European Actuarial Journal (2022) 12:33–85
https://doi.org/10.1007/s13385-021-00290-1

ORIGINAL RESEARCH PAPER

A comprehensive model for cyber risk based on marked point processes and its application to insurance

Gabriela Zeller[1] · **Matthias Scherer**[1]

Received: 12 August 2020 / Revised: 12 February 2021 / Accepted: 16 July 2021 /
Published online: 17 August 2021

Abstract
After scrutinizing technical, legal, financial, and actuarial aspects of cyber risk, a new approach for modelling cyber risk using marked point processes is proposed. Key covariates, required to model frequency and severity of cyber claims, are identified. The presented framework explicitly takes into account incidents from malicious untargeted and targeted attacks as well as accidents and failures. The resulting model is able to include the dynamic nature of cyber risk, while capturing accumulation risk in a realistic way. The model is studied with respect to its statistical properties and applied to the pricing of cyber insurance and risk measurement. The results are illustrated in a simulation study.

Keywords Cyber risk · Cyber insurance · Emerging risks · Marked point processes · Accumulation risk

1 Introduction

Researchers and practitioners from different disciplines have analysed ‘cyber risk’ and ‘cyber insurance’ from their provenience, among them IT system experts, economists, statisticians, actuaries, etc.; a recent survey of the literature on these topics in business and actuarial science is provided in Ref. [1]. Despite the lack of an established agreed-upon framework, all stakeholders share the opinion that cyber risk is on the rise. This is substantiated by continuously changing and expanding cyber threats [2] and an increasing frequency and magnitude of the financial consequences of cyber incidents [3–6]. The potential consequences of cyber incidents

✉ Gabriela Zeller
gabi.zeller@tum.de

Matthias Scherer
scherer@tum.de

[1] Chair of Mathematical Finance, Technical University of Munich, Parkring 11, 85748 Garching-Hochbrück, Germany

have also been prominently covered by the media; examples being [7–9]. This has lead to various cooperations between academia, industry, and government agencies (e.g. *CISA*[1] in the US or *CiSP*[2] in the UK) with the aim of developing defense strategies against cyber crime and enhancing the overall resilience of IT networks. Corporations have moved their perception of cyber security from a merely technical topic to a larger business risk [10], but this awareness does not yet seem to have translated into widespread institutionalisation of cyber risk management [11]. A recently highlighted aspect is the connection between *Cyber Incidents* and *Business Interruption*, which jointly ranked as the top global business risks in a 2019 survey [12].

One strategy to cope with risk is risk transfer, e.g. via insurance contracts. Parallel to the risk, the demand for cyber insurance solutions has been continuously increasing [10] over the last few years. In spite of its growth, however, today's cyber insurance market is still relatively small compared to the value of the assets that could be impaired by a cyber event [2]. Barriers are not a lack of demand for cyber risk transfer, but rather a number of obstacles that complicate the understanding and quantification of the underlying risk, including the lack of solid data on losses, a fast-paced evolution of cyber risk, and the disparity of data protection laws globally [4, 13].

Despite these challenges, especially in the US an existing market is already established; including underwriters, brokers, and organisations specialized on *cyber data analytics* [14]. Concerning the pricing of cyber risk, however, a surprising finding was published by Romanosky et al. [15]: they systematically analysed cyber policies across the US and found that the main themes used for pricing included *looking to competitors* and *estimation/guesswork*. The ad-hoc nature of cyber policy pricing confirms that a unified quantitative understanding of this new type of risk and its underlying drivers is still at its infancy.

The cyber risk model developed in the present work, designed from an actuarial point of view, constitutes a threefold contribution:

1. The model is based on a holistic approach to cyber risk, systematically describing the underlying risk factors while including information-technological, economic, and actuarial viewpoints.
2. The model is able to capture dependencies and accumulation risk in a realistic way by explicitly taking into account idiosyncratic cyber incidents and systemic cyber events.
3. Using the loss distribution approach, the model can easily be applied in an insurance framework. A simulation study illustrating this application is included.

