Hindawi
International Journal of Mathematics and Mathematical Sciences
Volume 2022, Article ID 7689828, 20 pages
https://doi.org/10.1155/2022/7689828

Research Article

Cyber Loss Distribution Fitting: A General Framework towards Cyber Bonds and Their Pricing Models

Oleg Kolesnikov,[1] Alexander Markov,[1] Daulet Smagulov,[1] and Sergejs Solovjovs [2,3]

[1]*Econophysica Ltd., Annecy Court, Ferry Works, Summer Road, Thames Ditton, Surrey KT7 0QJ, UK*
[2]*Department of Mathematics, Faculty of Engineering, Czech University of Life Sciences Prague, Kamýcká 129, Prague 16500, Czech Republic*
[3]*Department of Mathematics, Faculty of Informatics and Statistics, Prague University of Economics and Business, Ekonomická 957, Prague 14800, Czech Republic*

Correspondence should be addressed to Sergejs Solovjovs; solovjovs@tf.czu.cz

Received 2 November 2022; Revised 10 December 2022; Accepted 12 December 2022; Published 31 December 2022

Academic Editor: Niansheng Tang

Copyright © 2022 Oleg Kolesnikov et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Motivated by the considerable amount of losses in (finance) industry caused every year by the fast growing number of malicious cyber events and the need of an insurance against such cyber losses, we propose a general framework of cyber bond, whose main purpose is to insure (compensate) losses of a cyber attack. Based on a database of publicly available cyber events, we determine cyber loss distribution parameters and use them to numerically simulate cyber bond price, yield, and other characteristics. We also study two approaches to cyber bond coupon calculation.

1. Introduction

Cybersecurity risk is an operational risk to information and technology assets that has consequences affecting the confidentiality, availability, or integrity of information or information systems [1]. The problem of cyber risk is highly relevant today, as hacking techniques advance rapidly (see, e.g., [2]). New ways of bypassing security and new methods of finding vulnerabilities emerge every year. The number of cyber incidents grows by 25% and the number of companies falling victim increases by 22% annually [3]. The outcomes of such incidents are reputational damage and/or material loss. More detail on the modern cyber attack techniques and their consequences can be found in, e.g., [4–7]. We emphasize that a technical discussion of these cyber attacks is off the scope of the present paper due to the lack of competence of the authors in this topic.

With the evolution of hacking methods, cybersecurity techniques are improving constantly. These techniques are aimed at preventing cyber incidents and safeguarding companies against potential threats. The problem, however, is that cyberattacks are very abrupt and modeling and predicting this type of risk is complicated. Since the dynamics of cyberattacks are random and varied, full protection against cyber risk cannot be guaranteed due to the impossibility of predicting the methods and goals of an attack and the constant evolution of cyber risk [8]. Besides, there is the so-called zero-day problem when some new hacking technique emerges and no methods of defending against it are available. Also, there is no single universal method of assessing organization cyber security. There are certain models (FAIR, IRAM, CyberVaR), Global Cybersecurity Index (GCI), and ISO 27000, but no general standards and ratings have been developed. Deficiencies in cyber security techniques, lack of observation data, and complexity of loss assessment are also the factors that inhibit the development of cyber risk defense products.

Since managing cyber risk is complicated, a new problem that needs to be solved emerges. Based in post-defense, the problem is to soften the effect of cyber incidents and try to benefit from them. One of the possible ways to handle the

conditions of the problem is to create a model of risk bonds for a corresponding event.

Event risk bonds are widely used today. An example of such securities make weather derivatives (see, e.g., [9–13]). This type of financial instruments can be used by organizations or individuals to prevent risk associated with adverse or unexpected weather conditions as stipulated in the contract. This security is an index-based instrument and uses weather observation data to create an index that a payout can be based on. Another type of such securities are catastrophe bonds, or cat bonds (see, e.g., [14–17]). This type of financial instruments helps insurance companies when a major catastrophe occurs. Such incidents may incur a huge amount of loss since the affected damage cannot be covered by investments [18]. Organizations release the above-mentioned cat bonds and pay a coupon to the investor if no catastrophe occurred. Otherwise, an insurance company can stop coupon payments and, in some cases, take out the principal and use the obtained resources to pay their claim holders.

Event risk bonds are usually risky. However, they have higher coupons. In case of an event stipulated in the corresponding contract, the trigger is turned on. Depending on the amount of loss and the conditions of the contract, the company can stop coupon payment and take out the contract notional, allowing the company to offset the potential losses caused by the corresponding event.

Motivated by the considerable amount of losses in (finance) industry caused every year by the above-mentioned fast growing number of malicious cyber events and thus the urgent need of some insurance against these cyber losses, we propose a general framework of cyber bond, whose main purpose is to insure (compensate) losses of a cyber attack. More precisely, in this paper, we explore the issue of cyber post-defense and suggest a new type of financial instruments where cyber incidents are the triggering events. Some organizations and banks already use such securities widely as operational risk bonds that include cyber risk into their scope. Investors though are interested in having a broad selection of securities: one wants more gain, another wants less risk. By restricting the scope of security risk factors to cyber risk only, we allow investors to get a less risky financial instrument, even though less profitable. In view of the rapid evolution of cyber risk, we expect that this type of contract will be highly demanded as a security. Stated differently, we strongly believe that our proposed cyber bonds could take a similar niche with respect to the insurance of cyber losses as the above-mentioned catastrophe or cat bonds took with respect to the insurance of catastrophe losses.

This paper is structured as follows. Section 2 presents our proposed general methodology of cyber bonds (e.g., their pricing) and provides a short cyber bond example. Section 3 considers cyber loss distribution fitting. More precisely, given a publicly available cyber event database, Section 3 provides the respective cyber loss frequency (interval length in days to the next loss) and cyber loss severity (actual loss amount) distributions and their parameters. The former appears to be exponential and the latter–log-normal. Finally, Section 4 provides an extensive example of a cyber bond and estimates its basic characteristics like, e.g., price, yield, etc. These characteristics appear to depend significantly on bond coupon and notional triggers, which determine whether bond coupons and notional are paid to the bondholder. Section 4 also considers two approaches to calculating bond coupons, based in probability of loss and bond par yield. It also studies the distributions of two specific event groups (cyber-related data breach and cyber-related fraud) and finds out that even though the loss severity for both groups follows the general cyber loss severity distribution (the log-normal one), the respective loss frequency is different, since it follows the non-central Fisher distribution instead of the exponential one.

The authors would also like to observe that a preprint of the paper has already appeared on "arXiv" [19], which is freely available to the general public.

2. Methodology of Cyber Risk Bonds

2.1. Preconditions and Concept. The general concept of event risk securities includes some trigger that stops coupon payments partially or completely. A trigger takes some factor into account and turns on when the factor surpasses a given threshold. For example, [20] describes the following basic trigger types:

(i) with an indemnity trigger, coupon payments are stopped and/or the principal (or its part) is recovered in case one or several base events have their loss amount exceeding the threshold;

(ii) with a modeled loss trigger, coupon payments are stopped in case one or several base events have their estimated loss amount exceeding some given threshold; besides, the estimation can be performed constantly, while the actual losses are determined sometime after the incident;

(iii) with triggers indexed to industry loss, coupon payments are stopped if the total amount of insurance industry losses reaches the given threshold, which is predefined by some competent authority;

(iv) a parametric trigger is related to an actual danger and turns on if the critical level of certain conditions is reached, e.g., wind speed or area of a forest fire;

(v) a hybrid trigger combines the features of several of the triggers above.

Operating principle of a trigger is illustrated in Figure 1. Not all of the trigger types above meet the requirements to be used with cyber risk securities. Today, estimation of loss immediately after a cyberattack is impossible. A certain amount of time is required to determine the damage after the incident. It follows then that indemnity and industry loss triggers cannot be used for our securities. Next, due to the unpredictability of cyberattacks, we have no parameters that can signify that a cyber incident is imminent or the probability of its occurrence increases. This makes the parametric trigger inappropriate for the current problem as well.

However, possible losses from a cyber incident can be modeled using, e.g., Monte Carlo simulation. Thus, the

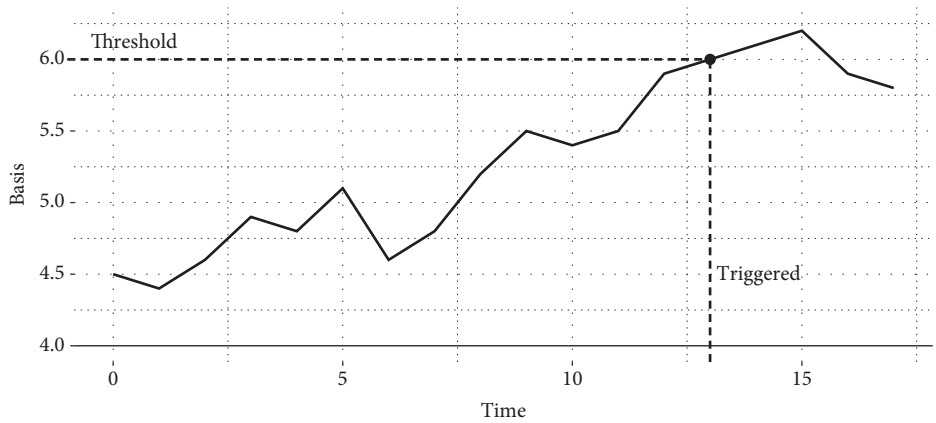

Figure 1: Trigger switches on if the basis exceeds the given threshold.

modeled loss trigger can be chosen for the model. Besides, the calculated threshold of expected losses should be specified in the contract.

Similarly to cat bonds, the structure of financial cyber risk instruments can be represented as follows. An issuer produces securities and takes the principal from an investor. According to the terms of the contract, the issuer then pays coupons to the investor with a given frequency unless the trigger is turned on. Also, the terms of the contract specify whether the principal should be forgiven. If the trigger is not activated for the whole time until the contract maturity, the investor takes all the coupons and the principal. The main problem is the calculation of a cyber risk contract price. The following chapter is dedicated to dealing with this problem.

2.2. Pricing Model. The classical approach to insurance securities pricing is to consider two distributions: distribution of events themselves and distribution of the periods between them. Throughout the paper, we will follow the same scheme generally, but certain specific features of cyber bonds in terms of pricing will be discussed.

In order to construct a procedure of pricing a contract, we have to.

(i) define the set of significant risk factors;

(ii) develop a model of the risk factors changing in time;

(iii) choose a pricing policy (fair value including risk premium, prudent valuation, etc.) and price valuation approach (analysis, Monte Carlo, or PDE solution).

We are going to consider the standard approach to pricing of event-linked securities, namely, fair value plus some risk premium.

