper, a generalized linear model (GLM) (Salmon, Schumacher, Stark & Höhle 2015), a generalized Dirichlet-multinomial hazard model (GDM hazard) and a generalized Dirichlet-multinomial survivor model (GDM survivor) (Stoner & Economou 2020). In the empirical part, we first compare the three models for their in-sample performance and then apply the best model for bias correction.

Let y_t be the total observable count at time t and after some delay unit (months in our case) a proportion of y_t, $z_{t,d}$, has been reported in this period, where d is the number of months delayed. This means that $\sum_{d=1}^{D} z_{t,d}$ gets close to y_t as the total number of months D increases.

The model based on GLM framework starts with a negative-binomial (NB) distribution for y_t:

$$y_t \sim NB(\lambda_t, \theta); \quad log(p_{t,d}) = g(t,d),$$

where λ_t is the expected rate of occurrences and θ allows for overdispersion, the multinomial probability $p_{t,d}$, which is the expected proportion of y_t that will be reported at delay d, is modeled via a log-link, and $g(t,d)$ represents a combination of covariate effects. Therefore, the marginal distribution for z_i is also NB:

$$z_{t,d} \sim NB(\mu_{t,d} = p_{t,d}\lambda_t, \theta); \quad log(\mu_{t,d}) = \iota + \alpha_t + \eta_t + \psi_d + \beta_{t,d},$$

where α_t is a penalized cubic spline to capture nonseasonal variation, η_t is a penalized cyclic cubic spline to capture within-year temporal effect, $\beta_{t,d}$ is intended to allow for temporal changes of delay mechanism, and ι and ψ_d are fixed effects.

Different from GLM framework, the models based on GDM are designed to account for heterogeneity in the delay mechanism and appropriately separate variability and uncertainty in the delay mechanism from the model of count number. The GDM hazard model is defined by:

$$\begin{aligned} y_t \sim NB(\lambda_t, \theta); \quad & log(\lambda_t) = \iota + \alpha_t + \eta_t; \\ z_t \mid y_t \sim GDM(\boldsymbol{\nu_t}, \boldsymbol{\phi}, y_t); \quad & log(\frac{\nu_{t,d}}{1-\nu_{t,d}}) = \psi_d + \beta_{t,d}, \end{aligned}$$

where $\nu_{t,d}$ is the expected proportion of counts which will be reported at delay d out of those which are yet-to-be-reported and $\boldsymbol{\phi}$ controls for dispersion. In this model, the delay mechanism is modeled through the difference of temporal structure in the proportion of reported cases across delay levels.

The GDM survivor model applies a different way of modeling delay mechanism:

$$y_t \sim NB(\lambda_t, \theta); \quad log(\lambda_t) = \iota + \alpha_t + \eta_t;$$
$$z_t \mid y_t \sim GDM(\boldsymbol{\nu_t}, \boldsymbol{\phi}, y_t); \quad probit(S_{t,d} = \psi_d + \beta_t);$$
$$\nu_{t,d} = \frac{S_{t,d} - S_{t,d-1}}{1 - S_{t,d-1}},$$

where $S_{t,d}$ is the expected value of the cumulative proportion of cases at time t for delay level d. Compared with the hazard model that considers a structure for each delay level, this method models the delay structure for each time point, which allows for any number of delay levels.

The models above provide flexible ways of modeling delay structures for cyber risk, but how to connect two delay stages in our cyber risk data remains a problem. Given that the data we have are at the second stage as defined above, we could back trace the original trend with available data.

In the second stage, assume that for time of first notice t, the number of total cases is a_t but is not fully available. Suppose after D months all the cases will be included in the database, but for now we only have data of D' months. Therefore, after applying the methods defined above, we can estimate the number of total cases as

$$\hat{a_t} = \sum_{1}^{D'} a_{t,d} + \sum_{D'+1}^{D} \hat{a_{t,d}},$$

where $a_{t,d}$ is the number of cases reported in delay time d, while $\hat{a_{t,d}}$ is the estimated number of cases in delay time d.

Additionally, the correction ratio q_t is defined as the estimate of actual total number divided by available number at time t:

$$q_t = \hat{a_t} / \sum_{1}^{D'} a_{t,d}.$$

This correction ratio can be further applied to the first stage. When considering the delay structure between accident date and first notice date, the number of cases reported $b_{t,d}$ is biased due to the delay in the second stage. Therefore, we can adjust this bias with the correction ratio: $\tilde{b_{t,d}} = b_{t,d} * q_{t+d}$. After the adjustment, we apply the models above to the database we have to account for first-stage bias, which provides us the corrected results of cyber risk.

B.2. Time dynamics of loss frequency

We study loss frequency and in this context focus on the estimation of change points over the period since it is of interest to understand whether cyber risk has undergone certain fundamental changes. There is extensive literature on change points detection methods (Truong, Oudre & Vayatis 2020), which can be categorized based on their cost functions, search methods and constraints. The literature mostly focuses on the problem under the assumption of piecewise-constant parameters. However, cyber loss frequency is not likely to follow this assumption due to the increasing

trend.

Therefore, we consider one newly proposed generic approach of detecting an unknown number of features occurring at unknown locations, narrowest-over-threshold detection (Baranowski et al. 2019). This method shows low computational complexity, ease of implementation and accuracy in the detection of the feature locations.

In this method, consider the model

$$Y_t = f_t + \sigma_t \epsilon_t, \quad t = 1, ...T,$$

where f_t is the signal, σ_t is the noise's standard deviation at time t, and ϵ_t follows standard normal distribution. We further assume that (f_t, σ_t) can be divided into $q+1$ segments with q unknown unique change points $0 = \tau_0 < \tau_1 < ... < \tau_q < \tau_{q+1} = T$. The structure of (f_t, σ_t) is modeled parametrically by a local real-valued d-dimensional parameter vector Θ_j, where d is known and typically small.

In the first step, we randomly draw subsamples such as $(Y_{s+1}, ..., Y_e)'$, where (s, e) is drawn uniformly from the set of pairs of indices in $\{0, ..., T-1\} \times \{1, ...T\}$. The generalized likelihood ratio (GLR) statistic for all potential single change points within the subsample is

$$\mathcal{R}^b_{(s,e]} = 2log[\frac{sup_{\Theta^1,\Theta^2}\{l(Y_{s+1}, ..., Y_b; \Theta^1) l(Y_{b+1}, ..., Y_e; \Theta^2)\}}{sup_\Theta l(Y_{s+1}, ...Y_e; \Theta)}],$$

where $l(Y_{s+1}, ...Y_e; \Theta)$ is the likelihood of Θ given $(Y_{s+1}, ..., Y_e)'$. Based on this statistic, we pick the maximum $\mathcal{R}_{(s,e]}(Y) = max_{b \in \{s+d, ...e-d\}} \mathcal{R}^b_{(s,e]}$.

In the next step, all $\mathcal{R}_{(s_m, e_m]}(Y)$ for $m = 1, ...M$ is tested against a given threshold and among the significant results, the one corresponding to the interval $(s_{m^*}, e_{m^*}]$ with smallest length will be chosen. This step can be repeated recursively to find all the possible change points. For more technical details, we refer to Baranowski et al. (2019).

B.3. Time dynamics of loss severity

Traditionally, the analysis of loss amount in the time dimension is reduced to the analysis of univariate time series such as average loss severity. Although this is a simple and efficient way of understanding the dynamics of loss, we are leaving out too much information in this process. Therefore, in this paper we adopt the recently developed method in statistics to analyze the change point in a sequence of distributions.

Dubey & Müller (2020) considers a sequence of independent random objects Y_t taking values in a metric space (Ω, d) rather than in $\mathbb{R}$ as in traditional methods (Niu, Hao & Zhang 2016). As in most practical situations, the differences of distributions are mostly in location or in scale. Therefore, this method aims to detect differences in means and variances which are in Fréchet type and provides a generalization of the notion of location and scale to metric spaces.

The test statistic for the change point can be written as:

$$T_n(b) = \frac{b(1-b)}{\hat{\sigma}^2}\{(\hat{V}_{[0,b]} - \hat{V_{[b,1]}})^2 + (\hat{V_{[0,b]}}^C - \hat{V_{[0,b]}} + \hat{V_{[b,1]}}^C - \hat{V}_{[b,1]})^2\},$$

where b is the possible value of the change point, $\hat{\sigma}$ is the asymptotic variance of the empirical Fréchet variance, $\hat{V_{[i,j]}}$ is the estimated Fréchet variance and lastly $\hat{V_{[i,j]}}^C$ is the "contaminated" version of Fréchet variance obtained by plugging in the Fréchet mean from the complementary data segment.

Based on this test statistic, Dubey & Müller (2020) further provides inference method for the identification of change point in a sequence of distributions. We refer to their paper for more technical details.

B.4. Time dynamics of tail risk

Tail risk is an important part of the analysis for cyber risk, especially in the sense that high tail risk, or heavy-tailedness has many unfavorable properties such as inducing nondiversification trap [9] (Ibragimov, Jaffee & Walden 2009). The analysis of loss distribution in the previous part does not pay special attention to the dynamics of tail risk, thus it is worthwhile to study the nature of cyber tail risk separately.

For the estimation of tail risk, we consider two basic non-parametric methods which are widely used in the literature. The first one is the Hill's estimator as follows (Hill 1975):

$$\zeta(k) = \{\frac{1}{k}\sum_{j=1}^{k} ln(x(n-j+1)) - ln(x(n-k))\}^{-1},$$

where $x(i)$ is the ith-order statistic such that $x(i) \geq x(i-1)$ for $i = 2, ...n$.

The second method is OLS log-log rank-size regression. We use the revised version proposed by Gabaix & Ibragimov (2011) which is consistent in small samples:

$$log(Rank - 1/2) = a - \zeta log(Size).$$

To further analyze the trend or potential change points in extreme value index, we rely on the recent work of Ibragimov & Müller (2016). The empirical strategy is to partition the sample into two periods, the period before a possible break point, i, and the period after the point, j. Then we divide each period into q groups chronologically, and compute the Behrens-Fisher statistic:

$$BF = \frac{\hat{\xi_1} - \hat{\xi_2}}{\sqrt{\frac{(s_1)^2}{q_1} + \frac{(s_2)^2}{q_2}}},$$

where $\hat{\xi_i} = q_i^{-1}\sum_{j=1}^{q_1}\xi_{i,j}$, $(s_i)^2 = (q_i - 1)^{-1}\sum_{j=1}^{q_i}(\xi_{i,j} - \hat{\xi_i})^2$, and $\xi_{i,j}$ is the tail estimator.

[9] When risk distributions have heavy left tails and insurance providers have limited liability, insurance providers may choose not to offer insurance for catastrophic risks and not to participate in reinsurance markets, even though there is a large enough market capacity.

With the BF statistic, we can compare it with the critical value of the Student-t distribution with $min(q_1, q_2) - 1$ degrees of freedom.

III. Empirical results

A. *Report delay*

To understand the problem of report delay, we first briefly compare our three datasets. To ensure the comparability of different datasets, we restrict the time period to start from 2005. [10]

Various sources and reports (e.g., Allianz 2021, Accenture 2021) suggest that cyber risk is increasing quickly over the years, but as shown in Figure 1[11], the increasing trend is not as obvious as we would expect. For example, the data from SAS show a steady trend, while the other two indicate an increasing trend during the early stage and then a steady trend in recent years. However, the sudden drop of cases in 2019 for PRC and slightly decreasing trend after 2018 for Advisen indicate that the problem of report delay may be one of the reasons behind this.

To look into the problem of report delay more deeply, we make use of the date of creation in Advisen to show how the trend evolves over the years in Figure 2. We plot the evolution of cyber risk based on four creation dates (every four years from 2009 to 2021), which provides a clear comparison of different points in time and shows that at each point there is a clear decreasing trend which undoubtedly relates to delayed report.

In general, the process of collecting data related to cyber risk can be divided into two stages. The first stage is from the accident date to the date of first notice. This period can be short for some types of events, such as cyber extortion or malfunction of devices, where the victims would notice almost immediately. But for other types including data breaches, the firms may take as long as months or years to find out that their data have been compromised. In general, the mean days of delay is 182 and the median is 33 days in our data.

The second stage starts with the date of first notice and ends with the creation date in the database of concern. The time delay in this stage is mainly related to the efficiency of the database of concern, in some cases the staff can update the data immediately but more likely there will be a moderate amount of delay in this stage, constrained by the investment of this database. In the Advisen data, the delay in this stage is much more severe than the first stage, with mean and median delayed days of 836 and 538. The major reason for this delay is that although the Advisen database begins to collect data in 2007, the majority of their events are created in recent years, especially during 2016-2018.

[10] There are some problems affecting the reliability of comparison. First, there is no exact accident date in SAS data, so certain biases may exist when comparing with other datasets. For the PRC data, because of the compulsory disclosure of data breach, the difference between the time when the event was made public and accident date should not be large. Second, another point which may affect the comparison is that cyber events in PRC are mostly about data breaches while the other two include all kinds of cyber risk.

[11] The abnormal and periodic peaks in Advisen data are related to the inaccuracy of accident date. For an event with only known accident year, the database assigns the first day of the year as its estimate date.