The remainder of this paper is structured as follows: Sect. 2 carefully reviews the existing literature on cyber risk and identifies key findings for an actuary. Section 3 presents a holistic view on cyber risk, including key characteristics and risk factors.

[1] https://www.cisa.gov.
[2] https://www.ncsc.gov.uk/section/keep-up-to-date/cisp.

A new model is developed and analysed in Sect. 4 and illustrated in a simulation study in Sect. 5. Section 6 concludes and reveals opportunities for further research.

2 Background and literature review

2.1 Literature review

Most papers on cyber risk and cyber insurance are restricted to one particular point of view (e.g. IT security, network modelling, actuarial approaches) and the overall picture remains fragmented. In what follows, we group the existing literature according to the main theme of investigation.

2.1.1 Game-theoretic studies

Bohme and Schwartz [16] studied a unifying framework for modelling cyber insurance and classified existing research approaches of cyber insurance market models. Until 2010, many academic papers were motivated by the study of interdependent security and primarily focused on questions of network security and its relation to the existence of an insurance market, often using game-theoretic approaches (e.g. Refs. [17–22]). Other works concentrated on the correlation properties [23] and monoculture effects [24] of cyber risk and the existence of an insurance market under these conditions.

More recently, a very comprehensive overview of various aspects of cyber insurance was given in Ref. [25], including a classification of existing research approaches with interdependent security according to the underlying insurance market model. While the listed approaches differ in their assumptions, the research aims are quite similar. Most studies focus on the existence of a *Nash Equilibrium* for security investments (e.g. Ref. [26]) and the existence or efficiency of an insurance market (e.g. Refs. [17, 19, 20, 22, 27–30]). Slightly different mathematical approaches include the use of *Bayesian network games* to design optimal cyber insurance contracts [31] or to study the effect of network externality on security adoption [32].

Under quite realistic assumptions, the socially optimal level of security investments cannot be attained in these models, as individuals are incentivised to underinvest [25]. Furthermore, given the availability of cyber insurance, individuals are even more reluctant to invest in self-protection and it is thus generally not possible to design insurance as a means to reach socially optimal levels of investment (e.g. Refs. [19, 20, 22, 27–30]). Some studies thus test whether regulatory actions (e.g. fines or rebates, taxes for low self-protection, or risk pooling arrangements) might enable insurance to incentivise self-protection, reaching conflicting conclusions (e.g. Refs. [17, 19, 22, 28, 29, 33, 34]).

2.1.2 Interdependence and network models

Given that an accepted terminology and framework for cyber risk does not yet exist, some authors concentrated on developing taxonomies and frameworks (e.g. Refs.

[35–37]) or on embedding cyber into the better-known context of operational risk management (e.g. Refs. [38, 39]).

One feature of cyber risk that is commonly regarded as particularly problematic is the lack of independence among the risks/claims, a problem that was addressed using copula approaches in Refs. [40, 41], linear correlations in Ref. [24], and a combination of both in Ref. [23]. More recently, Peng et al. [42] studied the multivariate dependence exhibited by real-world cyber attack data using a Copula-GARCH model. The latter works describe cyber attacks of different types or multivariate nature to be the source of dependence. Peng et al. [43] propose modelling and predicting extreme cyberattack rates by using marked point processes and similarly, studying an empirical data set of breach incidents [44] argue that stochastic processes rather than distributions should be used to model and predict hacking breach incident inter-arrival times and breach sizes. Baldwin et al. [45] find strong evidence of contagion in cyber attacks to different components of a firm's information system using self- and mutually-exciting point processes.

Instead of considering underlying attack rates, studies concerned with cyber insurance seek to quantify the expected monetary losses of an insurer's portfolio. To this end, dependencies between losses can also be captured by considering a model of epidemic spreading on the underlying network of firms. Fahrenwaldt et al. [46] use a (Markovian) SIS-process to model the infectuous spread of a cyber vulnerability and subsequently an adapted counting process for the occurrence of attacks. Xu and Hua [47] use Markovian and Non-Markovian processes for epidemic spreading and propose to use a copula approach to capture the dependence among time-to-infection distributions. Xu et al. [48] study a model of cyber epidemics over complex networks, additionally introducing copulas to capture dependencies between cyberattack events.