The risk factor modeling used in the process of pricing is based in the following assumptions. The moments when cyber incidents of type k occur can be described using time intervals between the incidents, where each of the intervals follows the same probability distribution

$$P\left(\tau_{k,r} \leqslant y\right) = F_k(y), \tag{1}$$

in which $\tau_{k,r}$ is the interval of time between incidents r and $(r+1)$ of type k. Moreover, losses induced by cyber incident r can be described by the probability distribution law

$$P\left(\xi_{k,r} \leqslant x\right) = G_k(x). \tag{2}$$

Distributions $F_k(y)$ and $G_k(x)$ are assumed to be parametric, i.e.,

$$\begin{aligned} F_k(y) &= F_k(y;\theta), \\ G_k(x) &= G_k(x;\lambda), \end{aligned} \tag{3}$$

and model risk is limited to the uncertainty of values of parameter vectors θ and λ. This uncertainty is covered by confidence intervals

$$\begin{aligned} \theta &\in [\theta_l;\theta_u], \\ \lambda &\in [\lambda_l;\lambda_u]. \end{aligned} \tag{4}$$

The price of the contract is defined as the value of the fair price that is the best (maximum) in terms of parameters, where fair price is calculated analytically for linear contracts and using a Monte Carlo method for the nonlinear ones:

$$\text{Price} = \max_{\theta\in[\theta_l;\theta_u],\lambda\in[\lambda_l;\lambda_u]} \text{FairPrice}\left(F_k(\cdot) = F_k(\cdot;\theta); G_k(\cdot) = G_k(\cdot;\lambda)\right). \tag{5}$$

We would like to emphasize that there currently exist other approaches to cyber bonds as in, e.g., [21]. Generally, the underlying machinery of cyber bond pricing stems from the already well-developed technique of pricing the above-mentioned cat bonds. One can find a plentitude of cat bond pricing methodologies in the literature as in, e.g., [22]. In particular, the paper in question considers two distributions: the distribution of loss frequency, i.e., how often do

catastrophic events occur (an analogue of $F_k(y)$ in our case) and the distribution of loss severity, i.e., how much money do catastrophic events require to cover the incurred losses (an analogue of $G_k(x)$ in our case). The authors find the appropriate distribution laws (e.g., Poisson law for the loss frequency distribution and, e.g., log-normal law for the loss severity distribution) as well as estimate the corresponding distribution parameters. The respective pricing model then depends on the obtained distribution laws and their estimated parameters relying, moreover, on a risk-neutral probability measure. We roughly follow the same path, where FairPrice in our formula (5) is taken to be the standard coupon-bearing bond pricing formula (6) of Subsection 4.1 of the present paper stemming from, e.g., [23], [Subsection 14.7.2] (i.e., the sum of the discounted bond principal and the coupons). What is the role of $F_k(x)$ and $G_k(x)$ then?. They determine, whether the number and/or total loss of cyber events is such that one should stop coupon payment and/or forget the payment of the bond principal (decreasing thus the number of summands in the bond pricing formula). More detail on our bond pricing technique can be found in Subsection 4.1.

2.3. Numerical Results. For the purposes of our study, a Monte Carlo simulation of events and periods between them was carried out. Based in the distributions fitted below, the average price of a bond over a number of simulations was estimated. In addition, Greeks and coupon payment probabilities were calculated.

Our cyber risk security pricing model supports the following risk factors:

(i) change of a risk-free rate (risk factor to be taken into account while discounting and valuating the coupons in case it is linked to, e.g., LIBOR or SOFR);

(ii) the moment when a cyber incident happened;

(iii) aggregated financial losses (optional, can be considered as a single risk factor or a sum of separate risk factors by the source of loss: client payments, business process interruption, reputational loss, etc.);

(iv) risk of the "incorrect" valuation of the risk factors above (model risk, which is significant in case the securities are linked to cyber incidents (insurance or security) due to unavoidable difficulties in modeling).

Dependence of the bond value on a risk-free rate and distribution parameters (located on the bounds of confidence intervals) can be assessed using the values of the corresponding Greeks shown in Table 1.

Presented values are computed using the values of parameters given in Table 2.

Dependence of the resulting prices on maturity and trigger values is presented in the following figures.

Figures 2–4 show strong dependence of cyber bond price on triggers and maturity, since all the risk can be described by these parameters.

Table 1: Values of Greeks for 99% confidence intervals bounds.

Bound	$dS/d\lambda$	$dS/d\mu$	$dS/d\sigma$	dS/dr
Lower	−1.464	−10.444	−3.422	
Middle	−2.723	−11.484	−6.295	−2.62
Upper	−3.775	−27.568	−24.438	

Table 2: Other parameters used for Greeks calculation.

Parameter	Value
Number of MC iterations	5000
Trigger for coupons	\$5 billion
Trigger for face value	\$50 billion
Risk-free rate	2.65%
Coupon	30\$, every 182 days
Face value	1000\$
Maturity	5 years

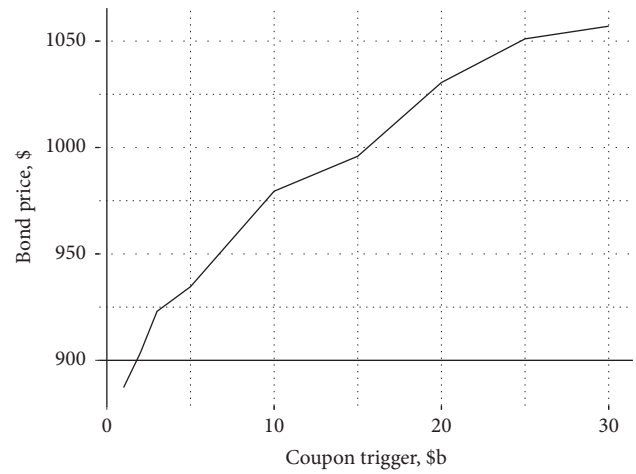

Figure 2: Cyber bond price vs. coupon trigger.

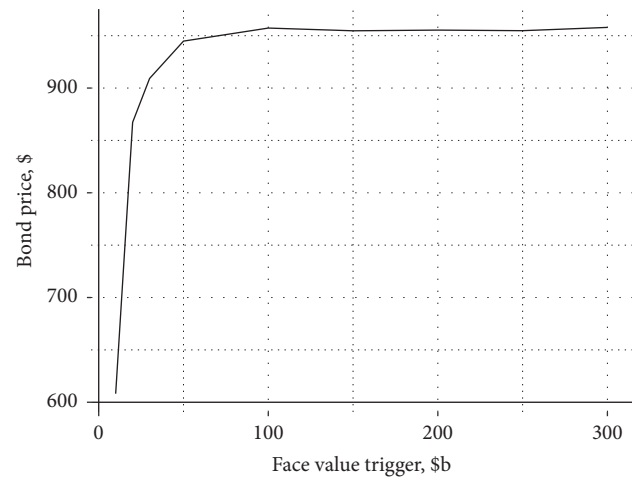

Figure 3: Cyber bond price vs. face value trigger.

Using parameters from Table 2, one can plot the probability of coupon payment, which is depicted in Figure 5.

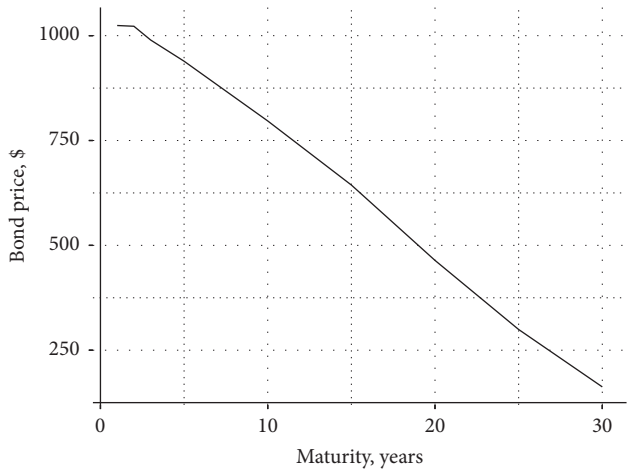

Figure 4: Cyber bond price vs. maturity.

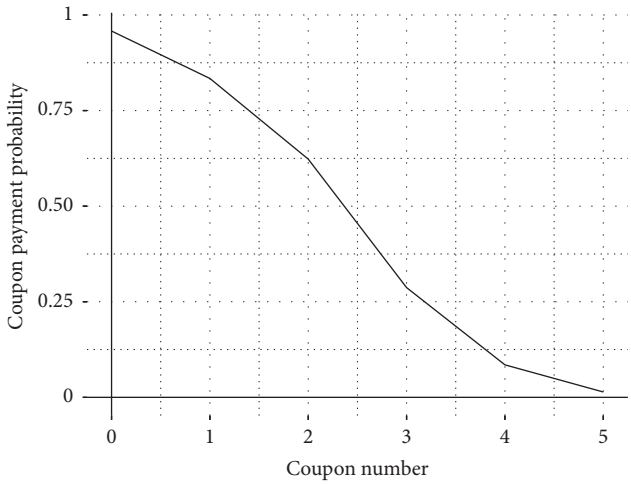

Figure 5: Probability of coupon payment.

Payment probabilities shown in Figure 5 display a low survival rate, though it strongly depends on a coupon trigger value.

3. Example of Distribution Fitting

3.1. Historical Data. According to the previous section, a cyber risk security price depends on the intervals of time between the incidents and the resulting material losses. In this section, we need to estimate the families of distributions $F_k(y|\theta)$ and $G_k(x|\lambda)$ and their parameters θ and λ, respectively. For this example of estimation, the historical data was downloaded from [3]. This data contains information about the cyberattacks and cyber incidents that happened within the period of 2017–2018. Histograms of the data are shown in Figure 6.

3.2. Estimation and Testing. From the histograms of Figure 6, we conclude that for the data of time series of both intervals and losses, we need to fit the distribution defined on a semi-infinite interval. It was also considered that the distribution of time intervals should be defined in the zero value. Thus, Weibull, gamma, χ^2, Fisher, and exponential distributions were selected for fitting.

The maximum-likelihood estimation procedure is performed to fit the distribution. The parameters are estimated using the Nelder–Mead method. The results and the corresponding standard error values are presented in Table 3.

Then, goodness-of-fit testing should be performed for each of the chosen distribution parameters. For this purpose, the Cramér–von Mises test is used [24]. We set the confidence level for the testing to 0.05. According to the results (Table 3), the exponential distribution fits our data better than the others. All tested probability distribution functions are represented in Figure 7.

Since we assume that cyber incidents always cause some non-zero material losses, we need to take a distribution that is not defined in the zero value. Also, the corresponding histogram shows that the data has heavy tails (the value close to $3 billion). The log-normal distribution meets all the requirements. In particular, [8] shows that the log-normal distribution fits losses data the best. The estimated parameters and goodness-of-fit test results are shown in Table 4. The test results show that this distribution satisfies the corresponding time series of losses. The results of fitting are shown in Figure 8. Note that the data is shown in a logarithmic scale, thus the log-normal probability distribution function visually looks like the normal distribution function.

3.3. Confidence Interval for Estimated Parameters. Following the idea of prudent valuation methodology [25], we need to calculate the confidence interval for the estimated parameters. The lower and upper bounds for the parameters were calculated at the 80%, 97%, 99%, and 99.9% confidence levels. The values are shown in Table 5.

4. Cyber Bond Example

4.1. General Example Setting. In this section, we consider an example of cyber bonds related to a concrete (and randomly chosen) cyber event. As follows from, e.g., [26] in February 2019, a Maltese bank (namely, Bank of Valletta) suffered a cyber attack which saw EUR13 million transferred out of the bank through false international transactions. In the wake of the above event, we assume that the bank wants to insure itself against such cyber attacks in the future. It recognizes though that concentrating on information technology security alone (even though it is an essential protection component) could not always be enough since cyber attacks are getting more sophisticated with time. Thus, as a possible additional preventive, one could issue cyber bonds to cover losses in the case of a successful cyber attack against the bank. We consider an example of such a cyber bond.

Motivated by the above-mentioned cyber attack loss, we will assume that the bond notional is set to $ 15 million (rounding the result of EUR/$ exchange). US dollars are chosen over euros for the specific Federal Reserve (FRED) databases used in the below bond-related calculations. The

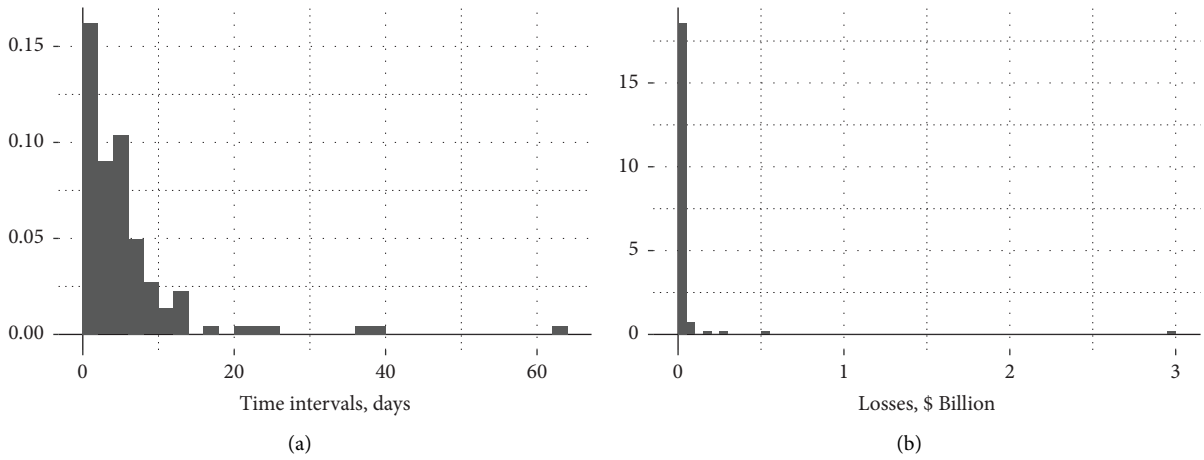

Figure 6: Input data histograms: time intervals between attacks (a) and losses (b).