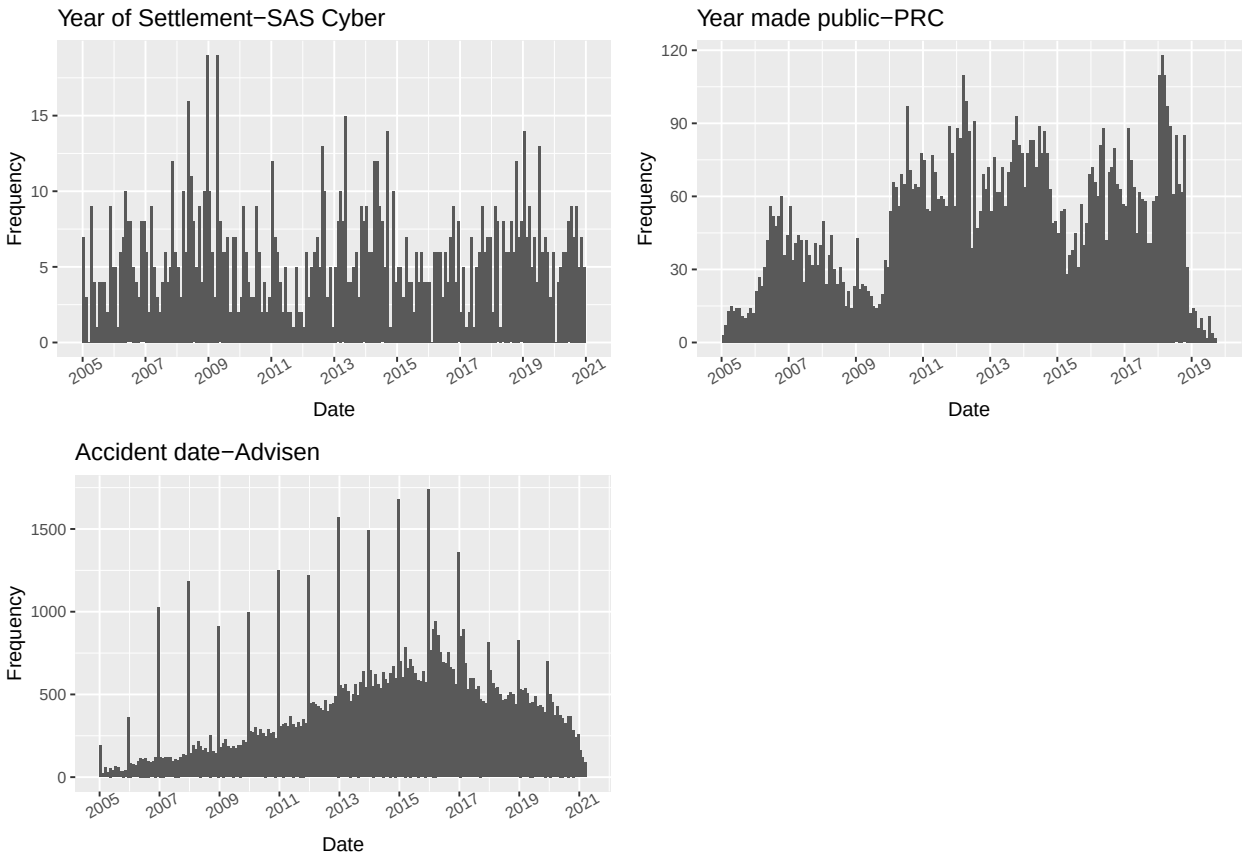

Figure 1. Different datasets of cyber risk

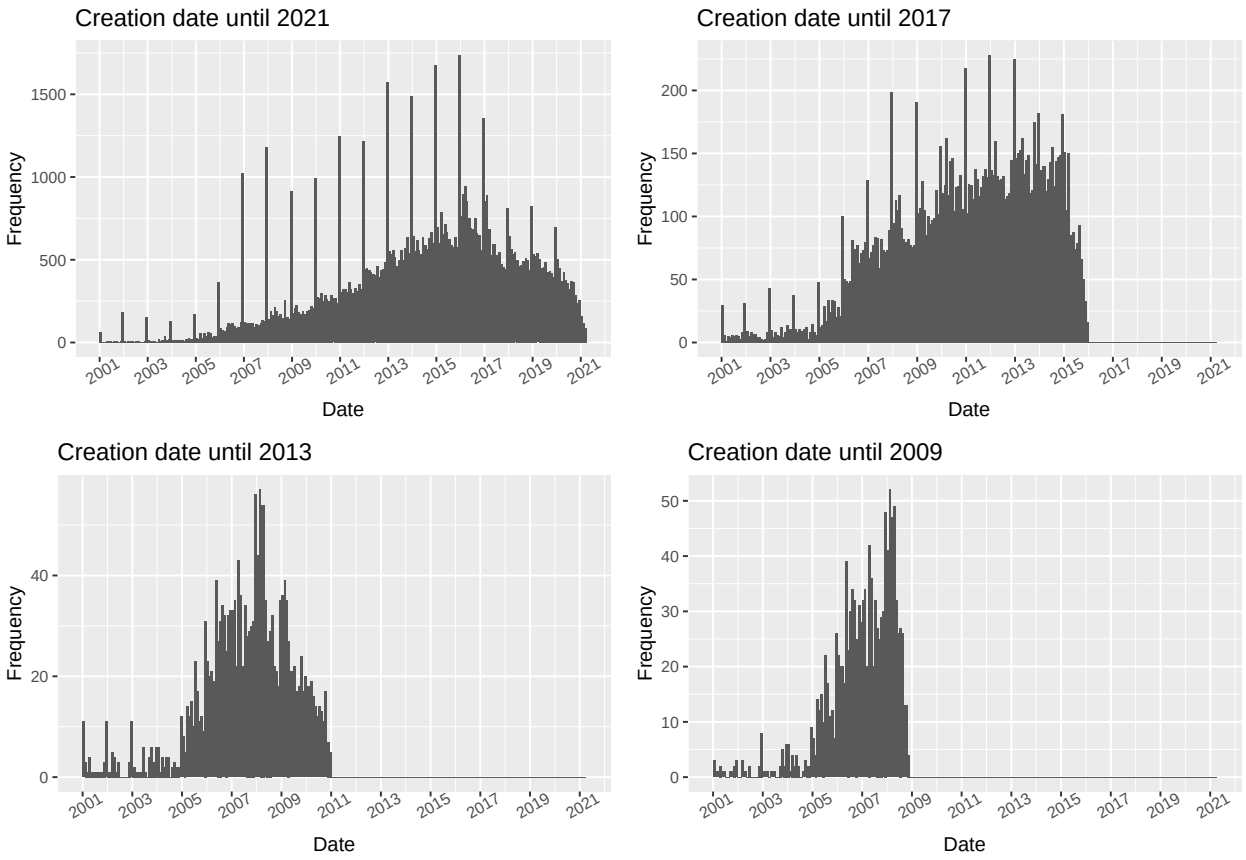

Figure 2. Different dates in Advisen

A.1. In-sample analysis

As shown in Figure 2, the data of Advisen contain multiple abnormal peaks due to inaccurate information. Therefore, to understand the true trend of cyber risk, it is necessary to deal with such abnormal data points. Traditionally, the literature tackle this issue by estimating the overall trend and replace the abnormal points with estimated results (Wang, Gu, Li, Yu, Kim, Wang, Gao & Wang 2021). However, for our data, the problem is more related to the misallocation of cyber cases, which means that we cannot just replace the high number with a lower and smoother one. To repair this anomaly, we assume the date of cyber events without accurate time follows normal distribution and then replace the original date with a more accurate one. Based on this method, we can smooth the time trend of cyber risk in our dataset. In the following analysis, we will present results with both the original and adjusted data.

For the modeling of delay structure, we have three models available: GLM, GDM hazard and GDM survivor. Therefore, it is useful to first test whether these models perform well for in-sample forecast. Since Advisen began to collect data on cyber risk from 2007, we need to exclude all cases occurred before 2007 to avoid inherent bias in the database. Therefore, we have 163 months from October 2007 to April 2021, and naturally the longest possible delay period for training is 163 months. But in this case, we would have no data for in-sample forecast, hence it is necessary to select a period when we assume all cyber cases are counted.

As an example, we can compare the cumulative proportion of cases reported for different maximum delay periods in Figure 3 (the delay between accident date and first notice date). Although there is an increasing trend in each graph due to more missing values in recent time, we can still find the differences across different maximum delay periods. There is a trade-off between sample size and accuracy for the selection of maximum delay period. For our case, we choose the period of 60 months since it includes at least 90% of all observable cases and also provides a sample of 104 months for in-sample analysis.

Given the maximum delay period of 60 months and available sample of 104 months, we choose the 92nd month (so that we can forecast the following one year) as the hypothetical present time, which means we only have observations up to this date. Then we censor the data accordingly, apply the models to this incomplete sample and compare their results with actual number. Figure 4 shows the results of median estimated number for original and adjusted data, with 95% posterior predictive interval. Among three models, GDM hazard has the most accurate confidence interval while GLM performs worst. Figure 5 provides the sample estimates of $Cov[z_{t,d}, z'_{t,d}]$ by density plots of the logarithm of the mean squared error (right) between replicated and observed covariances. This further confirms that GDM hazard is the least biased and GDM survivor comes second for both datasets. Therefore, for the out-of-sample analysis, we will focus on the GDM hazard framework.

A.2. Out-of-sample bias correction

To correct the bias related to report delay, we apply the two-stage method with GDM hazard to the whole sample period. As mentioned above, the present date is the 163rd month, which is

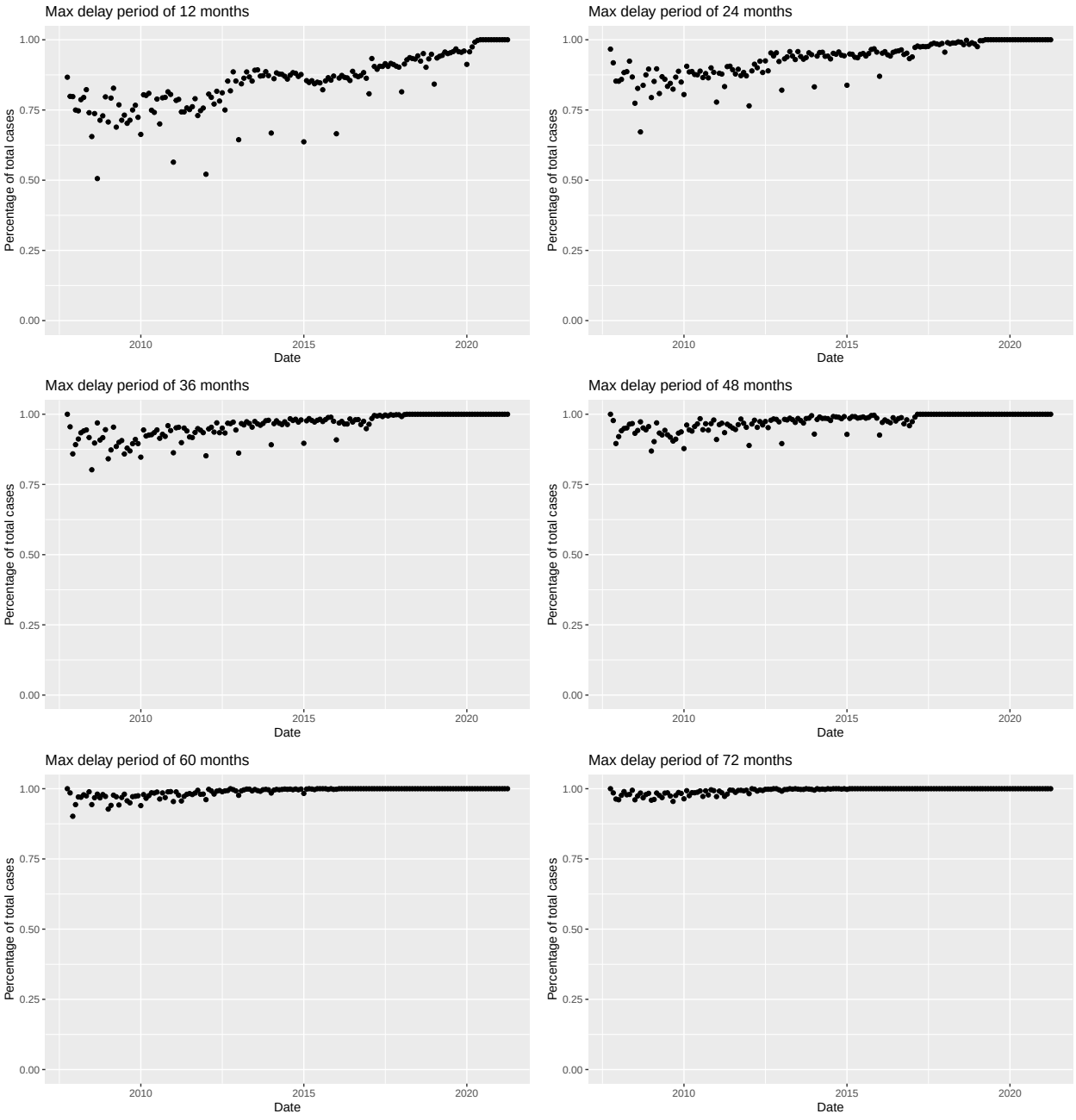

Figure 3. Cumulative proportion reported

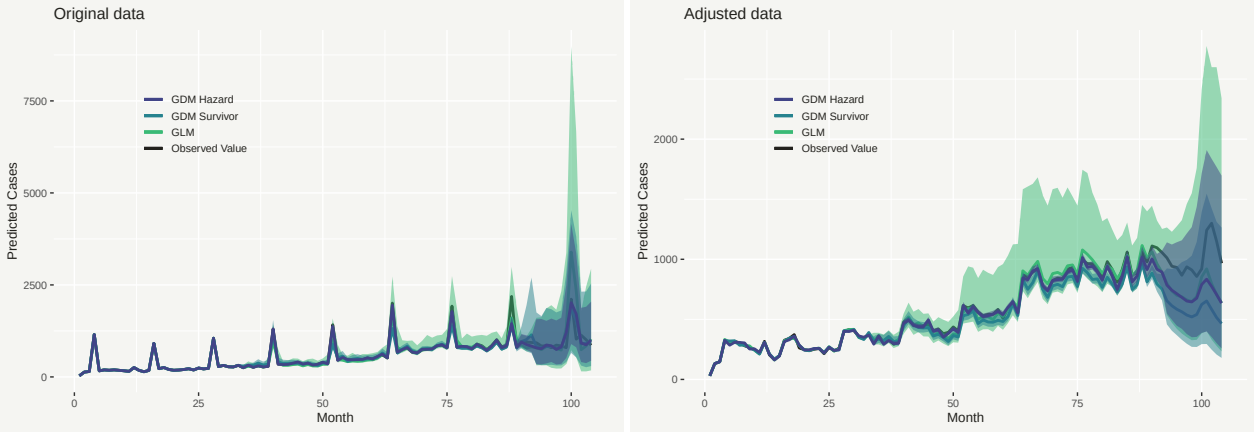

Figure 4. In-sample cyber forecast comparison

Figure 5. Covariance of Z

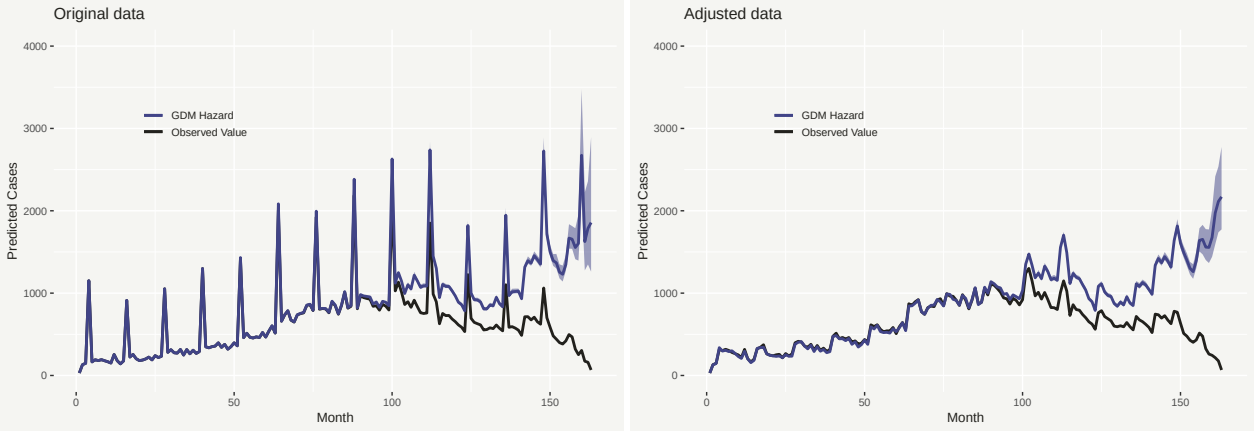

Figure 6. Out-of-sample bias correction

April 2021. The result is shown in Figure 6. Consistent with our expectation, for both datasets the trend of cyber risk is increasing steadily over the years rather than decreasing in the recent period. Also, since the results in Figure 6 are based on the median estimates of GDM hazard model in the first stage, it is important to see whether choosing different sets of estimates will significantly change the results. Figure 7 provides the forecast comparison when using the lowest and highest threshold of the confidence interval in the first stage. This shows that an increasing trend of cyber risk is robust even when considering the model bias. We will use the corrected sequence for the frequency analysis in the next part.

Since cyber risk is heterogeneous and different risk types and industries have quite diverse properties, we further explore the data series for these categories with our bias correction method. Figure 8 and Figure 9 plot the results for six different types and ten different industries of cyber risk[12], and we can find that the corrected time trends are significantly different from the original ones. Although in different magnitude, the increasing trend for most categories of cyber risk is evident. Further analysis of time pattern and structural changes of cyber risk is discussed in next section.