2.1.3 Data-driven studies

The lack of publicly available, reliable, and sufficiently large data sets for cyber incidents remains one of the obstacles for sound statistical investigations. Among the best-known data sources on data breaches are the continuously updated *"Chronology of Data Breaches"* dataset by the California-based nonprofit corporation *Privacy Rights Clearinghouse (PRC)*[3] and the *"Open security foundation data loss database"*.[4] The former data was e.g. studied by Edwards et al. [49], with the conclusion that the number of records exposed can be modeled by the log-normal law and the daily frequency can be described by a negative binomial distribution. Somewhat surprisingly, the study found neither size nor frequency of data breaches to exhibit a time trend. Eling and Loperfido [50] use multidimensional scaling and goodness-of-fit tests to analyze the distribution of the data breach information. They show that modelling severity using a log-skew-normal distribution seems adequate and find that different types of data breaches need to be modeled as distinct risk categories.

[3] Available for public download from https://privacyrights.org/data-breaches.

[4] Formerly available for public download from http://datalossdb.org.

Eling and Jung [51] study the cross-sectional dependence of the data breach losses and identify a significant asymmetric dependence of monthly cross-industry losses in four categories by breach types as well as cross-breach type losses in five categories by industries. Farkas et al. [52] analyze heterogeneity of the reported cyber claims through the use of regression trees.

The second database was examined in Ref. [53], who focus on the theft of personal information and report a stable power-law tail distribution of personal identity losses per event. Wheatley et al. [54] combined data from both databases to focus exclusively on large breaches and study maximum breach sizes as well as severity distributions. The best fit is obtained by using a doubly truncated Pareto (Power law) distribution with linearly decreasing shape parameter for breach sizes, with sub-linear growth for the maximum log breach size.

Romanosky [55] uses a (commercial) dataset from *Advisen*, a US-based consultant to the insurance industry, with the aim of examining the composition and costs of cyber events. They conclude that firms may lack a strong incentive to increase their investment in data security and privacy protection and the primary motivation may come from the cyber insurance industry through its use of incentive-based premium reductions.

While the aforementioned papers mostly concentrate on data breaches, Eling and Wirfs [56] has a wider focus: they define cyber risk as a subgroup of operational risk and analyze cyber data from a large operational risk database (*SAS OpRisk Global data*), including a global range of cyber incidents that have occurred over an around twenty-year period and considering actual costs instead of number of affected records only. The frequency of losses is found to be most adequately modelled by a Negative Binomial distribution in a static approach, and a Poisson process with covariate-dependent rate in a dynamic approach based on Ref. [57]. For the loss severity, none of the canonical candidates (exponential, Gamma, log-normal, log-logistic, generalized Pareto, Weibull) were found to accurately model the entire loss data. Promising alternatives were a non-parametric transformation kernel estimation and an extreme value approach, where excesses over a threshold were modelled by a generalized Pareto distribution. The study highlighted the importance of distinguishing between *cyber risks of daily life* and *extreme cyber risks*.

2.2 Background on cyber insurance

Marotta et al. [25] provides an excellent summary of the past, present, and future of the cyber insurance market; as seen in 2017. They report an ongoing growth of available coverage, spurred by rising demand for insurance protection against cyber risks, which in turn is often caused by public coverage of severe cyber incidents [14, 25, 58], the introduction of stricter legislation across the globe [2, 25], and firms' own loss experience [14, 58]. In 2015, the global market for cyber insurance was estimated to be worth around $2 billion in premium, with US business accounting for approximately 90%. At the time, fewer than 10% of all companies had purchased cyber insurance, with typical buyers coming from industries holding large volumes of personal data, such as healthcare and retail, or relying on digitalized technology

processes, such as manufacturing and telecommunications. A rapid market growth was projected, with total premium reaching $20+ billion by 2025 [4]. As of today, this estimate still seems realistic, with a global market size of around $7 billion in 2020 [59]. However, despite a strong growth and new insurance solutions being developed continuously, in 2017 the cyber insurance market in the US still had not reached the expected size predicted by optimistic forecasts [25]—thus the question of challenges inhibiting the market development arises.