Table 3: Parameter estimates, standard error, and test results of time interval distribution fitting.

Distribution	Parameters	Standard error	Statistic ω^2	P value
Weibull	$\lambda = 0.334$, $k = 4.07$	$\sigma_\lambda = 0.03$, $\sigma_k = 1.166$	3.94	<0.01
Gamma	$k = 0.233$, $\theta = 27.403$	$\sigma_k = 0.024$, $\sigma_\theta = 6.09$	29.58	<0.01
χ^2	$k = 1.02$	$\sigma_k = 0.087$	18.04	<0.01
Fisher	$d_1 = 0.392$, $d_2 = 1.334$	$\sigma_{d_1} = 0.044$, $\sigma_{d_2} = 0.298$	11.7	<0.01
Exponential	$\lambda = 0.156$	$\sigma_\lambda = 0.015$	0.23	0.22

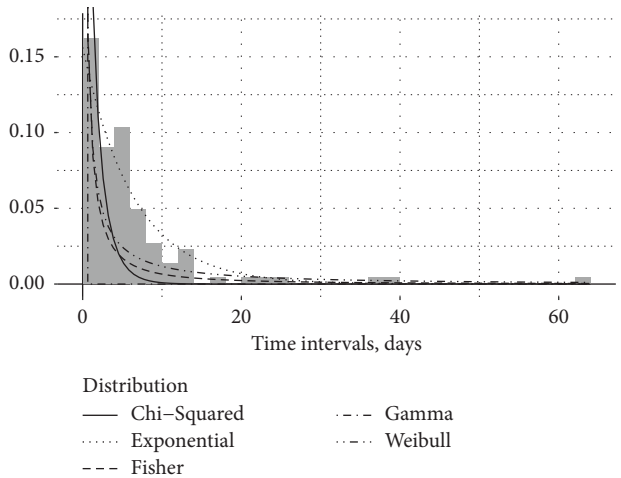

Figure 7: Probability distribution functions selected for time interval fitting.

Table 4: Parameter estimates and standard error for distributions of loss data.

Distribution	Parameters	Standard error	Statistic ω^2	P value
Log-normal	$\mu = 13.639$, $\sigma = 2.832$	$\sigma_\mu = 0.268$, $\sigma_\sigma = 0.189$	0.038	0.94

bond maturity will be chosen as 3 years (this reflects a time-changing cyber security risk as well as trims large numbers obtained for longer maturities). We assume that the bond pays a coupon every half a year. There could be up to 6 coupons (we will explain "could" in a moment) during the life of the bond. From the several possible cyber bond coupon calculation techniques, two of which are considered in Section 4.4, we choose the par yield approach (described in Section 4.4.2) and set bond coupon percentage to 5.09%, which amounts to \$764, 055.87. The funding rate for discounting during bond valuation is set to a 3-year Intercontinental Exchange (ICE) swap rate based on USD (taken from [27]) which equals 1.52% (as of August 15, 2019). The above characteristics of the cyber bond are summarized in Table 6.

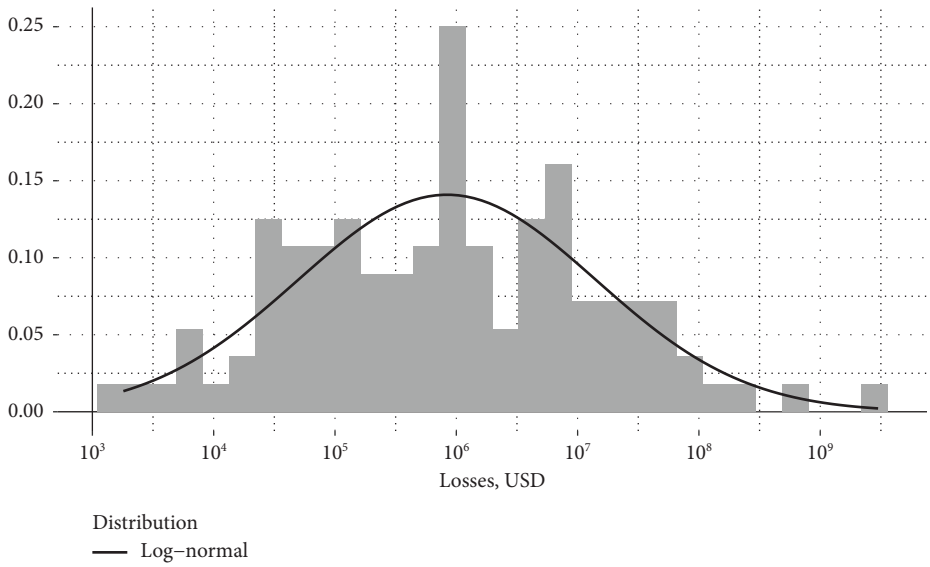

Figure 8: Probability distribution functions selected for loss fitting (logarithmic scale).

Table 5: Confidence interval for estimates.

Distribution	Parameter	Std. error	Bound	80%	97%	99%	99.9%
Exponential (time intervals)	$\lambda = 0.156$	$\sigma_\lambda = 0.015$	Lower	0.137	0.124	0.118	0.107
			Upper	0.175	0.188	0.194	0.205
Log-normal (losses)	$\mu = 13.639$	$\sigma_\mu = 0.268$	Lower	13.296	13.058	12.950	12.758
			Upper	13.982	14.220	14.328	14.519
	$\sigma = 2.832$	$\sigma_\sigma = 0.189$	Lower	2.589	2.421	2.344	2.209
			Upper	3.074	3.243	3.319	3.455

Table 6: Cyber bond parameters.

Bond parameter	Value
Notional	\$15 million
Maturity	3 years
Coupon rate	5.09%
Coupon value	\$764, 055.87
Funding rate	1.52%

We use the standard formula for bond price P:

$$P = \sum_{i=1}^{6} C \cdot e^{-R\cdot\left(d_i/365\right)} + N \cdot e^{-R\cdot(d/365)}, \tag{6}$$

where C is a coupon value, R is a funding rate, d_i (resp. d) is the date of the coupon payment (resp. Notional payment) in days, and N is the notional value. In our case, coupon payments are on days 182, 365, 547, 730, 912, and 1095. The last date also corresponds to the payment of the notional.

With formula (6) in mind, our cyber bond is assumed to be priced as follows. In the first step, one simulates cyber losses for the bond maturity period, i.e., 3 years. This simulation includes a day of the loss and its size (cyber loss distribution parameters will be discussed in a moment). In the second step, one uses two triggers, namely, notional and coupon trigger, to determine whether coupons and notional will be paid. More precisely, for every coupon (resp. notional) one sums up the simulated losses up to the respective payment day. If the losses are strictly less than the trigger, then the respective payment is made; otherwise not. This explains our "could" used to describe the number of coupons of our proposed cyber bond. These triggers are aimed to reflect the state of the industry with respect to cyber attacks. Coupon trigger is assumed to be less than the notional trigger and should define the first level of danger (payment of all or part of the coupons is therefore dropped). Notional trigger represents the second (and highest) level of danger when measures should be taken to compensate losses (payment of the notional is thus dropped). It should be noted, however, that the triggers of other nature are also possible. For example, one could possibly watch for the appearance of a certain number of events with certain losses. One could also watch for the events of a certain nature (e.g. current ransomware attacks) or a certain sequence of cyber events reflecting some pattern. These triggers will not be considered in this paper since they require a deeper and case-specific analysis of an available and comprehensive cyber event database.

4.2. Cyber Loss Distribution Parameters. A word is due to the distribution of cyber losses used in this section. Following the results of Section 3, we assume that cyber losses are characterized by two parameters, namely, the interval in days to the next loss and actual loss amount. Interval value is assumed to be distributed exponentially, whereas actual loss

value is assumed to have a log-normal distribution. The respective parameters together with the standard errors are given in Table 7.

We emphasize that the arrival times of the cyber events are modeled using the exponential distribution. This is similar to the distribution, which underlies models of traded credit instruments such as, e.g., credit default swaps (CDS) (see, e.g., [28]).

The parameters of Table 7 were calculated from our obtained table of publicly available cyber events. This table contains 328 items, with 136 of them having publicly disclosed loss amount. These events are ranging from the years 2009–2019. The motivating event for our considered cyber bond is taken from this table. The distribution parameters themselves were obtained through the maximum-likelihood method using Nelder–Mead and Broyden–Fletcher–Goldfarb–Shanno optimization algorithms for one- and two-parameter distributions, respectively. Moreover, to estimate the exponential distribution parameter λ, we made the next two preparatory steps with the available data:

(S1) The series of cyber event dates was modified to contain unique items only.

(S2) The series of interval lengths between two consecutive cyber events was modified to contain unique items only.

Table 8 shows the results of the goodness-of-fit (GOF) tests performed by us to justify the choice of cyber loss distribution and the respective distribution parameters (notice that the null hypothesis in each of the tests says that the true distribution is the one mentioned in the first column of Table 8 with the respective parameters taken from the second column of Table 8; to reject the null hypothesis with significance level of 5%, one searches a value less than 0.05 in the last column of Table 8).

Additionally, Figures 9 and 10 show the histograms of time interval (in days) to the next loss and actual loss amount, both with their assumed distributions.

Backed by the results of Table 8 (no rejected null hypothesis) and the visual inspection of Figures 9 and 10 (the proposed distributions are "reasonably" close to the histograms), we will rely on the cyber loss distributions and the parameters of Table 7 in the rest of the paper.

Finally, we do not claim to use the all-including table of losses since many cyber events are not publicly disclosed. We do believe, however, that this table is comprehensive enough to provide numerical estimations for our considered example of cyber bonds. Moreover, similar to [29], we do believe that there already exist enough available cyber event data for the successful treatment of cyber bonds.

4.2.1. Distribution of Cyber Losses of Specific Type. This section answers the question on whether all cyber event types in the used database follow the same distribution. More precisely, we single out two particular cyber event groups (namely, the two biggest ones in our database) and try to find their respective loss frequency (interval length in days to the next loss) and loss severity (actual loss amount) distributions. We will follow the distribution fitting steps of Section 3.

Table 7: Cyber loss distribution parameters.

Distribution	Parameters	Std. error
Exponential (number of days till the next loss)	$\lambda = 0.0211$	0.0029
Log-normal (actual loss amount)	$\mu = 14.9179$	0.2009
	$\sigma = 2.3434$	0.1421

(1) Cyber-Related Data Breaches. The first group contains cyber-related data breaches. We notice that this type of cyber events is extremely important for financial institutions often storing sensitive client data, which in their turn could be a lucrative target for cyber criminals. There are altogether 70 such events in our available database, with 12 of them having publicly disclosed loss amount.

We first concentrate on loss frequency distribution and its parameters. Table 9 shows possible loss frequency distributions of cyber-related data breach and their respective parameters with the standard errors (the reader may recall that we follow the fitting steps of Section 3 and, thus, the distributions).

The distribution parameters of Table 9 were obtained by the maximum-likelihood method using Nelder–Mead and Broyden–Fletcher–Goldfarb–Shanno optimization algorithms. The two preparatory steps from the beginning of Section 4.2 ((S1), (S2)) were taken to adjust available cyber event occurrence data.

Table 10 shows our performed GOF tests for the distributions of Table 9.

Based on the results of Table 10, namely, its last column, where the value below 0.05 leads to distribution rejection, we assume that the most suitable loss frequency distributions of cyber-related data breach are Fisher, Gamma, and Weibull with the respective parameters. After the visual inspection of Figure 11, which displays a cyber-related data breach loss frequency histogram and its assumed distributions, we conclude that the most suitable cyber-related data breach loss frequency distribution is Fisher with $d_1 = 0.66$, $d_2 = 2.0643$, and $\lambda = 10.3834$ (where, λ is non-centrality parameter).