A.3. Bias correction for SAS data

The main analysis on report delay problem is based on Advisen data since it has detailed information on the time dimension. To validate the results from this database, we further apply the method above to another dataset-SAS. However, since SAS data only have information on the yearly level about the date of occurrence, we use this data for robustness check but not further analysis. As shown in Figure 10, the whole sample on operational risk (left graph) exhibits a decreasing trend in recent years, even after controlling the problem of report delay. In comparison, there is a slightly increasing trend for cyber events in the data after the bias correction process (right graph). Therefore, this suggests the increasing trend we observe in Advisen data is not

[12]We do not include all types and industries due to the limited data for small categories over the time.

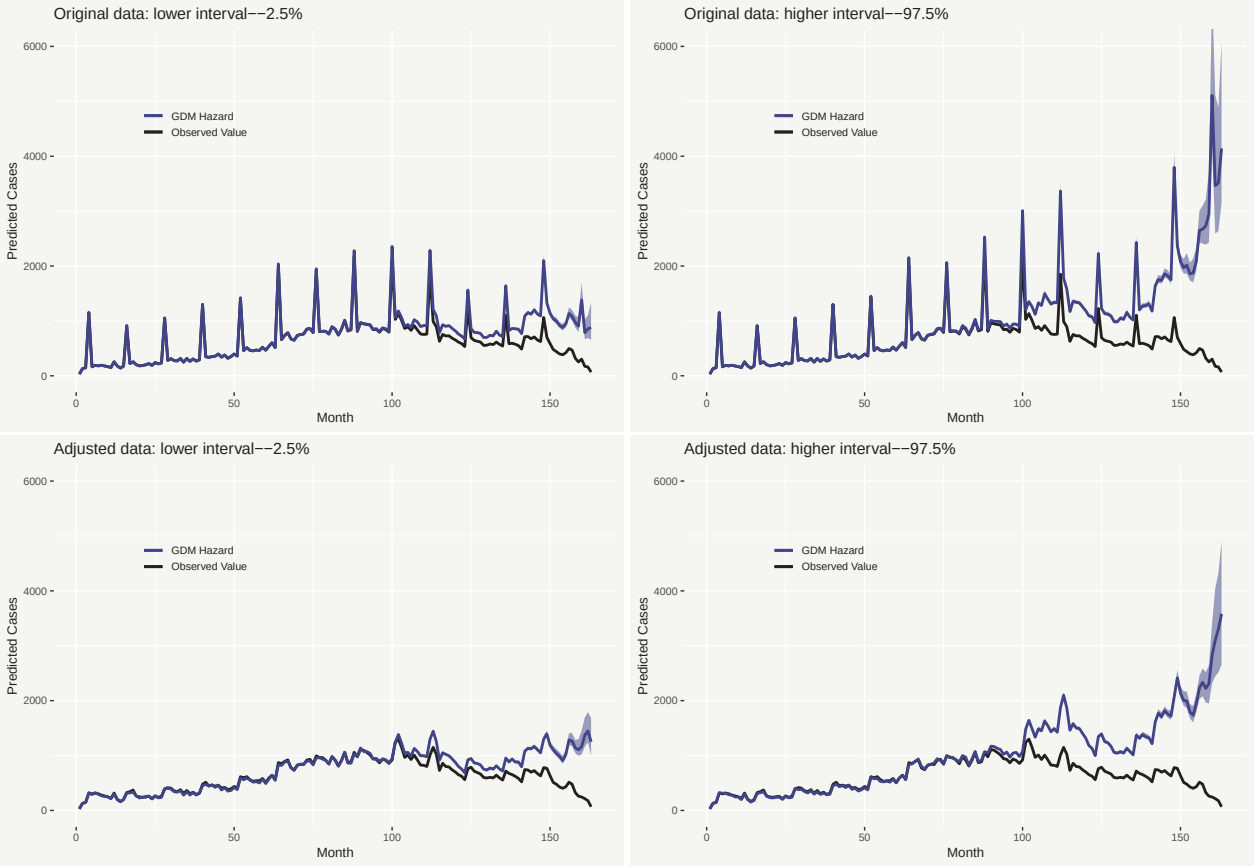

Figure 7. Confidence interval for bias correction

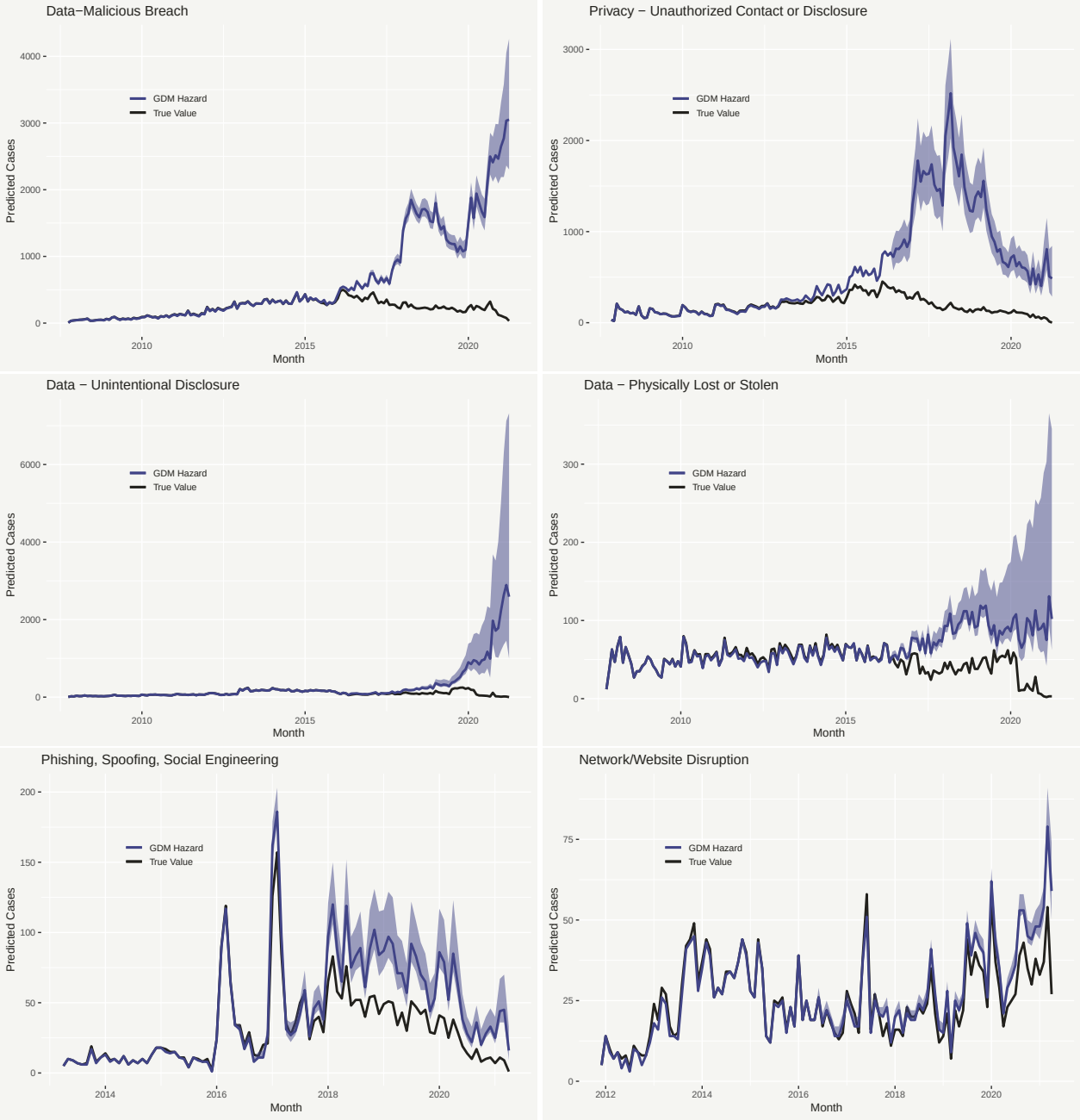

Figure 8. Bias correction by risk type

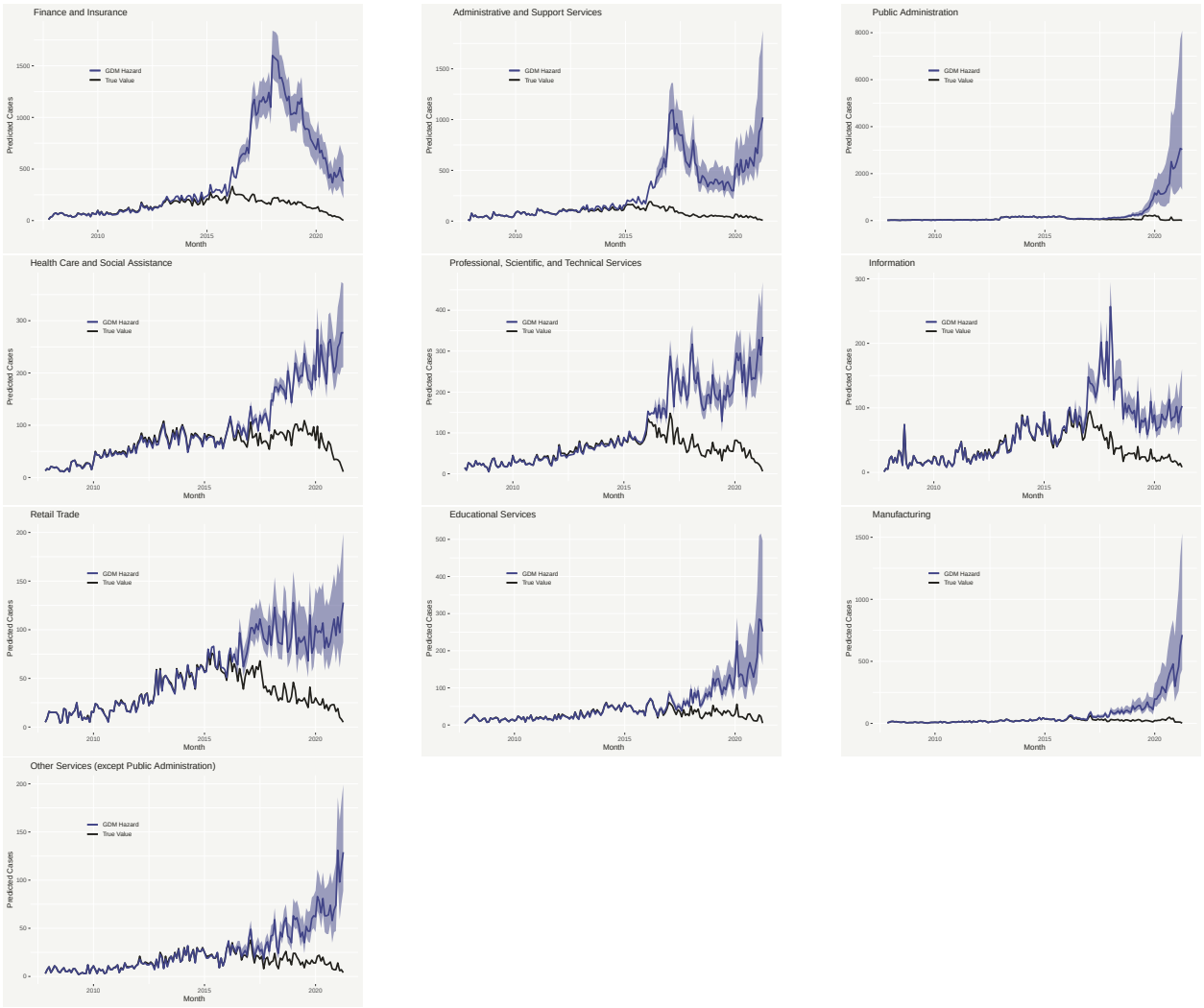

Figure 9. Bias correction by industry

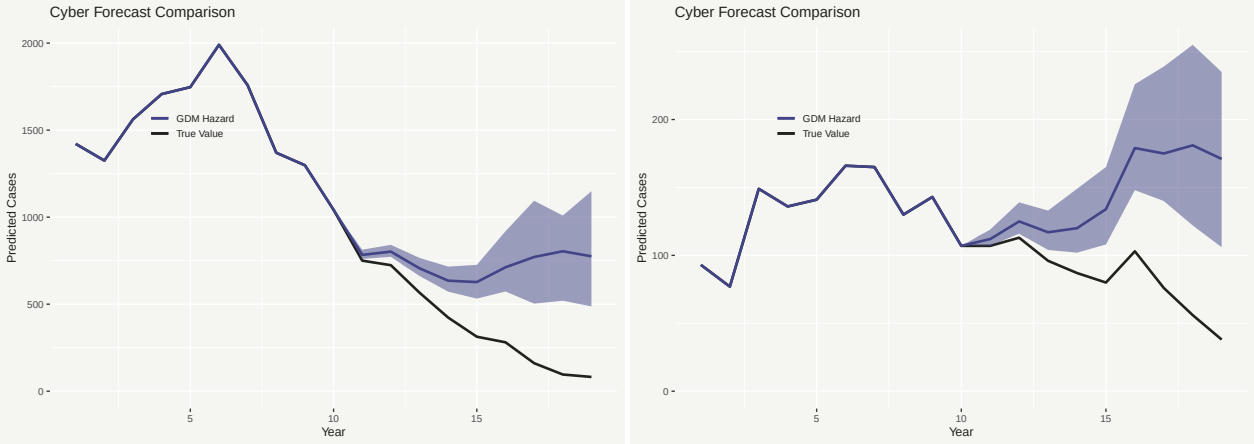

Figure 10. Bias correction for SAS data

uniqueand data specific, especially that the SAS data only include large events with loss amount higher than $10,000.

B. Time dynamics of loss frequency

B.1. Change point detection

To better understand the dynamics of loss frequency, we apply the narrowest-over-threshold method to the bias-adjusted time series data of cyber risk.

We first focus on the aggregate data of cyber risk. The top-left graph of Figure 11 shows the result with the bias-corrected data from the previous section. We identify 6 change points at the following dates: November 2011, October 2015, February 2017, September 2018, April 2020 and November 2020. The first two change points lead to faster rate of growth while the third change point at February 2017 marks a change into the declining trend in the number of cyber events in the following period. With the fourth change point, the increasing trend is back and the rate of increase becomes higher and higher.

Given the fact that we are working with time series data, serial dependence can be a problem of concern. Therefore, following the advice of Baranowski et al. (2019), we add additional IID Gaussian noise to the original data with mean 0. The standard deviation is chosen to be the standard deviation of the residuals after fitting the original data. The top-right graph of Figure 11 plots the result after adjusting serial dependence and we can find the overall pattern is consistent although fewer changes points are identified.

In addition, we present the results after transforming the original data into log scale. The results with and without dependence adjustment show similar pattern, which is the linear trend of cyber risk is increasing except for a small period of drop between 2017 and 2020. Overall, we find evidence of changing regimes for cyber risk frequency over the years with a general increasing pattern that is consistent with different methods.

To better understand the dynamics of loss frequency, we analyze the time patterns of different

types and industries. The results are presented with the method after adjusting serial dependence. Figure 12 shows the change points detected for 6 risk types. The type "Malicious breach" and "Unintentional disclosure" share similar patterns with a steady period before 2019 and a rapidly increasing period after 2019. This is intuitive in the sense that these two types are newly emerging risks in recent years. The type "Physically lost or stolen", "Phishing, Spoofing, Social Engineering" and "Network/website disruption" all have a relatively stable pattern with slightly upward trend. The only type that exhibits a decreasing trend is "Unauthorized contact or disclosure". More specifically, this risk increases significantly and peaks around 2018, followed by a volatile decreasing trend. This is not surprising since this risk is strongly associated with regulation and privacy-related penalty. In more recent years, companies can better comply with the regulation and naturally the number of events drops. Overall, we can find that the increasing trend of aggregate cyber risk is largely attributed to the surge of malicious breaches and unintentional disclosure.