We now pay attention to the loss severity distribution and its parameters. Tables 11 and 12 show cyber-related data breach loss severity distribution parameters with the standard errors and the respective GOF tests.

Based on the results of Table 12, namely, its last column, we assume that the log-normal distribution with the parameters $\mu = 15.6826$ and $\sigma = 2.6292$ is suitable for cyber-related data breach loss severity. This is confirmed by the visual inspection of Figure 12, which displays a cyber-related data breach loss severity histogram and its assumed distribution (notice that the number of events with publicly disclosed loss is small enough and, thus, the respective histogram has a rather awkward shape).

(2) Cyber-Related Fraud. The second group contains cyber-related fraud events, which are also an important issue for financial institutions (consider, e.g., credit card fraud or e-mail fraud; the latter is gaining in popularity more and more). There are altogether 96 such events in the available

Table 8: Cyber loss distribution GOF tests.

Distribution	Parameters	GOF test	Test statistic	P value
Exponential	$\lambda = 0.0211$	Chi-square	4.1698	0.8415
	$\lambda = 0.0211$	Kolmogorov–Smirnov	0.1138	0.4642
Log-normal	$\mu = 14.9179$ $\sigma = 2.3434$	Chi-square	7.3824	0.8313
	$\mu = 14.9179$ $\sigma = 2.3434$	Kolmogorov–Smirnov	0.057	0.7687

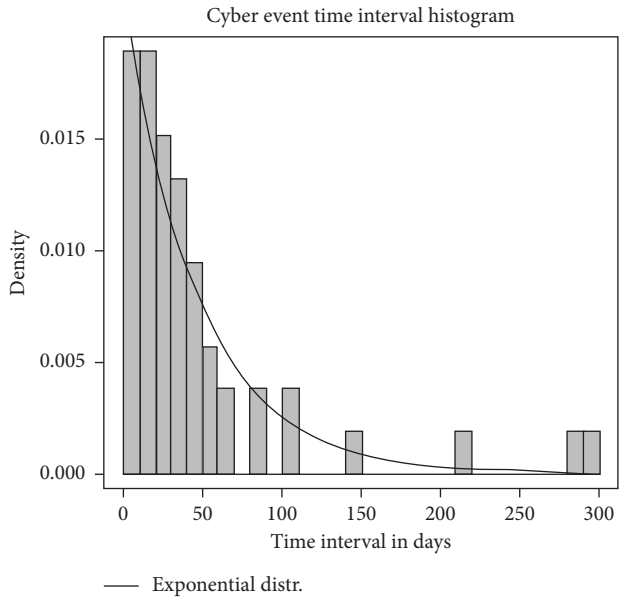

Figure 9: Histogram of time interval (in days) to the next loss and its assumed distribution.

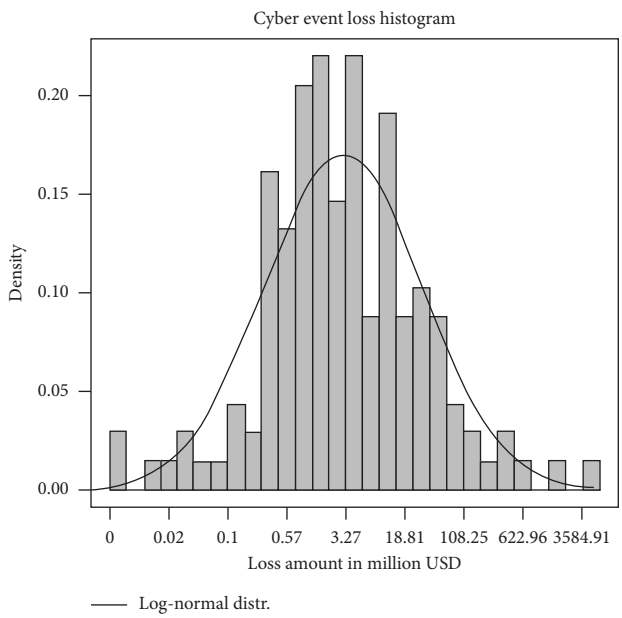

Figure 10: Histogram of actual loss amount and its assumed distribution.

Table 9: Cyber-related data breach loss frequency distribution parameters.

Distribution	Parameters	Standard error
Chi-square	$k = 24.475$	1.1423
Exponential	$\lambda = 0.0151$	0.0025
Fisher	$d_1 = 0.66$	0.4092
	$d_2 = 2.0643$	0.6131
	$\lambda = 10.3834$	4.3761
Gamma	$\alpha = 0.5979$	0.1179
	$\beta = 0.0091$	0.0026
Weibull	$k = 0.6912$	0.0832
	$\lambda = 48.5039$	12.4018

Table 10: Cyber-related data breach loss frequency distribution of GOF tests.

Distribution	Parameters	GOF test	Test statistic	P value
Chi-square	$k = 24.475$	Chi square	59.5	0.0000
	$k = 24.475$	Kolmogorov–Smirnov	0.3479	0.0002
Exponential	$\lambda = 0.0151$	Chi square	12.5	0.0853
	$\lambda = 0.0151$	Kolmogorov–Smirnov	0.2743	0.0069
Fisher	$d_1 = 0.66$ $d_2 = 2.0643$ $\lambda = 10.3834$	Chi square	1.5	0.9927
	$d_1 = 0.66$ $d_2 = 2.0643$ $\lambda = 10.3834$	Kolmogorov–Smirnov	0.0521	0.9999
Gamma	$\alpha = 0.5979$ $\beta = 0.0091$	Chi square	9.5	0.1473
	$\alpha = 0.5979$ $\beta = 0.0091$	Kolmogorov–Smirnov	0.1852	0.149
Weibull	$k = 0.6912$ $\lambda = 48.5039$	Chi square	6	0.4232
	$k = 0.6912$ $\lambda = 48.5039$	Kolmogorov–Smirnov	0.1385	0.4538

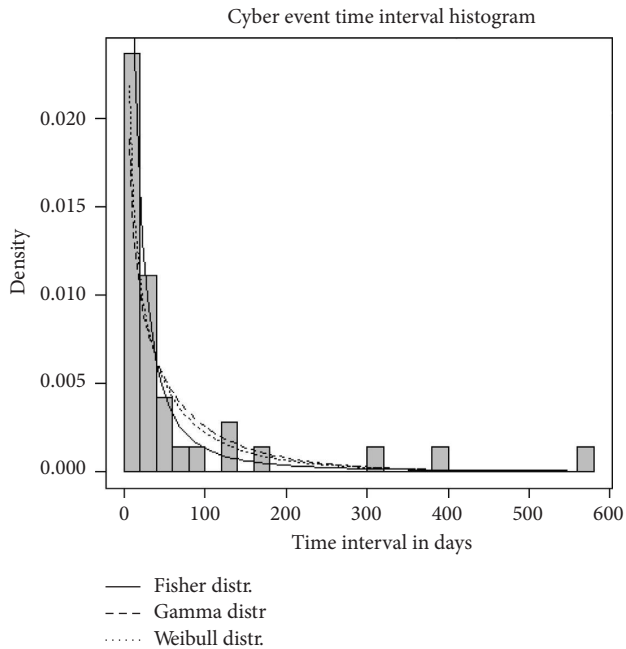

Figure 11: Cyber data breach loss frequency histogram and its assumed distributions.

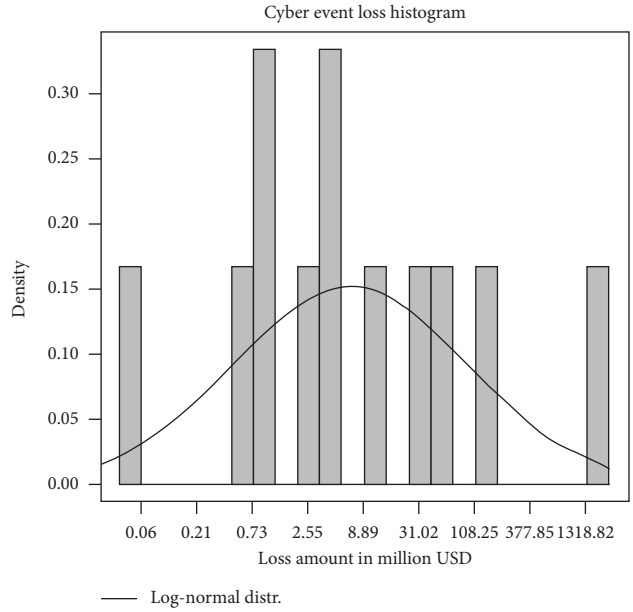

Figure 12: Cyber data breach loss severity histogram and its assumed distribution.

Table 11: Cyber-related data breach loss severity distribution parameters.

Distribution	Parameters	Standard error
Log-normal	$\mu = 15.6826$	0.759
	$\sigma = 2.6292$	0.5367

Table 12: Cyber-related data breach loss severity distribution of GOF test.

Distribution	Parameters	GOF test	Test statistic	P value
Log-normal	$\mu = 15.6826$ $\sigma = 2.6292$	Chi square	2	0.5724
	$\mu = 15.6826$ $\sigma = 2.6292$	Kolmogorov–Smirnov	0.1416	0.9424

database, with 69 of them having publicly disclosed loss amount.

We first study loss frequency distribution and its parameters. Table 13 shows possible cyber-related fraud loss frequency distributions and their respective parameters together with the standard errors.

The distribution parameters of Table 13 were obtained through the maximum-likelihood method with the two above-mentioned optimization algorithms. The preparatory steps of Section 4.2 ((S1), (S2)) were taken to adjust the available cyber event occurrence data.

Table 14 shows GOF tests for the distributions of Table 13.

Based on the results of Table 14, namely, its last column, where the value below 0.05 leads to distribution rejection, we assume that the most suitable cyber-related fraud loss frequency distributions are Fisher, Gamma, and Weibull. After the visual inspection of Figure 13, a displaying cyber-related data breach loss frequency histogram and its assumed distributions, we conclude that the most suitable cyber-related fraud loss frequency distribution is Fisher with $d_1 = 0.6983$, $d_2 = 2.5158$, and $\lambda = 10.4261$ (non-centrality parameter).

Table 13: Cyber-related fraud loss frequency distribution parameters.

Distribution	Parameters	Standard error
Chi-square	$k = 21.0688$	1.0713
Exponential	$\lambda = 0.0182$	0.0031
Fisher	$d_1 = 0.6983$	0.4044
	$d_2 = 2.5158$	0.8009
	$\lambda = 10.4261$	4.2168
Gamma	$\alpha = 0.6109$	0.1226
	$\beta = 0.0111$	0.0033
Weibull	$k = 0.6983$	0.0811
	$\lambda = 39.494$	10.1437

We now concentrate on the loss severity distribution and its parameters. Tables 15 and 16 show cyber-related fraud loss severity distribution parameters with the standard errors and the respective GOF tests.

Based on the results of Table 16 (namely, its last column), we assume that the log-normal distribution with the parameters $\mu = 14.6305$ and $\sigma = 2.4582$ is suitable for cyber-related fraud loss severity. This is confirmed by the visual

Table 14: Cyber-related fraud loss frequency distribution of GOF tests.