For the time pattern of different industries, the increasing trend is clear for most of the industries, as shown in Figure 13. The only clear exception is the finance and insurance industry, which exhibits a significant drop in cyber loss frequency after 2017. Even though the exact reason is difficult to identify, a probable reason is that the companies in this industry have a strong motivation to invest in cybersecurity as their data are highly valuable and sensitive, thus reducing the probability of successful cyberattacks and other risks.

B.2. Cross comparison of multiple sources

There are also many other papers looking at the time dynamics of cyber risk, although in different perspectives with different data sources. Jamilov et al. (2021) collect a complete set of transcripts from quarterly earnings conference calls of public firms from 85 countries over 2002-2020 period, and construct a cyber risk exposure measure for each quarter, as shown in the upper right graph in Figure 14. The time pattern of their results is very much similar to our bias-corrected pattern in the upper left graph. Jamilov et al. (2021) also highlights some notable events related to cyber risk, which in general fit into the change points we detect (although not precisely). In addition, Florakis, Louca, Michaely & Weber (2020) builds a cyber risk exposure measure based on the "Risk Factor" section of the SEC filings and presents the yearly average of this measure from 2011 to 2018 (lower left graph). Although they have less granular results, the increasing pattern is basically the same as what we show. Lastly, Jiang, Khanna & Yang (2020) compare the trend of google search on data breach and the actual number of events in PRC data (lower right graph).

C. Time dynamics of loss severity

For the analysis of loss severity, we focus on four kinds of data. The first one is the non-zero financial loss distribution of cyber events from Advisen, the second one is the non-zero distribution of number of accounts affected from Advisen, the third one is the non-zero financial loss distribution from SAS data, and the last one is the distribution of number of records breached in PRC data. As mentioned above, the difference for the financial loss data in Advisen and SAS is that SAS data

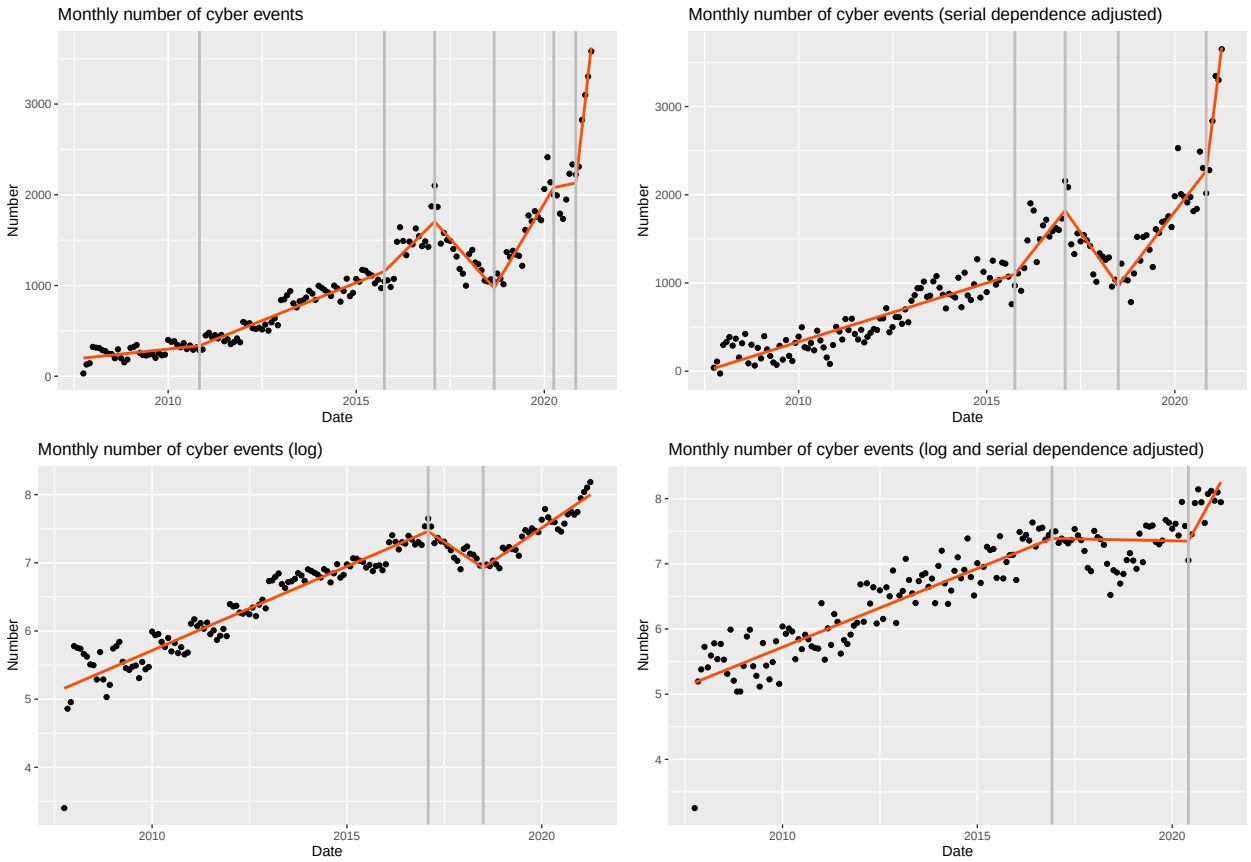

Figure 11. Change points for loss frequency

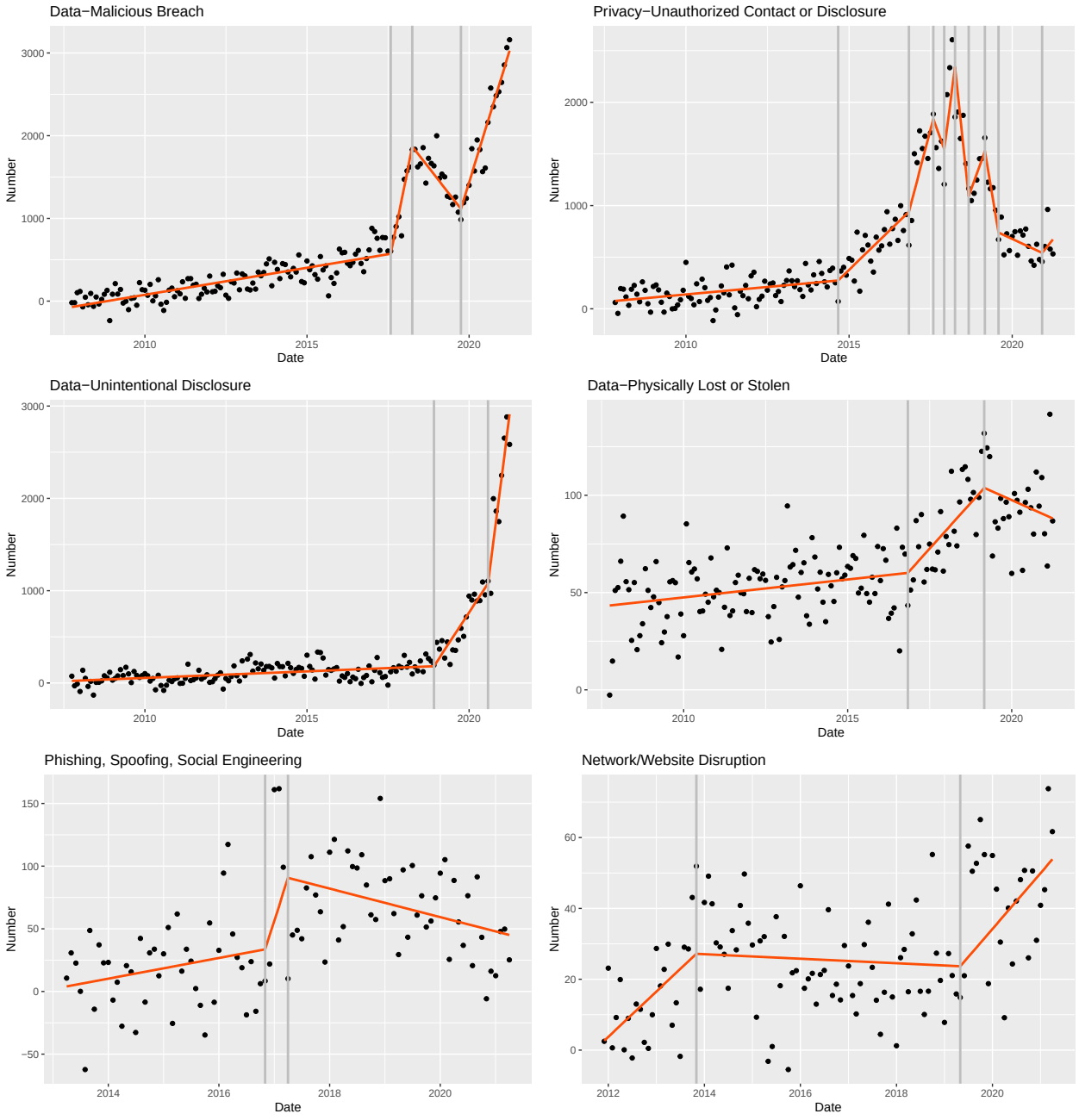

Figure 12. Change points for loss frequency by risk type

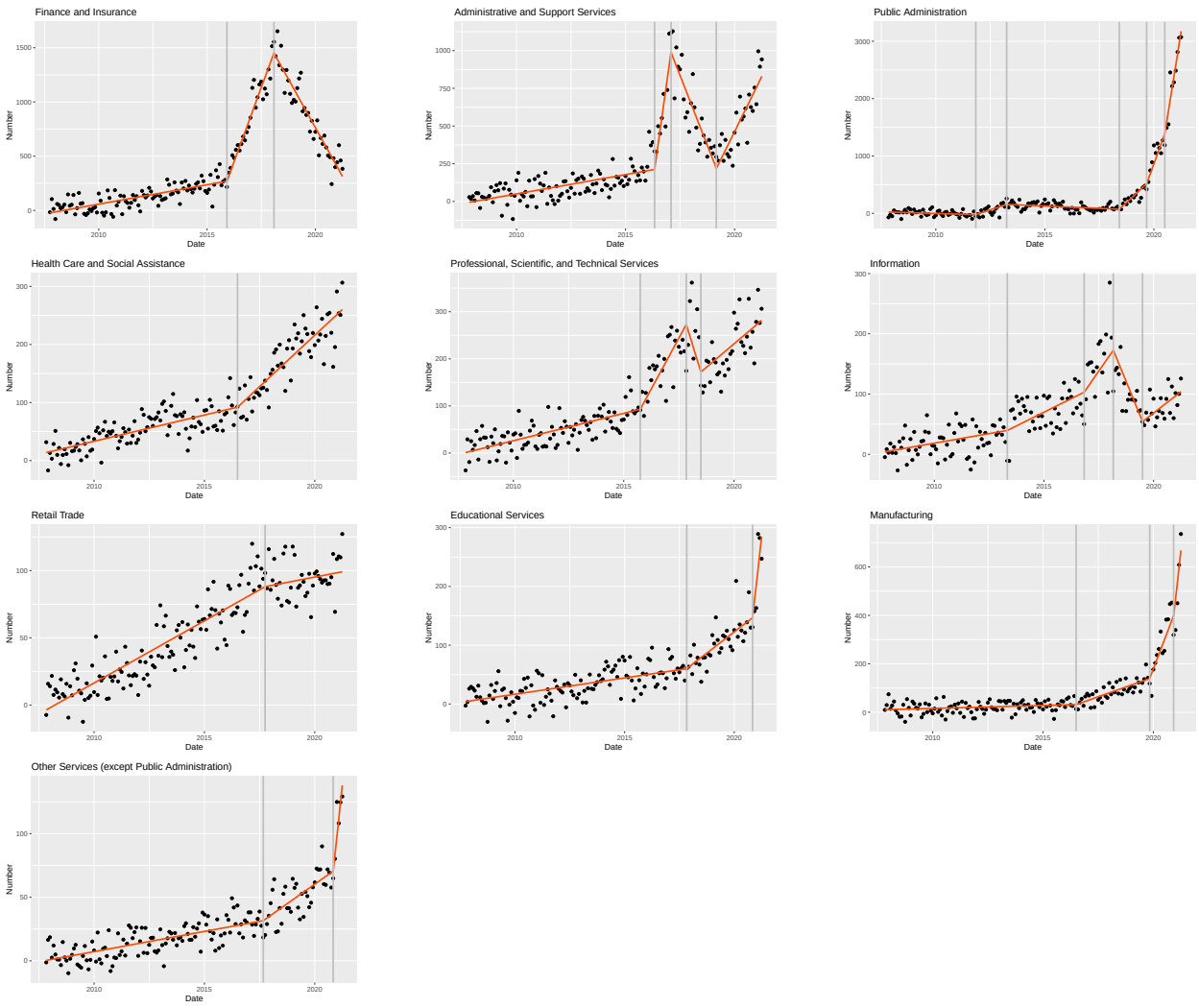

Figure 13. Change points for loss frequency by industry

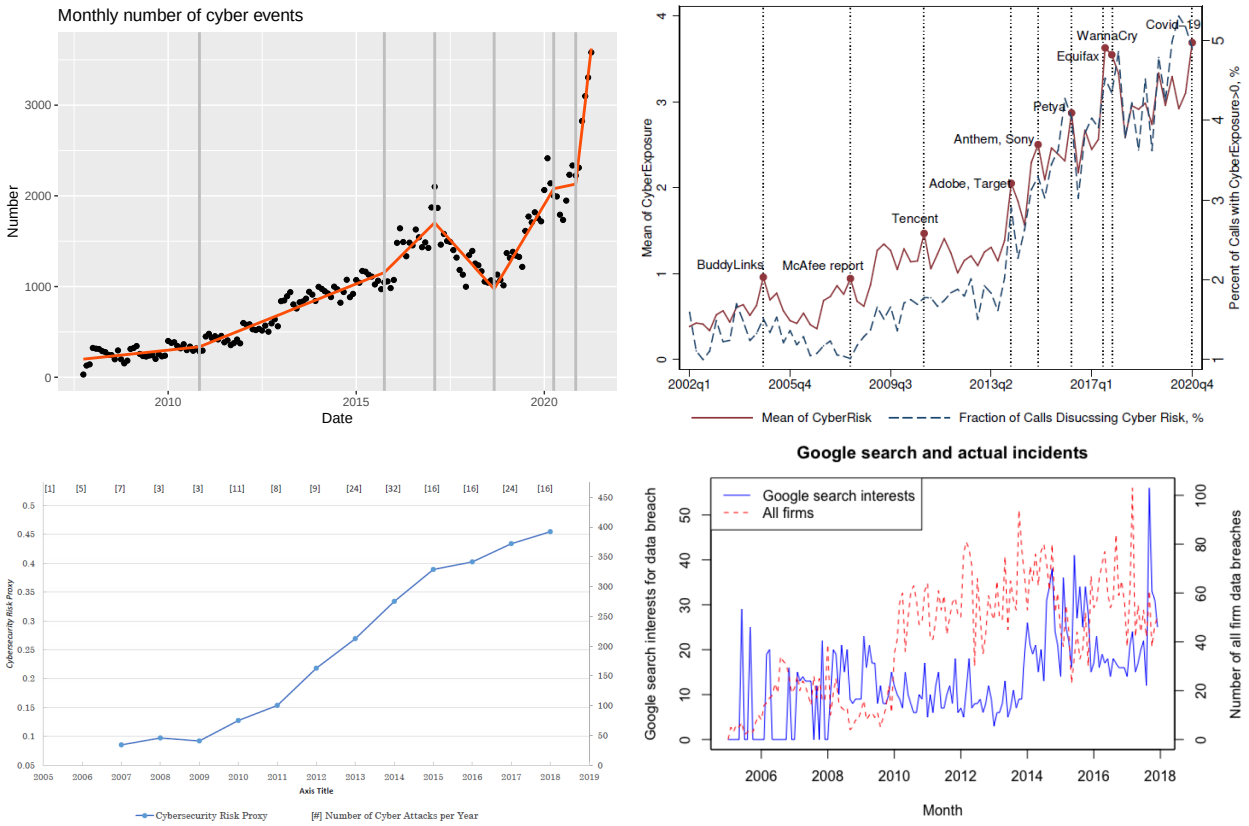

Figure 14. Cross comparison of multiple sources

only includes losses more than $100,000, therefore they are not directly comparable without further adjustment. In addition, there are also key differences between Advisen and PRC data for records and accounts affected such that Advisen data do not only focus on data breach cases and the term "accounts affected" is more general, including also the cases when the client account (e.g. bank account) is misused or has errors, etc. Therefore, there are more observations for accounts affected in Advisen than records breached in PRC.

We plot the log-transformed version of the distributions in Figure 15 since all the distributions are heavily right-skewed. In Figure 15, we can find there are potential change-points in each sequence. Also, the distribution of accounts affected in Advisen is different from others in the sense that there are a large amount of cases that only one account is affected. Therefore, two peaks can be seen in the graph.

Figure 16 provides further results on the dynamics of loss distributions using the change point detection method from Dubey & Müller (2020). The left panel shows the evolution of test functions and the highest value indicates the most likely change point location. Using the bootstrap critical values, we can find that the change points for the first three sequences are statistically significant while the last one is not. The identified change points for the first three sequences all take place in the early 21st century, ranging from 2003 to 2007. The right panel compares the distributions before and after the change point. A common feature is that the distribution is shifting to the left, which means lower loss severity in the recent period. There are two possible reasons for this change. First, with the development of IT and related technology, all firms, not only the large ones, are exposed to cyber risk. Therefore, the losses come from both the large and small firms and thus shift the overall loss profile to the left. Second, in the event of cyber loss, firms are reluctant to make such information public and small losses are easier to hide. But in recent years the regulation of data privacy becomes stricter and thus affected firms are less likely to hide the information. Therefore, we can find the loss severity becomes lower recently.

D. Time dynamics of tail risk

D.1. Basics of cyber tail risk

For the estimation of tail risk, a main question is the range of extreme values which will influence the accuracy of the estimation. Figure 17 shows the results by varying the range of extreme values for different databases, namely Advisen (loss amount), Advisen (accounts affected), SAS (loss amount), and PRC (records breached). As can be seen in Figure 17, although the estimation of tail index becomes more stable with the increasing number of extreme observations, we can find that the difference across different ranges is not significant (except the case of SAS since the data points are limited).

In addition, we provide a detailed comparison of tail index in Table II. We can find that the results when using 5% and 10% are not significantly different, while we can have a more accurate confidence interval with more observations. Therefore, for the following analysis, we will use the top 10% of the sample for analysis.

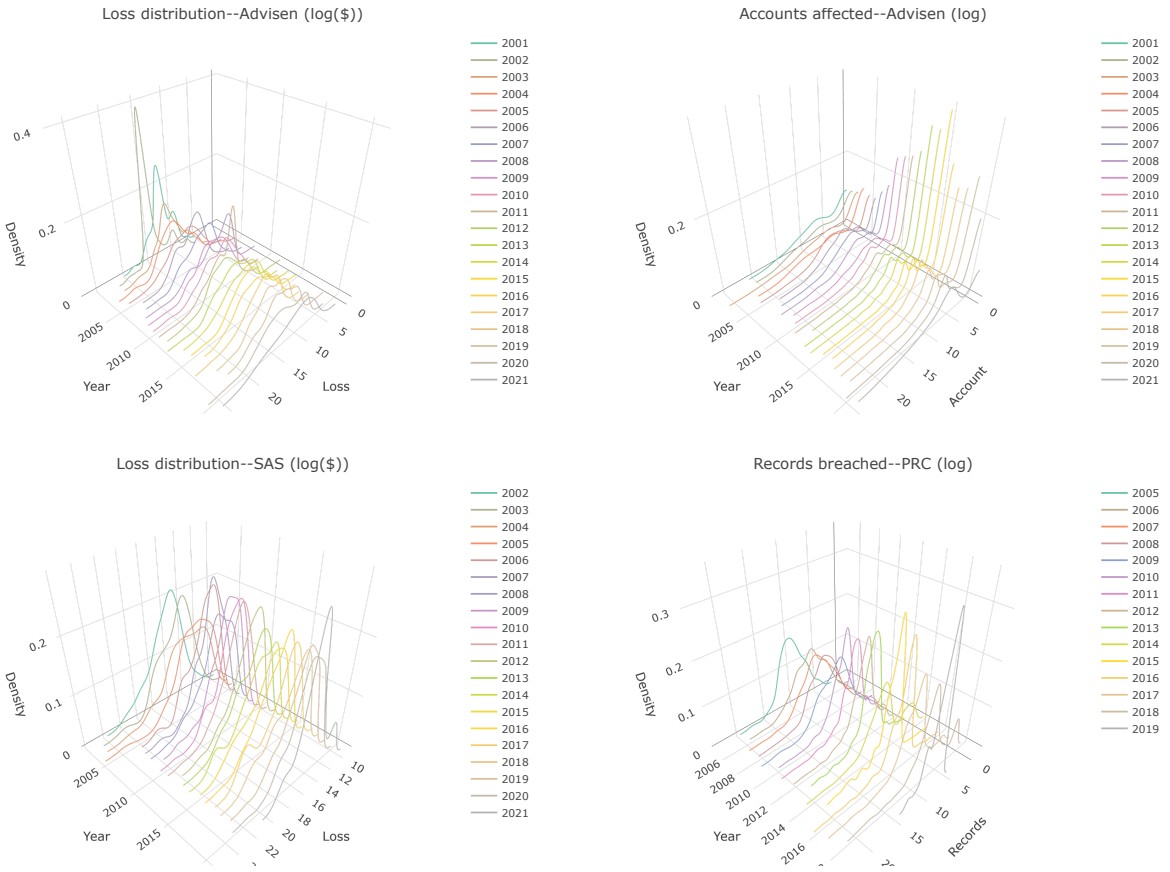

Figure 15. Dynamics of distributions

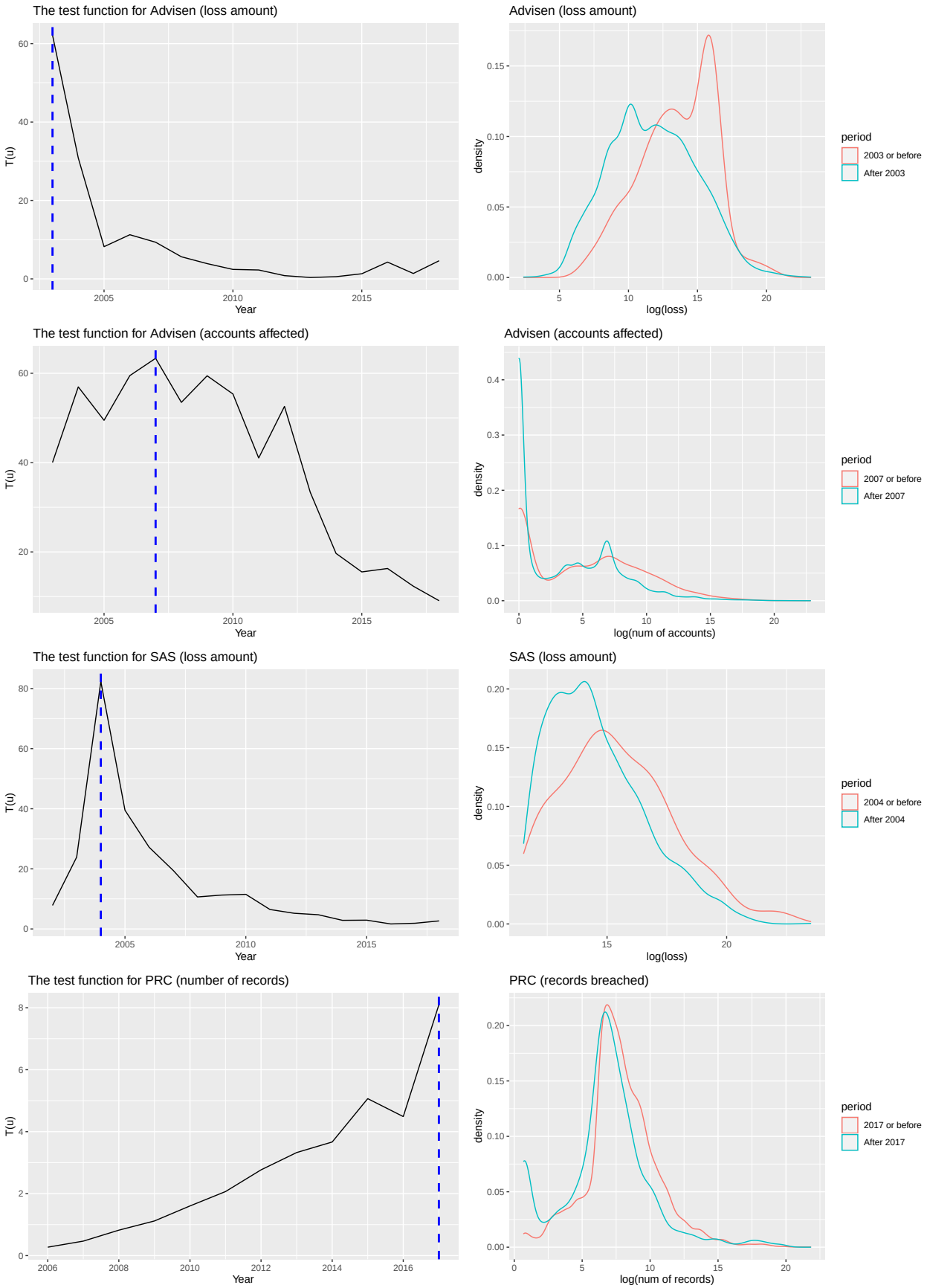

Figure 16. Comparison of distributions

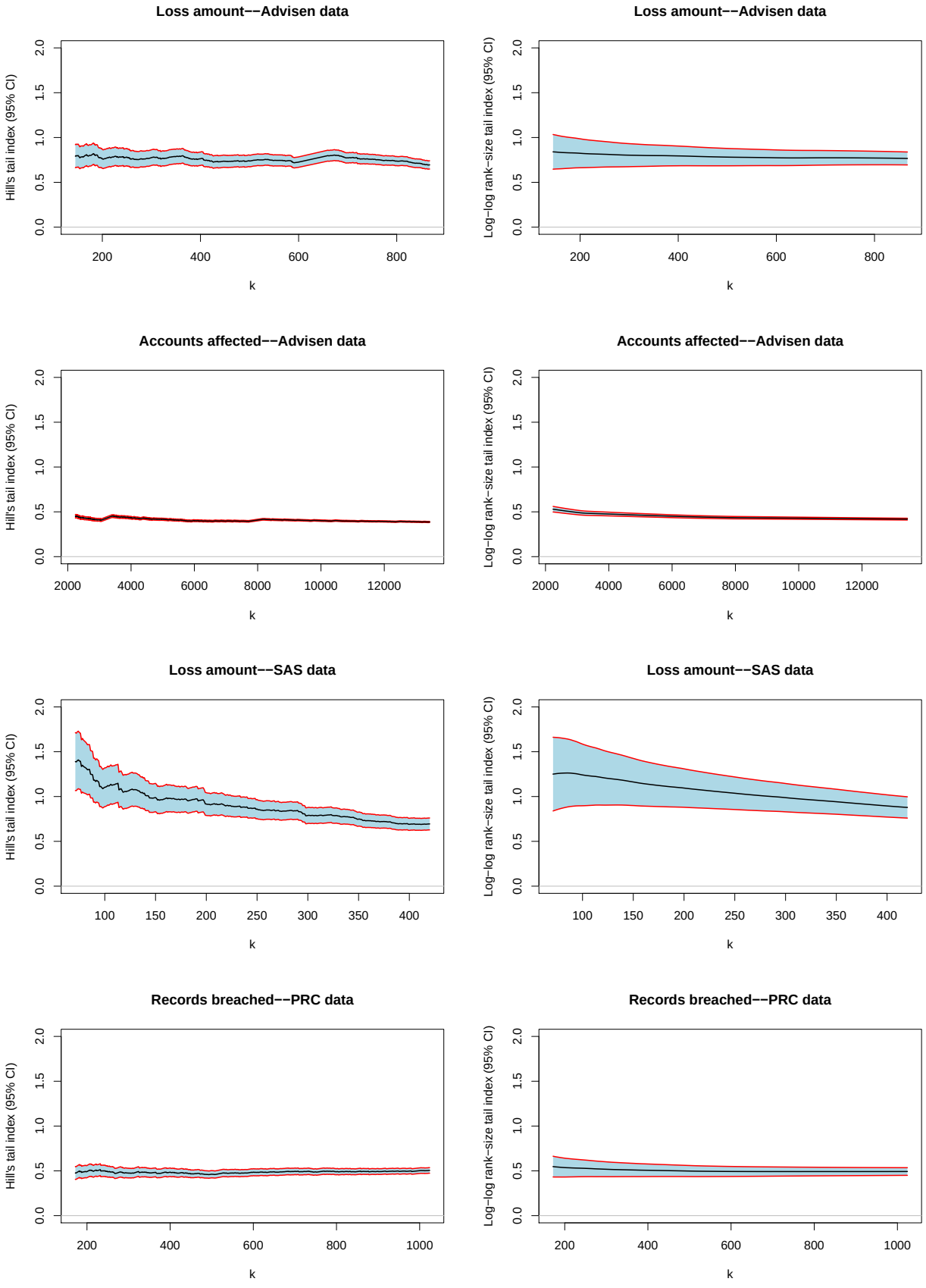

Figure 17. Comparison of tail index–The range of k (number of extreme observations) is from 2.5% to 15% of the whole sample

Table II Comparison of tail index

		Hill's estimator			Log-log rank-size estimator		
Sample	Number after truncation	Tail index	95% CI (lower)	95% CI (higher)	Tail index	95% CI (lower)	95% CI (higher)
Advisen (loss amount)							
Truncated at 5%	290	0.77	0.68	0.85	0.80	0.67	0.94
Truncated at 10%	578	0.74	0.68	0.80	0.78	0.69	0.87
Advisen (accounts affected)							
Truncated at 5%	4478	0.43	0.41	0.44	0.47	0.45	0.49
Truncated at 10%	8956	0.41	0.40	0.42	0.43	0.42	0.44
SAS (loss amount)							
Truncated at 5%	141	1.01	0.84	1.18	1.18	0.90	1.45
Truncated at 10%	280	0.84	0.74	0.94	1.01	0.84	1.17
Advisen (records breached)							
Truncated at 5%	342	0.48	0.43	0.54	0.51	0.44	0.59
Truncated at 10%	683	0.49	0.46	0.53	0.49	0.44	0.54

Note:
The truncation in this proposal is made for the right tail. Truncated at 10% level means the largest 10% is used.

For the estimation of tail risk, we can find the results of four data sequences are all below the threshold of 1, indicating extremely heavy-tailed nature of cyber loss distribution. Also, the record/account data have much higher severe tail risk compared with loss amount data. To have an idea, Maillart & Sornette (2010) and Wheatley et al. (2016) provide tail risk estimation of the amount of breached items for cyber risk, which are 0.7 and 0.37. Therefore, the results we have are consistent with the literature.