Distribution	Parameters	GOF test	Test statistic	P value
Chi-square	$k = 21.0688$	Chi square	56.2857	0.0000
	$k = 21.0688$	Kolmogorov–Smirnov	0.2839	0.0055
Exponential	$\lambda = 0.0182$	Chi square	11.0286	0.1374
	$\lambda = 0.0182$	Kolmogorov–Smirnov	0.2634	0.0124
Fisher	$d_1 = 0.6983$ $d_2 = 2.5158$ $\lambda = 10.4261$	Chi square	1.2571	0.996
	$d_1 = 0.6983$ $d_2 = 2.5158$ $\lambda = 10.4261$	Kolmogorov–Smirnov	0.048	1
Gamma	$\alpha = 0.6109$ $\beta = 0.0111$	Chi square	8.4571	0.2065
	$\alpha = 0.6109$ $\beta = 0.0111$	Kolmogorov–Smirnov	0.1846	0.162
Weibull	$k = 0.6983$ $\lambda = 39.494$	Chi square	9.4857	0.148
	$k = 0.6983$ $\lambda = 39.494$	Kolmogorov–Smirnov	0.1291	0.5602

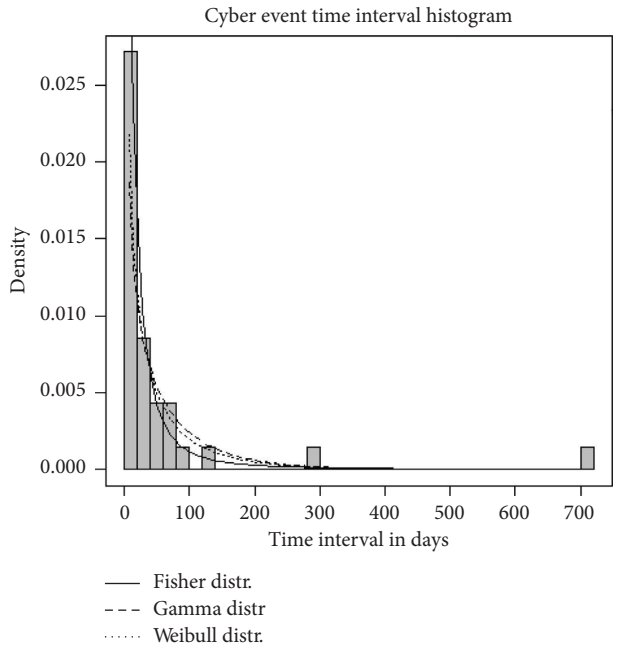

Figure 13: Cyber fraud loss frequency histogram and its assumed distributions.

Table 15: Cyber-related fraud loss severity distribution parameters.

Distribution	Parameters	Standard error
Log-normal	$\mu = 14.6305$	0.2959
	$\sigma = 2.4582$	0.2093

Table 16: Cyber-related fraud loss severity distribution GOF test.

Distribution	Parameters	GOF test	Test statistic	P value
Log-normal	$\mu = 14.6305$ $\sigma = 2.4582$	Chi square	9.5942	0.2947
	$\mu = 14.6305$ $\sigma = 2.4582$	Kolmogorov-smirnov	0.0993	0.504

inspection of Figure 14, which displays a cyber-related fraud loss severity histogram and its assumed distribution.

In conclusion, we shall notice that even though loss severity for both the initial database and two checked event groups can be assumed to follow log-normal distribution, loss frequency distribution for the initial (exponential) database differs from that of the two considered event groups (non-central Fisher). Therefore, a particular attention to the loss frequency distribution should be paid, when working with cyber events of a specific type.

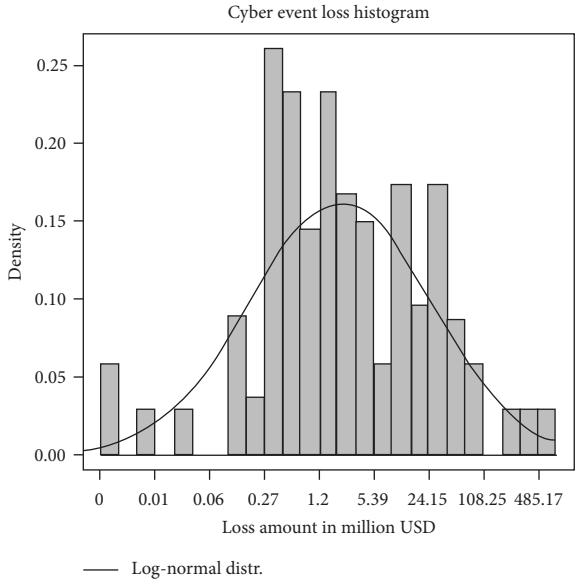

Figure 14: Cyber fraud loss severity histogram and its assumed distribution.

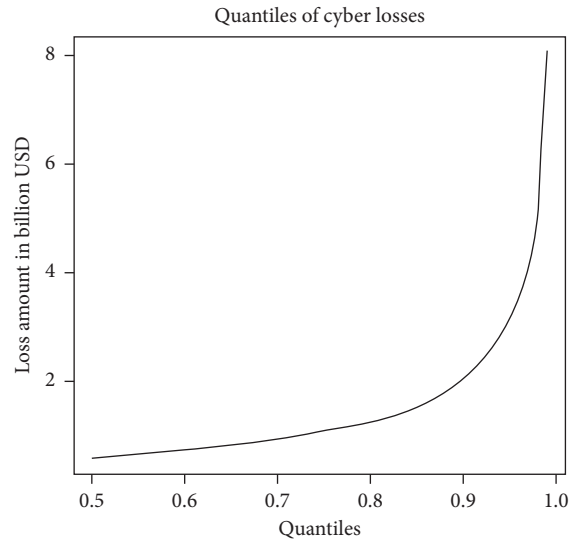

Figure 15: Quantiles of cyber losses for the period of 3 years.

4.3. Cyber Bond Numerical Results. This subsection lists the obtained numerical results on our proposed cyber bond example. We rely on Monte Carlo simulations, with the simulation number always being 5,000.

Figure 15 represents quantiles of losses for the maturity period of the cyber bond, that is, 3 years. The quantiles are calculated from Monte Carlo simulations. As can be seen from Figure 15, using our generated loss distribution parameters, the losses can reach the level of billion. We use these obtained loss amounts to test the influence of bond coupon and notional triggers on the actual bond parameters (e.g., price, yield, etc.).

We have already mentioned that a bond coupon trigger can influence the number of paid coupons on the bond. We now calculate a bond coupon survival curve. As

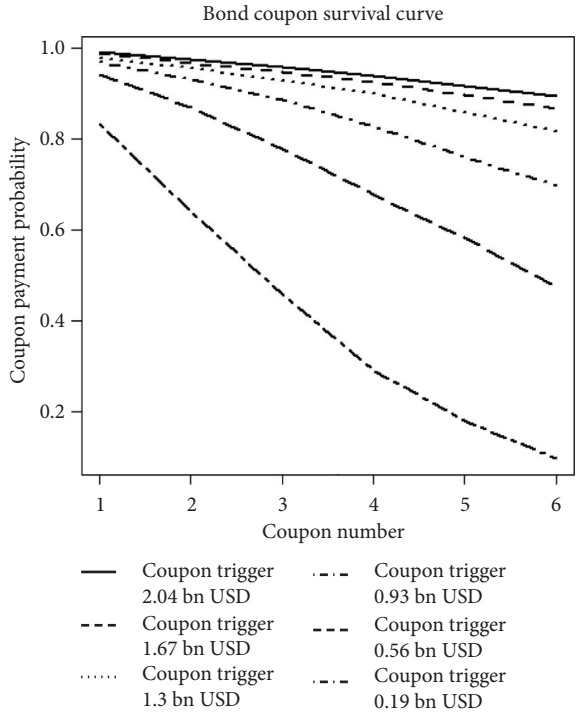

Figure 16: Cyber bond coupon survival curve for 3 years.

we mentioned before, the bond is assumed to pay a coupon every 6 months. Thus, altogether there are 6 coupons. Figure 16 shows the probability of the payment of each coupon depending on the coupon trigger. Recall that a coupon is not paid as soon as the total losses up to the coupon payment date exceed a specific amount (bond coupon trigger). Coupon payment probability is calculated as follows. In the first step, Monte Carlo simulations give a series or 0 s and 1 s depending on whether the respective coupon was paid or not. In the second step, one calculates the probability of coupon payment as the number of 1 s divided by the number of simulations. As can be seen from Figure 16, the coupon trigger of $2.04 billion, which corresponds to about 90% quantile as per Figure 15, gives a "reasonable" coupon payment probability close to 1. The lines in Figure 16 correspond to 10% –90% loss quantiles with the uniform step chosen between them.

Similar to the coupon survival curve, we now show a notional survival curve for our proposed cyber bond. As mentioned before, the bond notional is paid back provided that the total loss up to the payment date does not exceed the bond notional trigger. Figure 17 shows the probability of a notional payment for different notional triggers. The calculation methodology follows the one for the bond coupons. Notional triggers correspond to loss 10%–99% quantiles. Following Figures 15 and 17, losses above $ 2 billion (i.e., above 90% quantile) show a "reasonable" notional payment probability (above 90% as per Figure 17). In general, it is up to a risk-taker to decide which notional payment probability and, therefore, which notional trigger to choose for the issue of a cyber bond.

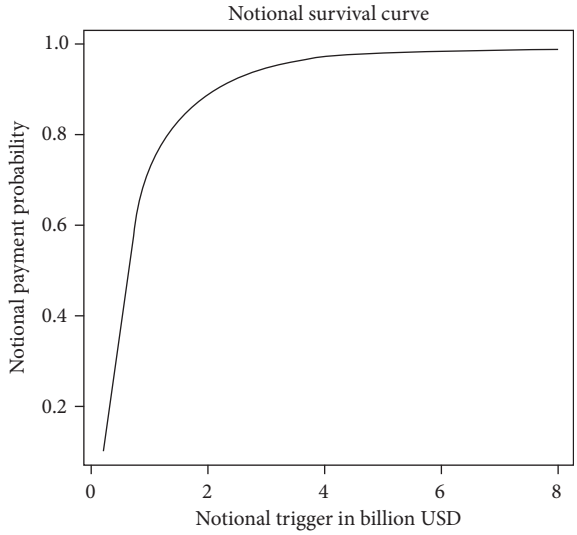

Figure 17: Cyber bond notional survival curve for 3 years.

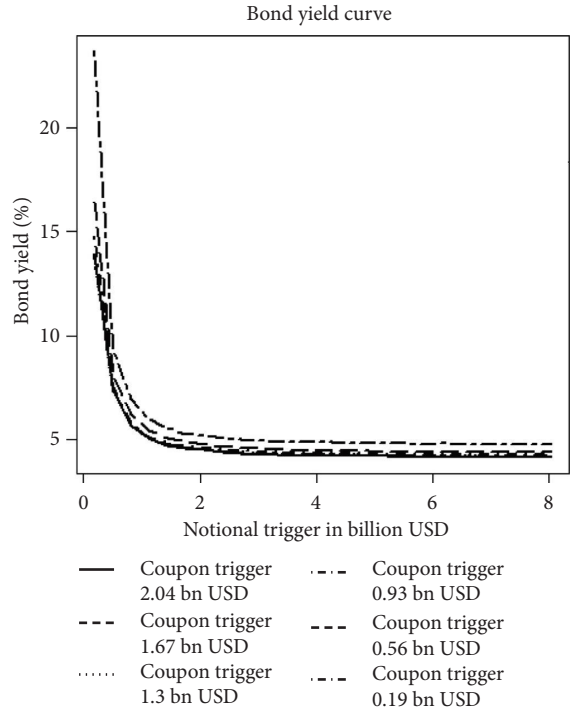

Figure 18: Cyber bond yield curve.

In the next step, we are going to show our proposed cyber bond yield curve, which allows one to judge the profitability of the proposed bond. A bond yield Y is calculated by the following formula:

$$Y = \frac{C}{P} \cdot 100\%, \tag{7}$$

where C is the bond coupon and P is the bond price. Figure 18 shows a cyber bond yield curve depending on both notional as well as coupon triggers. At least two things can be seen from the figure. First, a bond yield is not much influenced by a coupon trigger except for very small notional and coupon triggers. Second, starting from the notional trigger of about billion (corresponding roughly to 90% quantile as per Figure 15), the bond yield stabilizes around 5% with the exception of a relatively small coupon trigger of billion, for which the yield stays strictly above 5%, i.e., almost triples our assumed funding rate.

For the reader's convenience, Figure 19 shows our proposed cyber bond yield spread, i.e., the difference between the cyber bond yield and the funding rate used in the bond estimate (recall that the assumed funding rate amounts to 1.52%) depending on both coupon and notional triggers. As can be seen from the figure, the benefit of investing into our proposed cyber bond is about 3% (under "reasonable" assumptions on bond triggers).