For the dynamics of tail risk, we plot the trend with recursive and rolling window methods. To avoid small sample bias, we use a 2-year fixed window for the rolling window method. Therefore, the time period starts from 2003 (the estimation of PRC data starts from 2007). Figure 18 to 21 provide the results of these methods. We can find that the recursive measure provides stable results for tail risk, while rolling window method exhibits more volatility. Overall, the trend of tail index for cyber risk is steady across different periods, and the indices for all types of cyber data are consistently below the threshold of 1, although the results for records and accounts are more heavy-tailed than the results of monetary loss.

D.2. Structural breaks in tail risk

To understand the dynamic nature of cyber tail risk, we follow the method of Ibragimov & Müller (2016) and Chen & Ibragimov (2019) to test the equality of tail risk given a fixed point in time.

We partition the sample before and after the fixed time point into two groups and four groups for comparison. Also, we use both Hill and log-log rank size estimators for the calculation of tail risk. Figure 22 to Figure 25 show the results based on four types of data: loss amount in Advisen, number of accounts affected in Advisen, number of records breached in PRC and loss amount in SAS. For each figure, we consider every month as a possible break point and conduct student t test. [13] Then we plot the p value of the test for each month, where the upper graphs are based

[13] We select all the months two years after the start date of the sample and two years before the end date so that

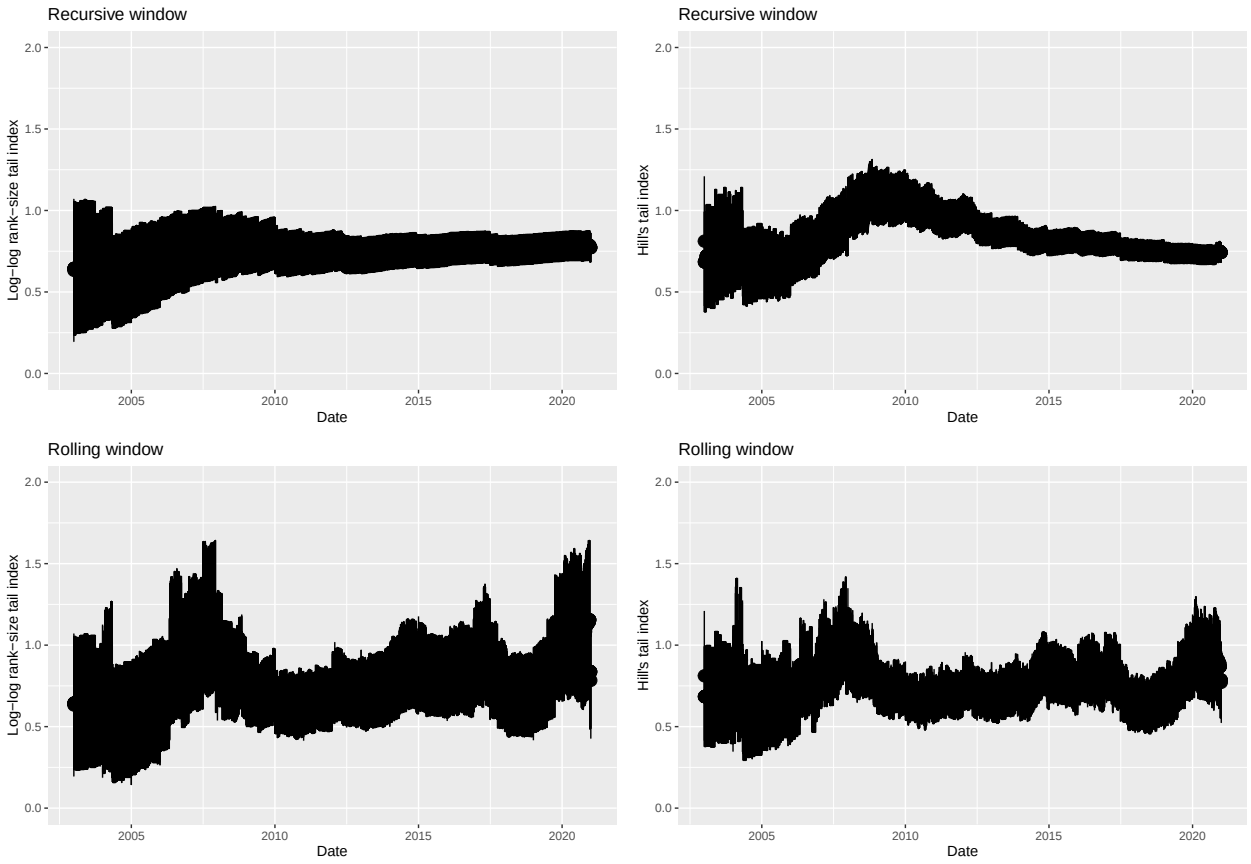

Figure 18. Recursive window and rolling window-Advisen (loss amount)

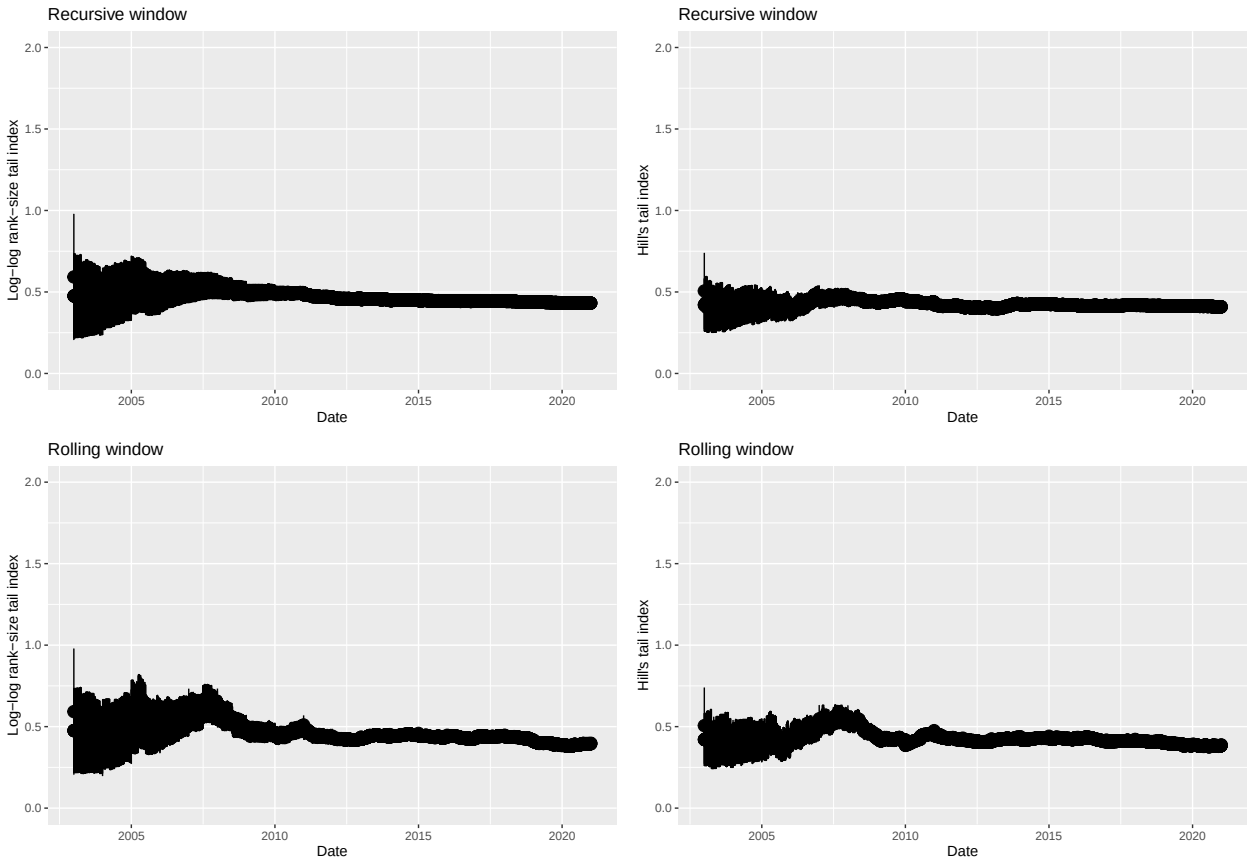

Figure 19. Recursive window and rollingw window-Advisen (accounts affected)

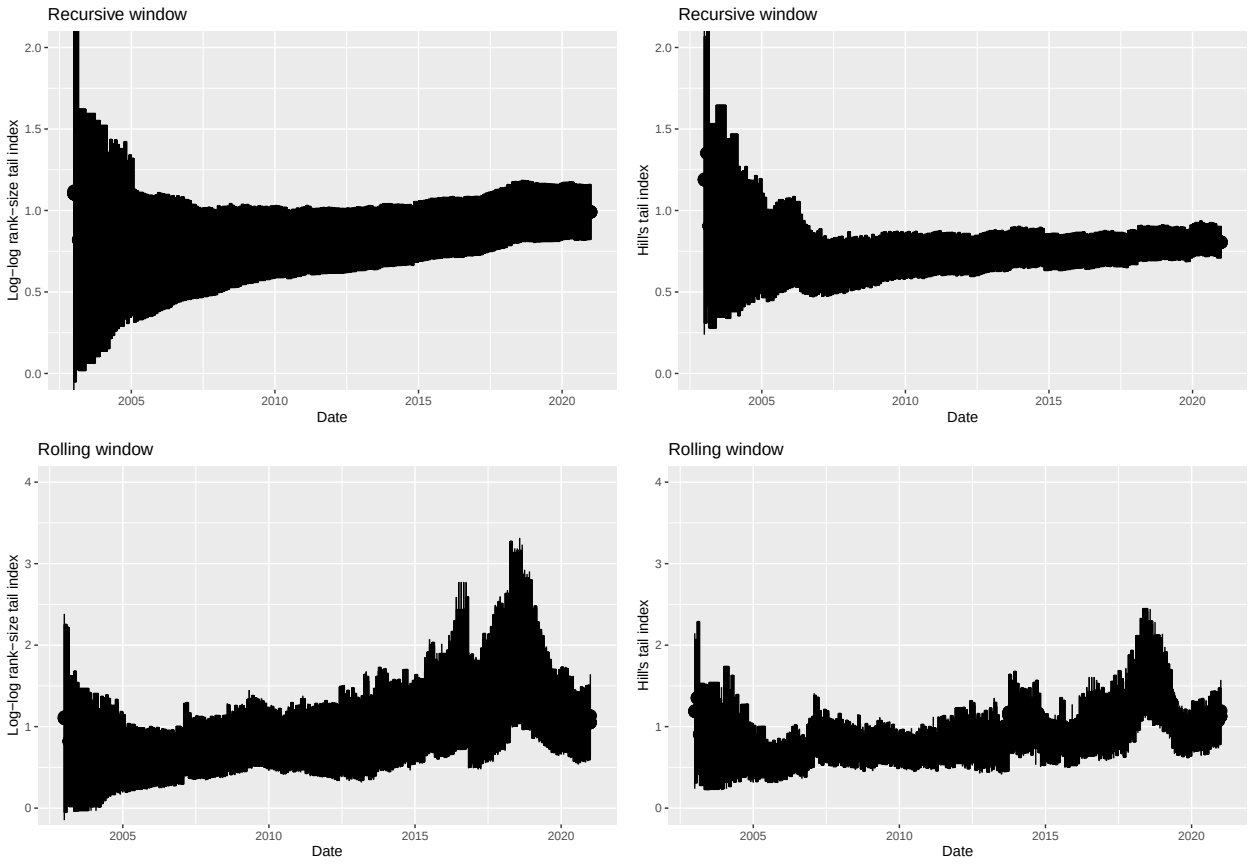

Figure 20. Recursive window and rollingw window-SAS (loss amount)

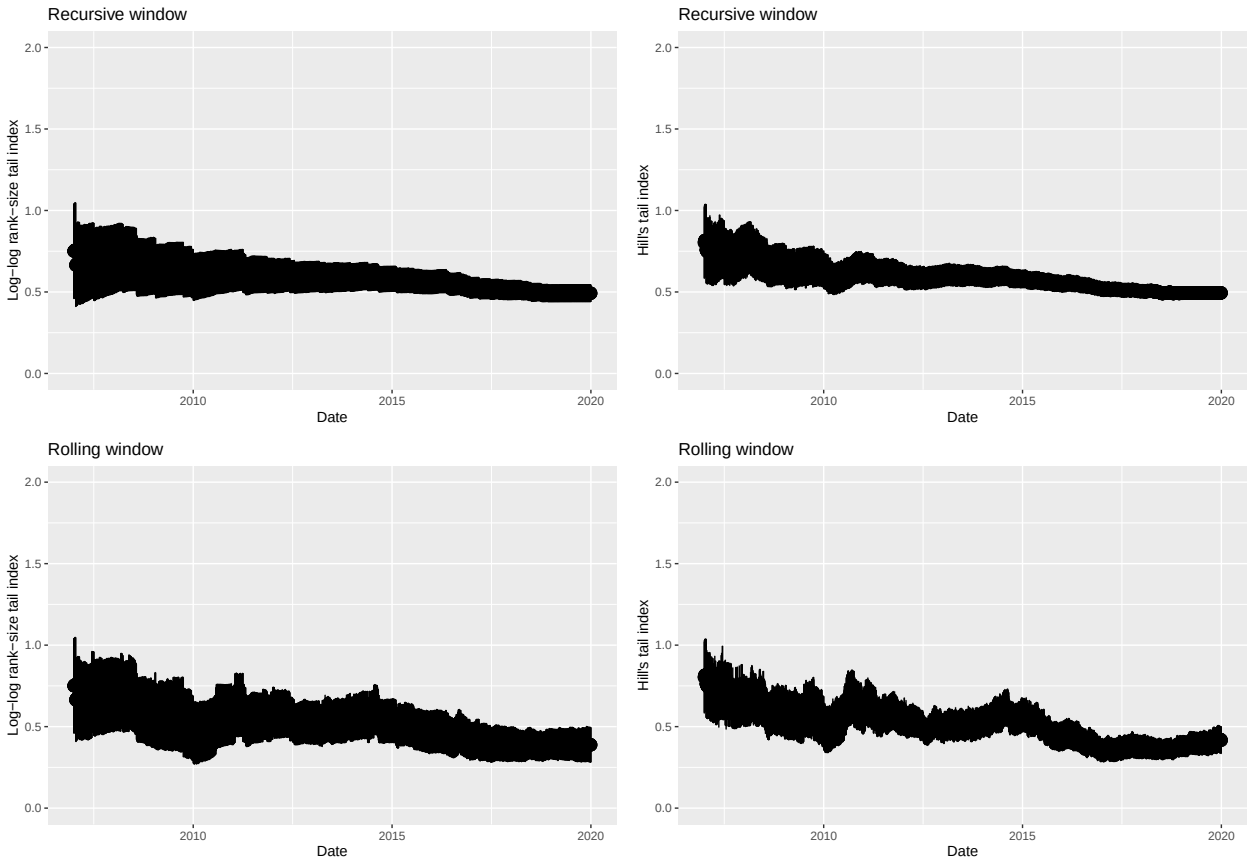

Figure 21. Recursive window and rolling window-PRC (records breached)

on two groups and lower graphs are based on four groups. The red lines in each graph indicate the 5% and 10% significance level for illustration.

From the results, we can find that four groups have more significant results than the case of two groups but they have similar trends as they go up and down in the same period. In Figure 22, the possible change points occur either in the early time before 2004 or later in 2013. To better understand this, we can compare this with Figure 18. We can find that there is a slightly increasing trend around these periods. For the loss data in SAS, we can also find a possible change point around 2013 in Figure 25 and after this change point tail risk becomes less severe, as shown in Figure 20.

Figure 23 shows the possible change points for data of accounts affected. The possible periods are 2008, 2011, and after 2017. As indicated in Figure 19, the change points may lead to decreasing tail index and increasing tail risk. The case of number of records breached is shown in Figure 24 and again the change points occur around 2008, 2011 and after 2014. Comparing with Figure 21 entails that the change points lead to higher tail risk afterwards.

Overall, the general pattern we find is that the tail risk for financial loss is becoming less severe while the case for accounts and records affected is getting more heavy-tailed. The reason for latter is very likely related to the rapidly increasing Internet technology with greater capacity to store data and higher risk of data breach. But the reason for the financial loss might not be clear, either this shows that indeed financial loss of cyber risk is less heavy-tailed recently, which is a good sign, or may relate to certain data issues such as selection bias.

IV. Conclusion

With the rise of cyber risk in recent years, it becomes more and more important to understand and manage cyber risk for the whole society, especially during the COVID-19 period. To better understand the dynamic nature of cyber risk, this papers exploits three main databases to study different dimensions of cyber risk. We first deal with the problem of report delay that is inherent to the database. Then we move on to analyze the frequency and severity of cyber risk using state-of-art statistical methods for the detection of structural changes. We show the increasing trend of cyber risk over the years is apparent and the dynamics of cyber risk is evident with several structural changes in the last decade. Moreover, we focus on the dynamics of tail risk and find that the heavy-tailedness of cyber risk is persistent over time.

we can have enough sample points for each subsample over time.

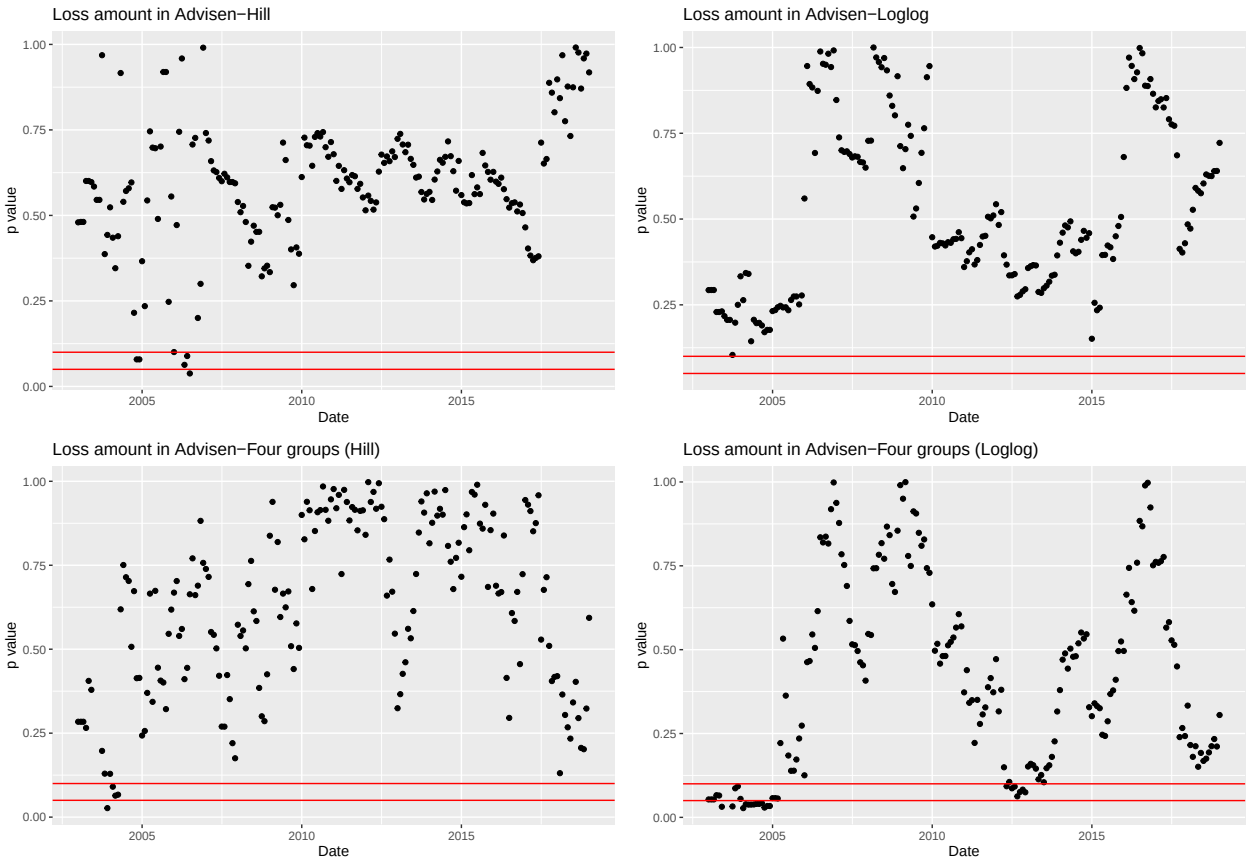

Figure 22. Two sample t test-Advisen (loss amount)

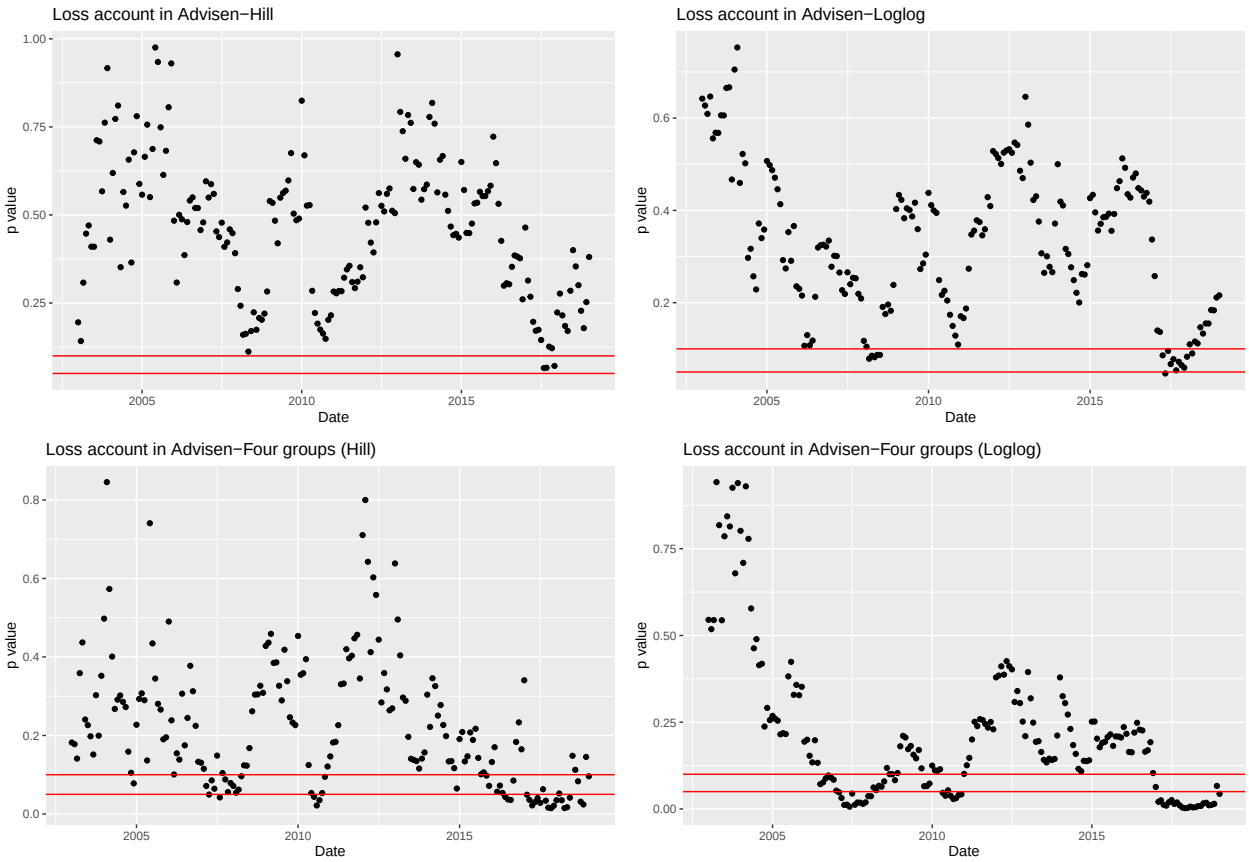

Figure 23. Two sample t test-Advisen (accounts affected)

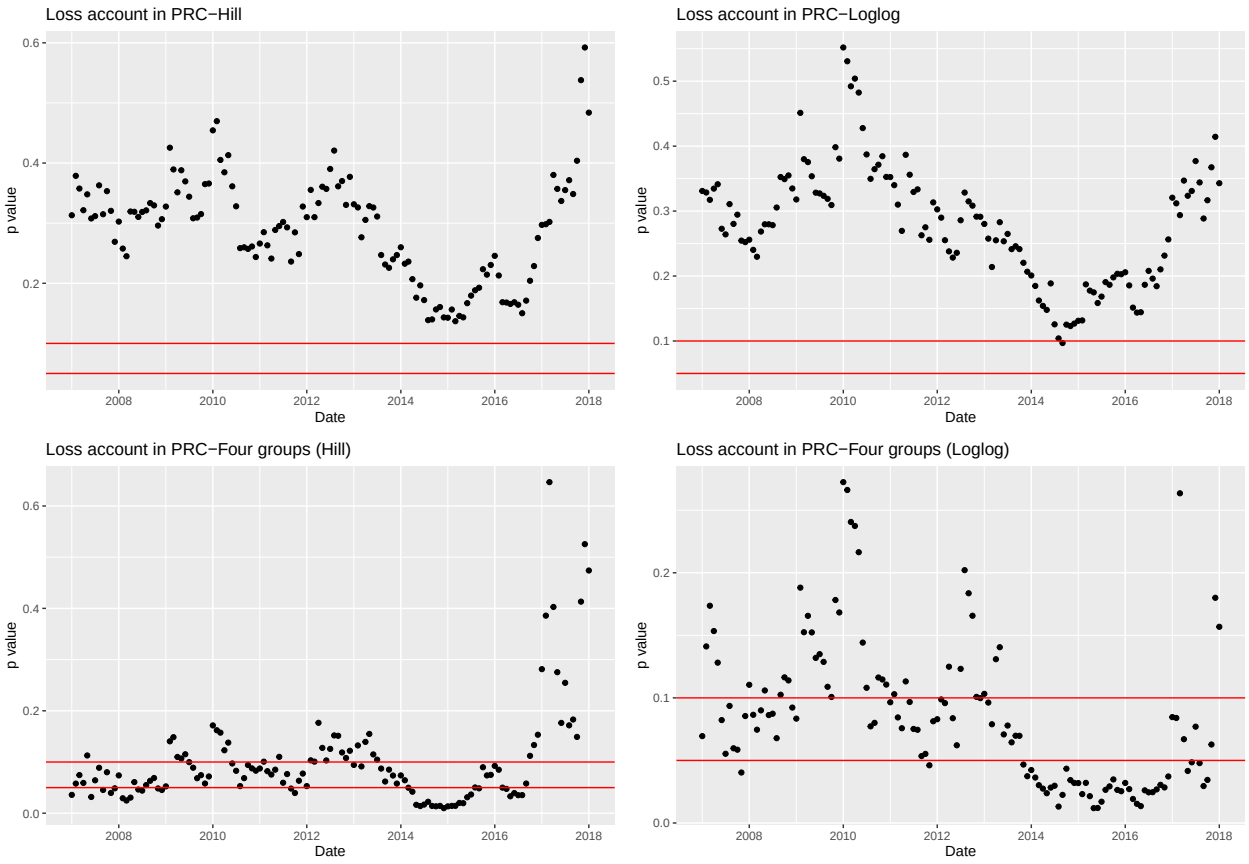

Figure 24. Two sample t test-PRC (records breached)

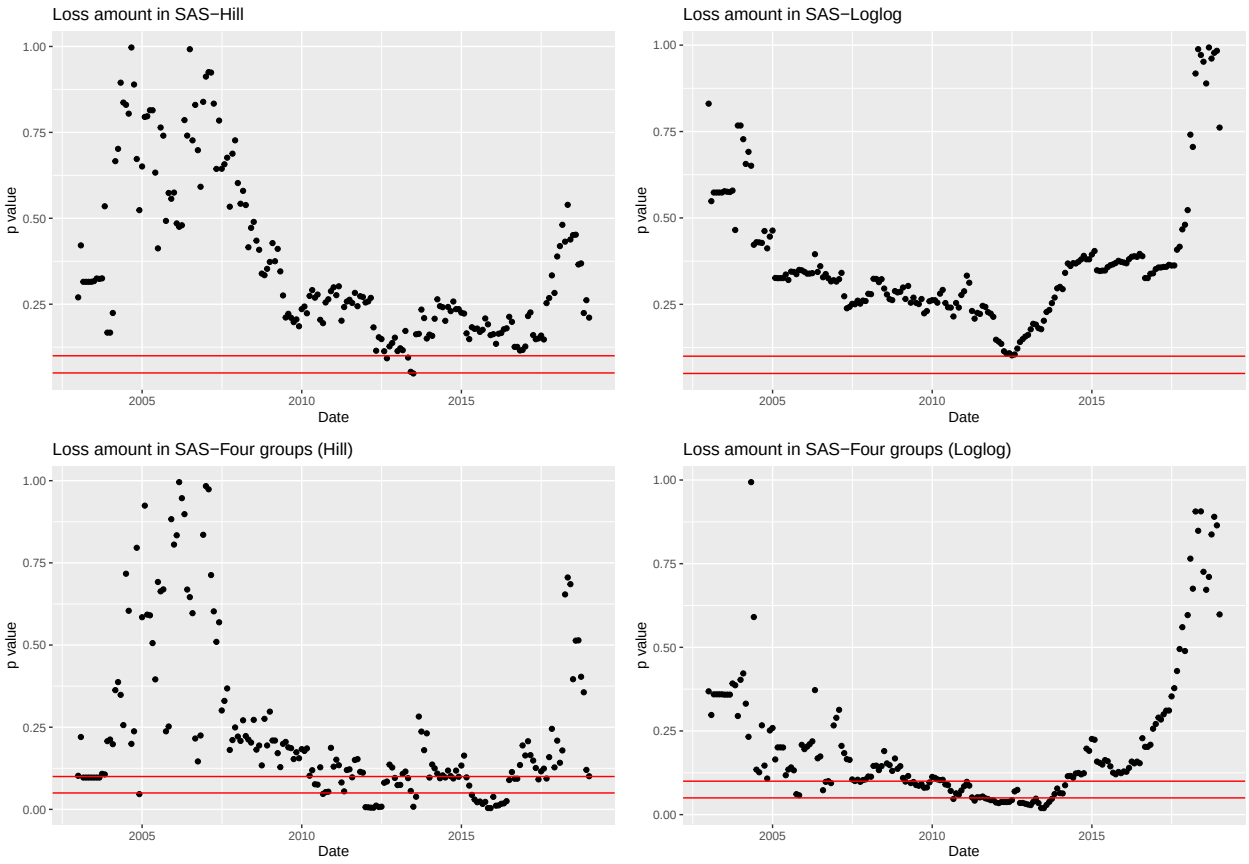

Figure 25. Two sample t test-SAS (loss amount)

Appendix A. Literature review

We summarize the works studying the empirical properties of cyber risk in the following table. Although there have been works with empirical data before 2010, the data are not actual cyber events but cyberattack attempts without information on the realization of such attempts (e.g., Böhme & Kataria 2006). Therefore, Maillart & Sornette (2010) is the earliest empirical work on cyber risk analysis with actual cyber events data. In addition, we do not include the empirical work on estimating the financial impact of cyber events based on event study approaches (e.g., Kamiya et al. 2021) since they do not focus on the statistical properties of cyber risk per se.