Finally, we present our proposed cyber bond price curve. Figure 20 shows that for "reasonable" coupon and notional triggers the bond price stabilizes somewhere around \$ 17 million. We notice that the standard bond price (calculated by formula (6)), i.e., omitting both a coupon and a notional trigger, is \$18, 797, 813.26.

4.4. Cyber Bond Risk Premium. This section considers several approaches to calculating our proposed cyber bond risk premium, namely, a bond coupon, to account for possible coupon (or even the notional itself) loss. It is up to the ultimate issuer of the cyber bond to choose the most suitable technique or invent a new one if necessary.

4.4.1. First Alternative: Probability of Loss. As the first approach to calculating cyber bond coupons, we take the analogy of catastrophe bonds (cat bonds for short) studied in, e.g., [30], since a cyber attack could be considered as a kind of catastrophe. A general coupon calculation formula for cat bonds can be written as follows:

$$\text{Couponrate}(\%) = \text{LIBOR}(\%) + \text{Riskpremium}(\%), \tag{8}$$

where the risk premium should hedge the exposure of investors (into the bonds) to catastrophe risk (notice that following the current trend (see, e.g., [31]), LIBOR rate could be replaced by an alternative reference rate (ARR)). The above-mentioned risk premium could be then determined as follows:

$$\begin{aligned}\text{Riskpremium}(\%) = {} & \text{Constant}(\%) \\ & + \text{Lossmultiplier} \cdot \text{Expectedloss}(\%),\end{aligned} \tag{9}$$

where the expected loss is a percentage of the notional expected to be lost during the bond maturity period, the constant is the rate of return requested by investors, and the loss multiplier reflects the uncertainty related to the expected loss. For example, following the results of [30], [p. 1491], which are based on catastrophe bonds issued during the years 2006–2012 and covering earthquake risks, the constant amounts to 3.35% and the multiplier amounts to 1.4817. Additionally, as follows from the results of [32], [p. 168] based on the US catastrophe bonds issued during the years 1998–2008 and covering wind risks, the constant (resp. multiplier) amounts to 3.33% (resp. 2.4).

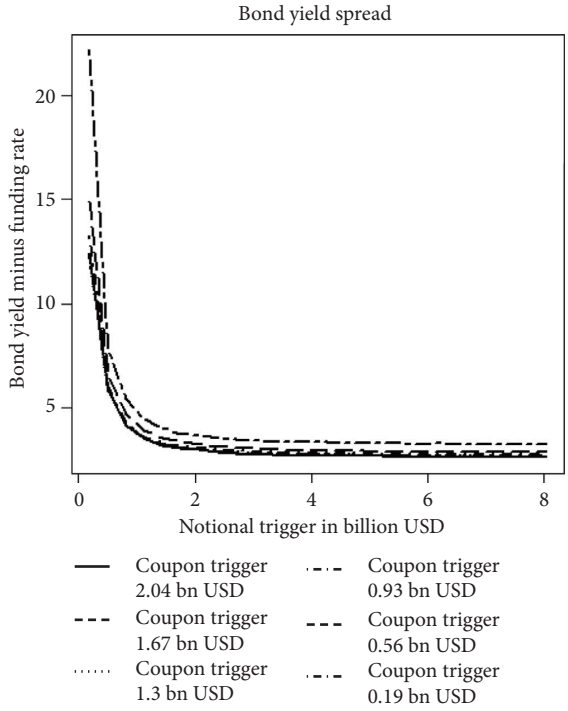

Figure 19: Cyber bond yield spread.

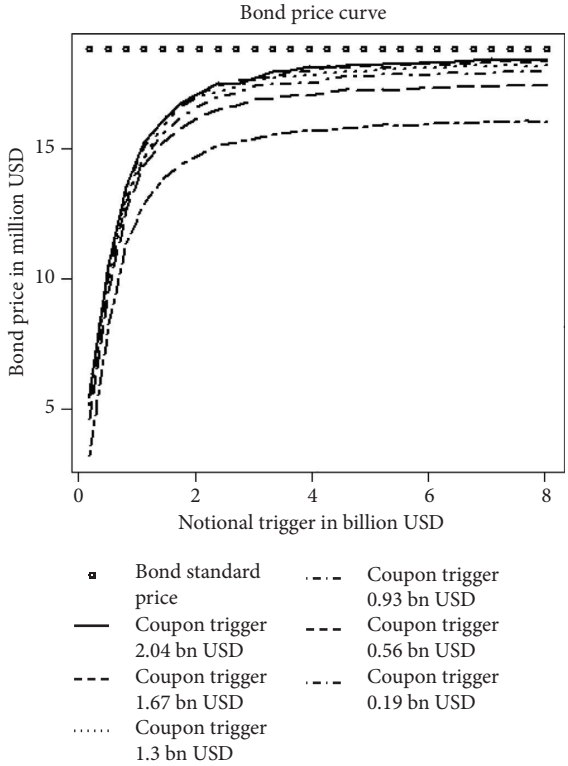

Figure 20: Cyber bond price curve.

To simplify the setting, we assume that the constant (the loss multiplier, respectively) in formula (9) is equal to 0 (resp. 1) since these parameters are highly dependent on investors. Moreover, following [15], [p. 817], we assume that expected loss EL is related to probability of loss PL and percentage of notional lost PNL given the loss occurs as follows:

$$\mathrm{EL}(\%) = \mathrm{PL} \cdot \mathrm{PNL}(\%). \tag{10}$$

In our cyber bond setting, PNL always amounts to 100%, since the notional is either paid back or not paid at all (cases of the partial repayment of the bond notional, despite the fact that they are possible, are not considered in this paper). Thus, in our considered case of cyber bonds, formula (8) simplifies to

$$\mathrm{Couponrate}(\%) = \mathrm{LIBOR}(\%) + \mathrm{PL}(\%). \tag{11}$$

Moreover, it is clear that PL of our proposed cyber bond depends on the notional trigger. The lower is the trigger, the more probable it is that the notional will not be paid back. Since this paper does not specify a specific trigger but rather considers trigger influence on bond characteristics, we calculated the average probability of not getting back notional from the notional survival curve of Figure 17. Thus, we obtain 11.58% (notice that according to [30], [p. 1490], for catastrophe bonds issued during the years 1999–2012 and covering earthquake risks, mean, maximum, and minimum risk premiums are 5.63%, 14.5%, and 1.5%, respectively, with the standard deviation being 2.70%. Therefore, our obtained number is in line with, e.g., earthquake risk). The average was taken over all the loss quantiles considered in the figure (see Section 4.3 for more details). For convenience of the reader, Figure 21 shows PL for different notional triggers. As can be seen from the figure, for low notional triggers PL could exceed 80%.

Altogether, taking into account that 6-month LIBOR on USD (taken from, e.g., [27] on August 15, 2019) is 2.05% and that our proposed cyber bond pays a coupon every 6 months, the total bond coupon resulting from the first coupon calculation technique (i.e., according to formula (11)) is 13.63%.

4.4.2. Second Alternative: Par Yield. As the second approach to cyber bond coupon calculation, we consider the concept of a bond par yield. Recall from, e.g., [33], [p. 85] that a bond par yield is a coupon rate for which the bond price equals its par value, namely, the notional value. It is easy to see (taking into consideration formula (6)) that the bond coupon C for par yield can be calculated as follows (keeping in mind that N is bond notional):

$$C = \frac{N \cdot \left(1 - e^{-R \cdot (d/365)}\right)}{\sum_{i=1}^{6} e^{-R \cdot \left(d_i/365\right)}}. \tag{12}$$

The respective par yield PY is then derived as

$$\mathrm{PY} = \frac{C}{N} \cdot 100\% = \frac{\left(1 - e^{-R \cdot (d/365)}\right)}{\sum_{i=1}^{6} e^{-R \cdot \left(d_i/365\right)}} \cdot 100\%. \tag{13}$$

The obtained par yield PY is then set to be the bond coupon rate.

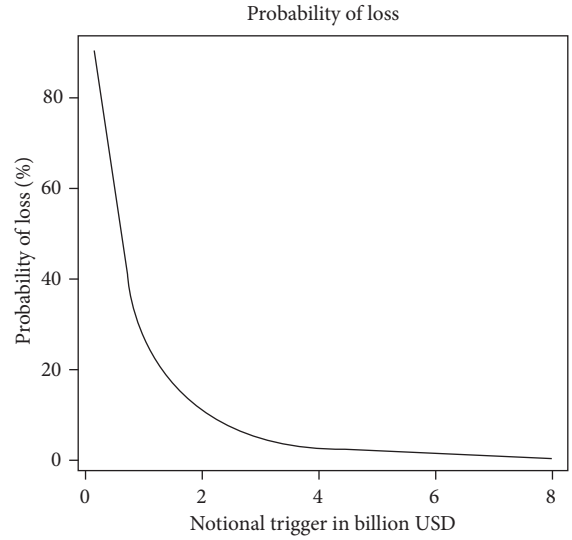

Figure 21: Cyber bond probability of loss for the period of 3 years.

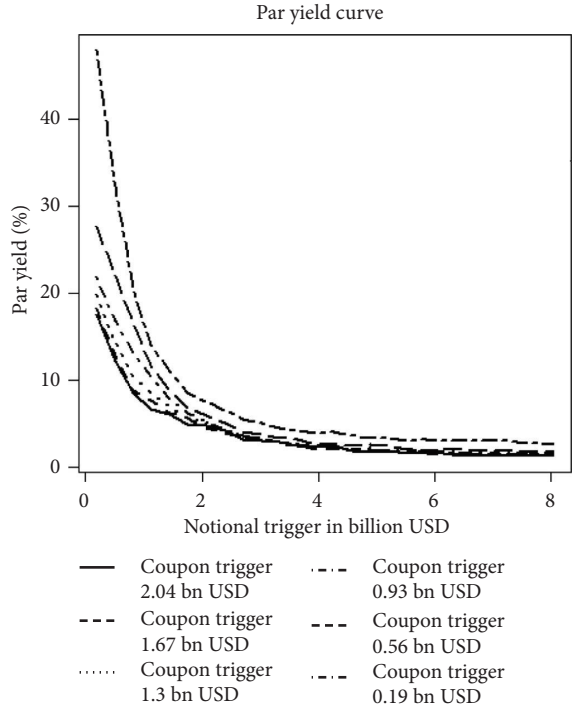

Figure 22: Cyber bond par yield curve.

In the case of our proposed cyber bond, some of the coupons and even the notional itself may not be paid back to the bondholder, which depends on the actual cyber losses. Thus, we first simulate cyber losses for the bond maturity period and then calculate cyber bond PY by formula (13), where now some of $e^{-R\cdot(d_i/365)}$ and even $e^{-R\cdot(d/365)}$ may be taken 0 depending on whether the respective item is paid to the bondholder or not.

Figure 22 shows the obtained par yield curves depending on both notional and coupon triggers. Since none of the triggers (both depending on the actual bond issuer) is fixed in this paper, we calculate the final coupon percentage as the average par yield over all the obtained curves getting thus 5.09% (recall from Section 4.1 that this amounts to as per assumed bond notional of million).

In order to be more aggressive in bond coupons, one could increase the parameters of Table 7, namely, the loss frequency (severity) parameter λ (resp. μ). As an example, Figures 23 and 24 show par yield curves for 25% (resp. 5%) increase of λ (resp. μ) value. The resulting cyber bond par yields are then 6.52% and 10.92%, respectively. One could tune both parameters increase according to the needs of the bond issuer. It is also easy to see that the unreasonable increase of the loss severity parameter μ could badly influence a bond coupon rate (namely, in the current cyber bond setting, 5% increase of μ almost doubles the coupon rate obtained through 25% increase of λ).

Notice that increasing the cyber loss frequency or severity parameter will influence other cyber bond characteristics as well. For example, Figures 25–27 show cyber bond spreads (namely, bond coupon percentage minus funding rate) for initial λ and μ as well as their increased values for 25% and 5%, respectively.