The early stage of the empirical work focuses on the general statistical properties of cyber risk, including correlation structure (Böhme & Kataria 2006; Wang & Kim 2009*a*; and Wang & Kim 2009*b*) and time trends (Maillart & Sornette 2010; Wheatley et al. 2016; Edwards et al. 2016; and Romanosky 2016). Starting from Eling & Loperfido (2017), more and more studies begin to study cyber risk frequency and severity by fitting existing statistical models (Eling & Wirfs 2019; and Woods, Moore & Simpson 2021) or proposing new frameworks to model cyber risk (Bessy-Roland et al. 2021; Farkas et al. 2021; Sun, Xu & Zhao 2021; Fang, Xu, Xu & Hu 2021; and Zhang Wu, Luo, Fang, Xu & Zhao 2021). These works have exploited the available database to show the good performance of their models, and the basic consensus is that the modeling of severity should be based on heavy-tailed (at least highly right-skewed[14]) distributions, although the specific choice of the model is very diverse.

Still, the study on time dynamics of cyber risk has been scare (such as Jung 2021; and Wheatley et al. 2021) and results are inconsistent, therefore there is still large uncertainty in this area, which motivates us to consider this topic using different datasets and methodologies.

[14]For example, the results of Woods et al. (2021) show the gamma distribution has better performance, which is not heavy-tailed distribution but exhibits high skewness.

Table III Empirical work on cyber risk

Number	Title	Author (Year)	Dataset	Time period	Study Focus	Main Empirical Result/Implication
1	Models and Measures for Correlation in Cyber-Insurance	Böhme & Kataria (2006)	Honeypot data on attack intensity of network exploits	Feb 2003 to Sep 2005	Correlation of internal and global network structure	They show the existence of correlation and the result for global correlation is more robust than internal correlation.
2	A Value-at-Risk Approach to Information Security Investment	Wang, Chaudhury & Rao (2008)	Daily data from a large financial institution	Jan 2004 to Mar 2005	Value-at-risk of daily losses an organization faces	They propose the firms can make better security investment choice based on their proposed approach.
3	Cyber Attacks: Cross-Country Interdependence and Enforcement	Wang & Kim (2009*a*)	Attack data from Internet Storm Center (ISC)	Jan 2003 to Dec 2007	The impact of the first international treaty against cybercrimes on cyber attacks	They find the treaty lowers the cyber attacks by around 20% and affects the interdependency across countries.
4	Cyberattacks: Does Physical Boundry Matter?	Wang & Kim (2009*b*)	Attack data from Internet Storm Center (ISC)	Jan 2003 to Dec 2007	Spatial correlation of cyber attacks	They show strong evidence of spatial correlation over time.
5	Heavy-tailed Distribution of Cyber-risks	Maillart & Sornette (2010)	Identity Data (ID) loss event data from Open Security Foundation	Jan 2000 to Nov 2008	Heavy-tailedness of ID losses	They find the presence of a stable heavy-tailed distribution of personal identity losses per event with a strong non-stationary growth of ID losses culminating in July 2006 followed by a more stationary phase.
6	Insurability of Cyber Risk: An Empirical Analysis	Biener et al. (2015)	Cyber losses extracted from SAS OpRisk database	Mar 1971 to Sep 2009	Insurability of cyber risk	They show the distinct characteristics of cyber risk compared to other operational risk and discuss the main insurability limitations.
7	The Extreme Risk of Personal Data Breaches and the Erosion of Privacy	Wheatley et al. (2016)	ID loss event data from Open Security Foundation and Privacy Rights Clearinghouse	Jan 2007 to Apr 2015	Projection of extreme risk	They find the maximum breach size is expected to grow by 50% and the total amount is to double in 5 years.
8	Hype and Heavy Tails: A Closer Look at Data Breaches	Edwards et al. (2016)	Privacy Rights Clearinghouse	Jan 2005 to Sep 2015	Trend of data breach	They show no evidence of increasing trend for size or frequency of data breaches.

9	Examining the Costs and Causes of Cyber Incidents	Romanosky (2016)	Advisen	Jan 2004 to Dec 2015	Statistical analysis of costs of cyber risk	They indicate while there is an increase in the number of events and legal actions, the estimates of firm costs are not of large magnitude.
10	Data Breaches: Goodness of Fit, Pricing, and Risk Measurement	Eling & Loperfido (2017)	Privacy Rights Clearinghouse	Jan 2005 to Dec 2015	Model fitting for cyber risk	They find log-skew-normal is a good distribution for data breach amount.
11	Copula Approaches for Modeling Cross-sectional Dependence of Data Breach Losses	Eling & Jung (2018)	Privacy Rights Clearinghouse	Jan 2005 to Dec 2016	Cross-sectional dependence of data breach	They show the presence of a significant asymmetric tail dependece among risk factors.
12	What are the Actual Costs of Cyber Risk Events?	Eling & Wirfs (2019)	Cyber losses extracted from SAS OpRisk database	Jan 1995 to Mar 2014	Model fitting for cyber risk	They suggest that extreme value theory is needed for the modeling of severity and cyber risk is inherently dynamic.
13	Addressing Insurance of Data Breach Cyber Risks in the Catastrophe Framework	Wheatley et al. (2021)	ID loss event data from Open Security Foundation and Privacy Rights Clearinghouse	Jan 2005 to Sep 2017	Catastrophic cyber risk and the dynamics	They state the rate of breaches in excess of 50k ids is constant but an increasing trend for both frequency and severity of hack type events.
14	Multivariate Hawkes Process for Cyber Insurance	Bessy-Roland et al. (2021)	Privacy Rights Clearinghouse	Jan 2010 to Dec 2017	A multivariate Hawkes framework for modelling and predicting attack frequency	They show the proposed method has good perfomance.
15	Cyber Claim Analysis Using Generalized Pareto Regression Trees with Applications to Insurance	Farkas et al. (2021)	Privacy Rights Clearinghouse	Jan 2005 to Jan 2019	Analyzing cyber claims with regression trees	They find that some sectors (such as healthcare, education, and nonprofit organization) have lighter tails than the others, and it is important to separate typical and extreme claims.
16	Modeling Malicious Hacking Data Breach Risks	Sun et al. (2021)	Privacy Rights Clearinghouse	Jan 2005 to Mar 2019	Modeling data breach risk with a frequency-severity framework	They show the proposed framework captures the nonlinear dependence of data breach risk.
17	Extreme Data Breach Losses: An Alternative Approach to Estimating Probable Maximum Loss for Data Breach Risk	Jung (2021)	Cowbell Cyber	Jan 2005 to Dec 2018	Projection of extreme data breach losses	A significant increase with a break in 2014 for loss severity and substainally larger loss in 5 years compared to the estimate of Pareto model

18	A Framework for Predicting Data Breach Risk: Leveraging Dependence to Cope With Sparsity	Fang et al. (2021)	Privacy Rights Clearinghouse	Jan 2005 to Dec 2018	Predicting the frequency of data breach at enterprise level	Using the proposed model considering dependence, they show data breach sizes exhibit large variability and large skewness, and consecutive breaches are unlikely to occur to an enterprise within a short period of time.
19	Modeling Multivariate Cyber Risks: Deep Learning Dating Extreme Value Theory	Zhang Wu et al. (2021)	Honeypot data on attack intensity of network exploits	Mar 2013 to Aug 2013	Modeling cyber risk with deep learning and extreme value theory	They show the proposed method has high accurate prediction power.
20	The County Fair Cyber Loss Distribution: Drawing Inferences from Insurance Prices	Woods et al. (2021)	Insurers' pricing information from SERFF Filing System	Jan 2008 to Dec 2018	Inferring cyber loss distribution from prices	Using the proposed method, they show that Gamma and Lognornal distributions have better fitting perfomance.

REFERENCES

ABC (2007), 'Tjx data breach may involve 94 million credit cards'.
URL: *https://abcnews.go.com/Technology/story?id=3773782*

Accenture (2021), '2021 cyber threat intelligence report'.
URL: *https://www.accenture.com/lu-en/insights/security/cyber-threat-intelligence-report-2021*

Allianz (2021), 'Managing the impact of increasing interconnectivity: Trends in cyber risk'.
URL: *https://www.agcs.allianz.com/news-and-insights/reports/cyber-risk-trends-2020.html*

Anderson, R. & Moore, T. (2006), 'The economics of information security', *science* **314**(5799), 610–613.

Baranowski, R., Chen, Y. & Fryzlewicz, P. (2019), 'Narrowest-over-threshold detection of multiple change points and change-point-like features', *Journal of the Royal Statistical Society: Series B (Statistical Methodology)* **81**(3), 649–672.

Bessy-Roland, Y., Boumezoued, A. & Hillairet, C. (2021), 'Multivariate hawkes process for cyber insurance', *Annals of Actuarial Science* **15**(1), 14–39.

Biener, C., Eling, M. & Wirfs, J. H. (2015), 'Insurability of cyber risk: An empirical analysis', *The Geneva Papers on Risk and Insurance-Issues and Practice* **40**(1), 131–158.

Böhme, R. & Kataria, G. (2006), Models and measures for correlation in cyber-insurance., *in* 'WEIS', Vol. 2, p. 3.

Campbell, K., Gordon, L. A., Loeb, M. P. & Zhou, L. (2003), 'The economic cost of publicly announced information security breaches: empirical evidence from the stock market', *Journal of Computer security* **11**(3), 431–448.

Chen, Z. & Ibragimov, R. (2019), 'One country, two systems? the heavy-tailedness of chinese a-and h-share markets', *Emerging Markets Review* **38**, 115–141.

de Haan, L. & Zhou, C. (2020), 'Trends in extreme value indices', *Journal of the American Statistical Association* pp. 1–15.

Dubey, P. & Müller, H.-G. (2020), 'Fréchet change-point detection', *The Annals of Statistics* **48**(6), 3312–3335.

Edwards, B., Hofmeyr, S. & Forrest, S. (2016), 'Hype and heavy tails: A closer look at data breaches', *Journal of Cybersecurity* **2**(1), 3–14.

Eling, M. & Jung, K. (2018), 'Copula approaches for modeling cross-sectional dependence of data breach losses', *Insurance: Mathematics and Economics* **82**, 167–180.

Eling, M. & Loperfido, N. (2017), 'Data breaches: Goodness of fit, pricing, and risk measurement', *Insurance: mathematics and economics* **75**, 126–136.

Eling, M., McShane, M. & Nguyen, T. (2021), 'Cyber risk management: History and future research directions', *Risk Management and Insurance Review* **24**(1), 93–125.

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

Fang, Z., Xu, M., Xu, S. & Hu, T. (2021), 'A framework for predicting data breach risk: Leveraging dependence to cope with sparsity', *IEEE Transactions on Information Forensics and Security* **16**, 2186–2201.

Farkas, S., Lopez, O. & Thomas, M. (2021), 'Cyber claim analysis using generalized pareto regression trees with applications to insurance', *Insurance: Mathematics and Economics* **98**, 92–105.

FBI (2020), '2020 internet crime report'.
URL: *https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics*

Florakis, C., Louca, C., Michaely, R. & Weber, M. (2020), Cybersecurity risk, Technical report, National Bureau of Economic Research.

Gabaix, X. & Ibragimov, R. (2011), 'Rank- 1/2: a simple way to improve the ols estimation of tail exponents', *Journal of Business & Economic Statistics* **29**(1), 24–39.

Gordon, L. A. & Loeb, M. P. (2002), 'The economics of information security investment', *ACM Transactions on Information and System Security (TISSEC)* **5**(4), 438–457.

Hill, B. M. (1975), 'A simple general approach to inference about the tail of a distribution', *The annals of statistics* pp. 1163–1174.

Ibragimov, R., Jaffee, D. & Walden, J. (2009), 'Nondiversification traps in catastrophe insurance markets', *The Review of Financial Studies* **22**(3), 959–993.

Ibragimov, R. & Müller, U. K. (2016), 'Inference with few heterogeneous clusters', *Review of Economics and Statistics* **98**(1), 83–96.

Jamilov, R., Rey, H. & Tahoun, A. (2021), The anatomy of cyber risk, Technical report, National Bureau of Economic Research.

Jiang, H., Khanna, N. & Yang, Q. (2020), 'The cyber risk premium', *Available at SSRN 3637142* .

Jung, K. (2021), 'Extreme data breach losses: An alternative approach to estimating probable maximum loss for data breach risk', *North American Actuarial Journal* pp. 1–24.

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A. & Stulz, R. M. (2021), 'Risk management, firm reputation, and the impact of successful cyberattacks on target firms', *Journal of Financial Economics* **139**(3), 719–749.

Maillart, T. & Sornette, D. (2010), 'Heavy-tailed distribution of cyber-risks', *The European Physical Journal B* **75**(3), 357–364.

McAfee (2020), 'The hidden costs of cybercrime'.
URL: *https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf*

Niu, Y. S., Hao, N. & Zhang, H. (2016), 'Multiple change-point detection: a selective overview', *Statistical Science* pp. 611–623.

Reuters (2017), 'Yahoo says all three billion accounts hacked in 2013 data theft'.
URL: *https://www.reuters.com/article/us-yahoo-cyber-idUSKCN1C82O1*

Romanosky, S. (2016), 'Examining the costs and causes of cyber incidents', *Journal of Cybersecurity* **2**(2), 121–135.

Salmon, M., Schumacher, D., Stark, K. & Höhle, M. (2015), 'Bayesian outbreak detection in the presence of reporting delays', *Biometrical Journal* **57**(6), 1051–1067.

Stoner, O. & Economou, T. (2020), 'Multivariate hierarchical frameworks for modeling delayed reporting in count data', *Biometrics* **76**(3), 789–798.

Sun, H., Xu, M. & Zhao, P. (2021), 'Modeling malicious hacking data breach risks', *North American Actuarial Journal* **25**(4), 484–502.

Truong, C., Oudre, L. & Vayatis, N. (2020), 'Selective review of offline change point detection methods', *Signal Processing* **167**, 107299.

Wang, G., Gu, Z., Li, X., Yu, S., Kim, M., Wang, Y., Gao, L. & Wang, L. (2021), 'Comparing and integrating us covid-19 data from multiple sources with anomaly detection and repairing', *Journal of Applied Statistics* pp. 1–27.

Wang, J., Chaudhury, A. & Rao, H. R. (2008), 'Research notea value-at-risk approach to information security investment', *Information Systems Research* **19**(1), 106–120.

Wang, Q.-H. & Kim, S. H. (2009*a*), Cyber attacks: Cross-country interdependence and enforcement, WEIS.

Wang, Q.-H. & Kim, S.-H. (2009*b*), Cyber attacks: Does physical boundary matter?, AIS.

Wheatley, S., Hofmann, A. & Sornette, D. (2021), 'Addressing insurance of data breach cyber risks in the catastrophe framework', *The Geneva Papers on Risk and Insurance-Issues and Practice* **46**(1), 53–78.

Wheatley, S., Maillart, T. & Sornette, D. (2016), 'The extreme risk of personal data breaches and the erosion of privacy', *The European Physical Journal B* **89**(1), 1–12.

Woods, D. W. & Böhme, R. (2021), Systematization of knowledge: Quantifying cyber risk, *in* 'IEEE Symposium on Security & Privacy'.

Woods, D. W., Moore, T. & Simpson, A. C. (2021), 'The county fair cyber loss distribution: Drawing inferences from insurance prices', *Digital Threats: Research and Practice* **2**(2), 1–21.

Zhang Wu, M., Luo, J., Fang, X., Xu, M. & Zhao, P. (2021), 'Modeling multivariate cyber risks: deep learning dating extreme value theory', *Journal of Applied Statistics* pp. 1–21.