Additionally, Figures 28 and 29 show the bond notional survival curves for loss frequency (λ) and loss severity (μ) in the intervals $\lambda \pm \lambda \cdot 25\%$ and $\mu \pm \mu \cdot 5\%$, respectively. It can be easily seen from Figure 29 that 5% loss severity parameter increase visibly reduces notional payment probability with the set of current possible notional triggers.

Finally, Figures 30 and 31 show the probability of (notional) loss PL for different notional triggers for loss frequency (λ) and loss severity (μ) in the intervals $\lambda \pm \lambda \cdot 25\%$ and $\mu \pm \mu \cdot 5\%$, respectively. These two figures just mirror the results of Figures 28 and 29.

4.5. Simple Result Analysis. The numerical results of Section 4.3 show that the choice of notional and in some cases, coupon trigger could significantly influence our proposed cyber bond parameters. For example, as follows from Figure 18, under the small notional and coupon triggers, the cyber bond yield could reach double-digits. Such a high bond yield, however, comes from a rather low bond price as per Figure 20. It is additionally influenced by the bond risk premium, which should be tuned to the needs of a specific investor. Under the "reasonable" notional and coupon triggers, as follows from Figure 19, the benefit of investing into our proposed cyber bond over relying on the funding rate is about 3%. Since we propose a general cyber bond framework only, it is up to the actual risk-taker to decide which notional and coupon trigger should be deemed reasonable. Moreover, other trigger types (instead of just summing up losses up to a certain date) could be explored in case it is necessary for the bond issuer as mentioned at the end of Section 4.1.

The two techniques to calculate a cyber bond coupon rate considered in Section 4.4 could provide an entry point for the actual calculations done by the bond issuer. The expected loss approach (taken from the setting of cat bonds) provides a higher coupon rate in comparison with the par yield approach (13.63% versus 5.09%, respectively). The latter

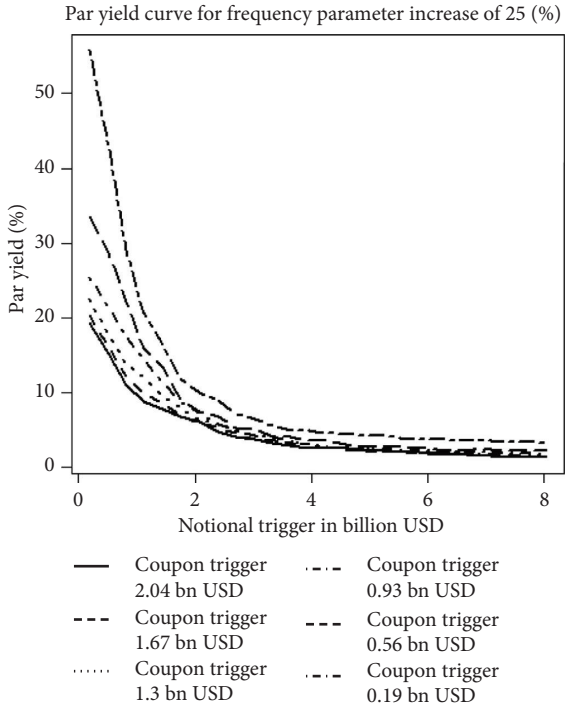

Figure 23: Cyber bond par yield curve for loss frequency parameter λ increase of 25%.

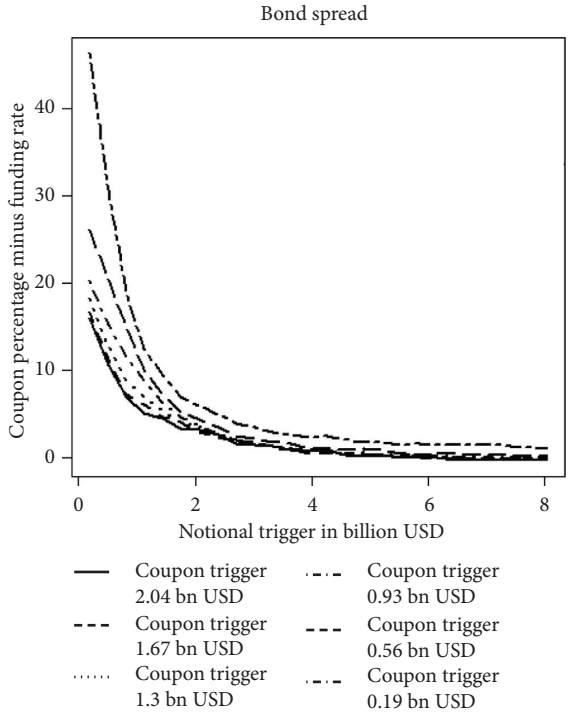

Figure 25: Cyber bond spread.

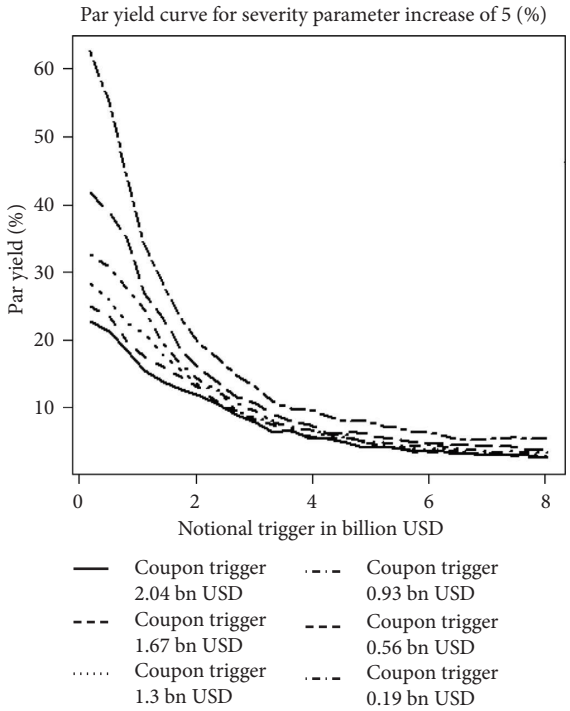

Figure 24: Cyber bond par yield curve for loss severity parameter μ increase of 5%.

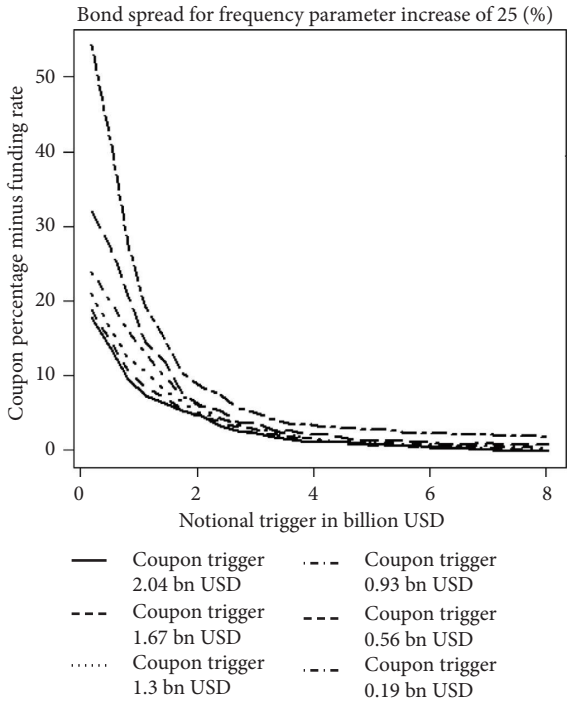

Figure 26: Cyber bond spread for loss frequency parameter λ increase of 25%.

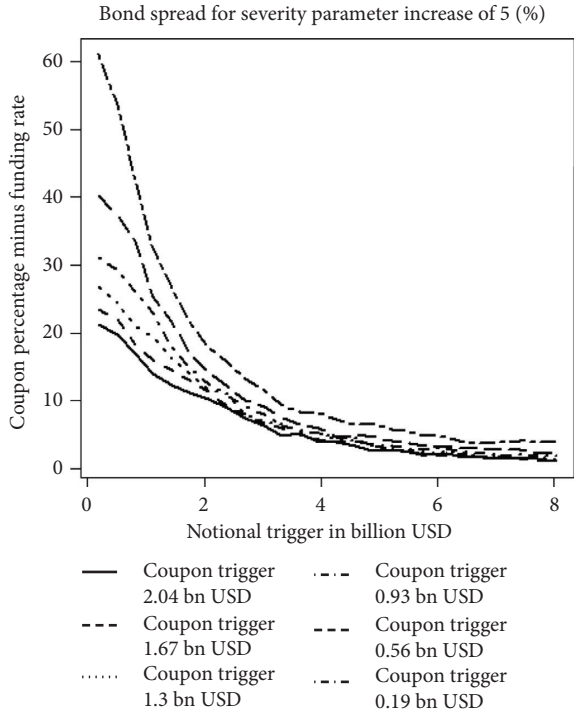

Figure 27: Cyber bond spread for loss severity parameter μ increase of 5%.

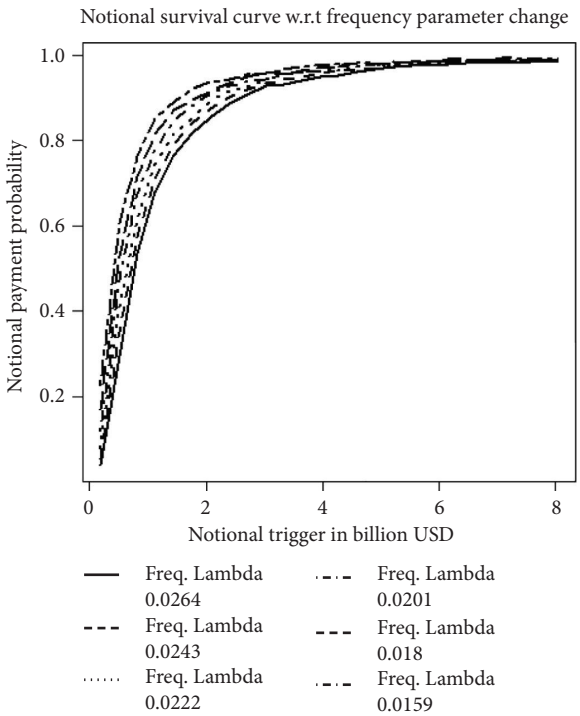

Figure 28: Cyber bond notional survival curve for 3 years for λ in the interval $\lambda \pm \lambda \cdot 25\%$.

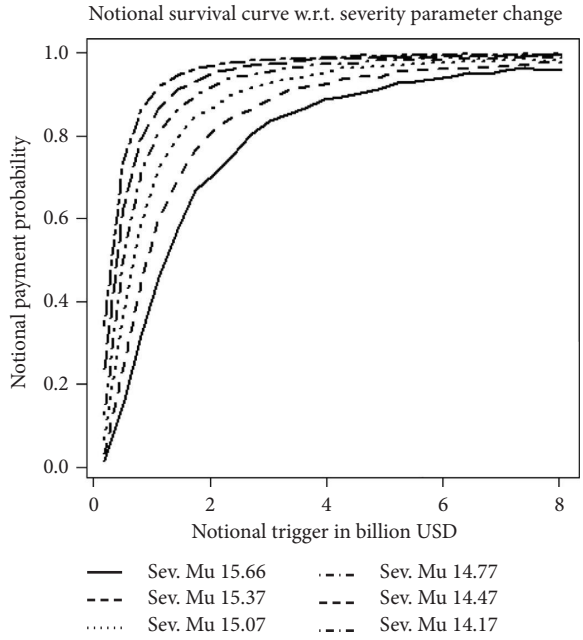

Figure 29: Cyber bond notional survival curve for 3 years for μ in the interval $\mu \pm \mu \cdot 5\%$.

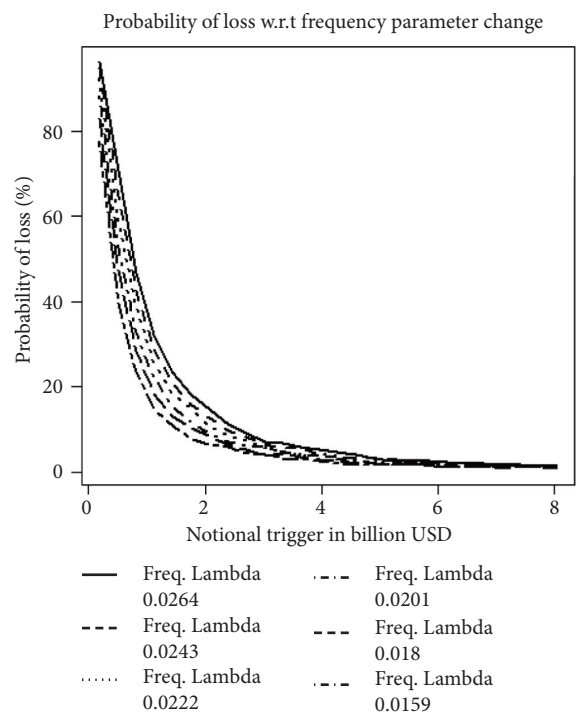

Figure 30: Cyber bond probability of loss for 3 years for λ in the interval $\lambda \pm \lambda \cdot 25\%$.

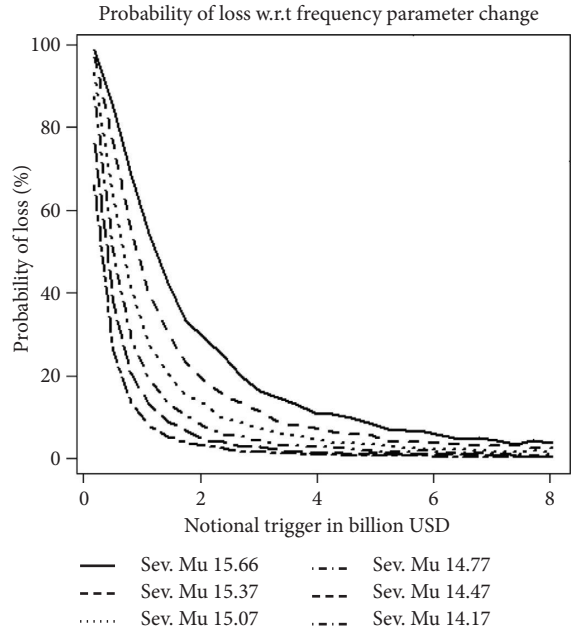

FIGURE 31: Cyber bond probability of loss for 3 years for μ in the interval $\mu \pm \mu \cdot 5\%$.

rate, however, could be easily increased through changing the cyber loss frequency and loss severity parameters (to 6.52% and 10.92%, respectively). Changing those parameters though could lead to a significant worsening of other cyber bond characteristics, e.g., increasing the probability of the notional loss for the notional trigger.

Finally, we would like to emphasize that due to lack of properly developed cyber bond framework in the literature, we are unable to make a proper comparison of our setting with some other main-stream techniques. For example, Xu and Zhang [21] rely on the setting of cat bonds to deal with the insurance of losses of a cyber-related data breach. In particular, they develop a multi-period pricing model for data breach cat bonds by combining data breach risks and financial market risks based in the equilibrium pricing theory. The main advantage of our approach is two-fold: it is simple and also sufficiently general to be applied to any type of cyber-related loss. For instance, we can easily switch from cyber-related data breach to cyber-related fraud, both of which were considered in this section. Moreover, while calculating the coupons of a cyber bond, we do not only follow the classical cat bond approach but also present an alternative par yield technique, which could be more suitable for cyber bonds, since cyber events are essentially different from the classical catastrophe events (like, e.g., hurricanes) in terms of, e.g., that the actual loss caused by a cyber event is not always seen immediately.

5. Conclusion

This paper presented a general setting of cyber bonds and considered a specific and extensive cyber bond example, including a bond price, yield, risk premium, etc. The setting appears to be convenient to use and could be easily tuned to the needs of the bond issuer. Moreover, we showed that the publicly available cyber loss event databases provide enough information to estimate the cyber loss severity and frequency distributions. Finally, two important points arose from our investigation. First, the proposed cyber bond characteristics are heavily influenced by coupon and notional triggers (determining the payment of bond coupons and notional, respectively). Second, the loss frequency distribution of specific cyber event groups can be different from that of the whole cyber event database. Both points should be necessarily cared about by the bond issuer.

For several years, several financial institutions have been using operational risk securities that specifically cover cyber risk. The materiality of these securities is growing constantly, and the separation of their scope is a matter of time. The proposed new type of financial instruments based on cyber risk allows satisfying the investors' demand for the range of available products and extend the range of potential returns and risks. On the other hand, issuers will be able to decrease coupon payments as compared to operational risk securities and mitigate the damage from cyberattacks.

The proposed financial instrument factors in the accidental occurrence of cyber incidents and unexpected losses after such events. It is considered that losses cannot be defined promptly. Thus, the modeled loss trigger is used to catch the moment of a potential cyberattack.

The proposed cyber risk securities are the instruments of current interest since it is complicated to predict the underlying risk. Furthermore, we currently have no methods to assess the potential damage from a cyberattack as far as the real damage immediately after the incident.

Further research is aimed at finding a method that will allow assessing losses from a cyber incident immediately. Thus, we will be able to use an indemnity trigger in the corresponding financial instrument.

Data Availability

The data used in the paper can be found at: (1) P. Passeri, Hackmageddon. Information security timelines and statistics, https://www.hackmageddon.com, 2011, Accessed: 2019-02-27. (2) FRED, Federal Reserve Bank of St. Louis, https://fred.stlouisfed.org/, 2019, Accessed: 2019-08-15.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this article.

Acknowledgments

The present study received no financial support of any kind.

References

[1] J. J. Cebula and L. R. Young, "A taxonomy of operational cyber security risks," Tech. report, Software Engineering Institute, Carnegie Mellon, 2010.

[2] Weforum, "The global risks report," 2016, http://www3.weforum.org/docs/GRR/WEF_GRR16.pdf.

[3] P. Passeri, "Hackmageddon. Information security timelines and statistics," 2011, https://www.hackmageddon.com.

[4] S. Ashraf, M. H. Shawon, H. M. Khalid, and S. M. Muyeen, "Denial-of-service attack on IEC 61850-based substation automation system: a crucial cyber threat towards smart substation pathways," *Sensors*, vol. 21, no. 19, pp. 6415–6419, 2021.

[5] U. Inayat, M. F. Zia, S. Mahmood, H. M. Khalid, and M. Benbouzid, "Learning-based methods for cyber attacks detection in IoT systems: a survey on methods, analysis, and future prospects," *Electronics*, vol. 11, no. 9, pp. 1502–1520, 2022.

[6] H. M. Khalid and J. C.-H. Peng, "A Bayesian algorithm to enhance the resilience of WAMS applications against cyber attacks," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 2026–2037, 2016.

[7] A. S. Musleh, H. M. Khalid, S. M. Muyeen, and A. Al-Durra, "A prediction algorithm to enhance grid resilience toward cyber attacks in WAMCS applications," *IEEE Systems Journal*, vol. 13, no. 1, pp. 710–719, 2019.

[8] M. Eling and N. Loperfido, "Data breaches: goodness of fit, pricing, and risk measurement," *Insurance: Mathematics and Economics*, vol. 75, pp. 126–136, 2017.

[9] A. Ahčan, "Statistical analysis of model risk concerning temperature residuals and its impact on pricing weather derivatives," *Insurance: Mathematics and Economics*, vol. 50, no. 1, pp. 131–138, 2012.

[10] H. M. Botoş and C. Ciumaş, "The use of the Black-Scholes model in the field of weather derivatives," *Procedia Economics and Finance*, vol. 3, pp. 611–616, 2012.

[11] P. Li, "Pricing weather derivatives with partial differential equations of the Ornstein-Uhlenbeck process," *Computers & Mathematics with Applications*, vol. 75, no. 3, pp. 1044–1059, 2018.

[12] J. W. Taylor and R. Buizza, "Density forecasting for weather derivative pricing," *International Journal of Forecasting*, vol. 22, no. 1, pp. 29–42, 2006.

[13] I. Štulec, K. Petljak, and D. Naletina, "Weather impact on retail sales: how can weather derivatives help with adverse weather deviations?" *Journal of Retailing and Consumer Services*, vol. 49, pp. 1–10, 2019.

[14] A. Balbás, I. R. Longarela, and J. J. Lucia, "How financial theory applies to catastrophe-linked derivatives – an empirical test of several pricing models," *Journal of Risk & Insurance*, vol. 66, no. 4, pp. 551–581, 1999.

[15] A. Braun, "Pricing in the primary market for cat bonds: new empirical evidence," *Journal of Risk & Insurance*, vol. 83, no. 4, pp. 811–847, 2015.

[16] K. Burnecki, G. Kukla, and D. Taylor, *Pricing of Catastrophe Bonds, Statistical Tools for Finance and Insurance*, Springer, Heidelberg, Germany, 2005.

[17] P. Nowak and M. Romaniuk, "Pricing and simulations of catastrophe bonds," *Insurance: Mathematics and Economics*, vol. 52, no. 1, pp. 18–28, 2013.

[18] K. Aase, "An equilibrium model of catastrophe insurance futures and spreads," *The Geneva Papers on Risk and Insurance - Theory*, vol. 24, no. 1, pp. 69–96, 1999.

[19] O. Kolesnikov, A. Markov, D. Smagulov, and S. Solovjovs, "Cyber bonds and their pricing models," 2019, https://arxiv.org/abs/1911.06698.

[20] J. Spry, *Non-life Insurance Securitization: Market Overview, Background and Evolution, the Handbook of Insurance-Linked Securities*, pp. 7–18, John Wiley & Sons, New Jersey, NJ, USA, 2009.

[21] M. Xu and Y. Zhang, "Data breach cat bonds: modeling and pricing," *North American Actuarial Journal*, vol. 25, no. 4, pp. 543–561, 2021.

[22] Z.-G. Ma and C.-Q. Ma, "Pricing catastrophe risk bonds: a mixed approximation method," *Insurance: Mathematics and Economics*, vol. 52, no. 2, pp. 243–254, 2013.

[23] P. Wilmott, *Paul Wilmott Introduces Quantiative Finance*, John Wiley & Sons, New Jersey, NJ, USA, 2007.

[24] H. Cramér and R. E. von Mises, "On the composition of elementary errors," *Scandinavian Actuarial Journal*, vol. 1928, no. 1, pp. 13–74, 1928.

[25] European Banking Authority, *Final Draft Regulatory Technical Standards (RTS) on Prudent Valuation under Article 105(14) (EU) No 575/2013 (Capital Requirements Regulation – CRR)*, CRR, Brussels, Belgium, 2014.

[26] MaltaToday, "Update 3 - BOV cyber attack: EUR 13 million transferred out with false transactions," 2019, https://www.maltatoday.com.mt/news/national/92964/bank_of_valletta_shuts_down_operations_following_cyber_attack_.XTF_qegzbIU.

[27] Fred, "Federal Reserve Bank of st," 2019, https://fred.stlouisfed.org/.

[28] D. Lando, *Credit Risk Modeling: Theory and Applications*, Princeton University Press, New Jersey, NJ, USA, 2004.

[29] S. Carter and M. Mainelli, *Cyber-catastrophe Insurance-Linked Securities on Smart Ledgers, Long Finance - Distributed Futures*, Z/Yen Group, London, UK, 2018, https://www.longfinance.net/media/documents/Insurance-Linked_Securities_and_Cyber_Catastrophe_v3.4_for_online_use.pdf.

[30] C. Ciumaş and R. A. Coca, "Analysis of risk premium determinants on cat bonds," *Procedia Economics and Finance*, vol. 32, pp. 1487–1493, 2015.

[31] Ey, "End of an Ibor era Ernst & young LLP," 2018, https://www.ey.com/Publication/vwLUAssets/EY-end-of-an-ibor-era/FILE/EY-%20end-of%20-an-ibor-era.pdf.

[32] N. M. Bodoff and Y. Gan, "An analysis of the market price of cat bonds, Variance," *Advancing the Science of Risk*, vol. 6, no. 2, pp. 161–177, 2013.

[33] J. C. Hull, *Options, Futures, and Other Derivatives*, Pearson, New York, NY, USA, 2018.