2.2.1 Challenges and insurability of cyber risk

For the European market's supply side, ENISA et al. [13] identified the lack of solid data on losses, the fast pace of technology evolution, and the lack of adequate reinsurance among the key factors. Regarding the demand side, companies' most often mentioned reasons to refrain from purchasing cyber insurance include high prices [10, 11, 14, 58, 60], lack of availability of desired limits and coverage [14, 58, 60], concerns about numerous exclusions and restrictions [10], and lack of understanding about own exposure [61] or about policy offers [11].

A fundamental question is if, and under what circumstances, cyber risk is insurable at all, given its complex nature. ENISA et al. [13] first examined this question and concluded that cyber might well be an insurable type of risk fulfilling almost all of the considered desiderata. A more detailed analysis based on a dataset from an operational risk database was conducted in Ref. [62] and subsequently adressed in Ref. [63]. Their study identified the main problems to be lack of independence of loss occurrence, presence of information asymmetries, and lack of adequate cover limits. However, they remark that some problematic aspects might be alleviated in the future and thus advocate for systematic data collection, e.g. via platforms for data sharing organised by national regulators or international associations.

2.2.2 Cyber insurance policies: coverage and exclusions

Ignoring the academic question "to be (insurable), or not to be," in practice an immature cyber insurance market has developed and an increasing scope of cyber insurance products is available. The majority of coverage is offered as dedicated cyber coverage [11, 14], with customers frequently shifting from endorsement to standalone policies [58]. The most sought-after types of coverage include cyber-related business interruption, data breaches, cyber extortion, and fund transfer fraud/social engineering [14, 58]. Cyber policies typically cover the most common and costly incidents, including human error, mistakes, and negligence, external attacks by cyber criminals, system or business process failures, and malicious or criminal insiders. Rarely, however, attacks against business partners, vendors, or other third parties are included [10]. All policies generally distinguish between first and third party (liability) losses [15]. A systematic qualitative analysis of cyber insurance policies across the US [15] found a surprisingly strong similarity regarding covered losses, where the ten most commonly covered losses included costs of claims expenses (including legal expenses from penalties, defense, and settlement costs), public relations services, costs of notification of affected individuals, business income loss, data or

system restoration, forensic investigation costs, and data extortion expenses. Romanosky et al. [15] points out that the top covered costs are *cleanup costs*, i.e. indirect costs in order to comply with laws, manage the firm's reputation, and reduce further expenses following a breach. Other studies found similar results for the covered types of losses (e.g. Refs. [2, 10, 16, 25]).

Regarding exclusions, Romanosky et al. [15] found more variation between policies, where the most common exclusions stemmed from criminal, fraudulent, or dishonest acts, errors or omissions, intentional violation of a law, criminal investigations or proceedings, and payment of fines, penalties, or fees. Furthermore, hard-to-quantify costs like loss of employee productivity or brand damage are often excluded [10].

Lastly, an important issue to mention is *non-affirmative* or *silent* cyber cover, meaning that cover for cyber incidents may exist for example in traditional property and casualty policies, even though this was not the intention of the underwriter [12]. Misconceptions like this might lead to a dangerous perception gap for insureds [11] who suffer from an illusion of protection as well as insurers who might suffer from (unintentionally written) exposure to cyber risk.

2.2.3 Cyber insurance: risk assessment and pricing in practice

In the US, carriers typically assess an applicant's cyber risk through questionnaires, most of which emphasize the amount and type of data handled by the investigated company, whereas the technical infrastructure and IT security management receive less attention [15]. The sample questionnaire for risk assessment for cyber insurance by the German Insurance Association [64] differentiates between three risk categories primarily according to the annual turnover of a company and, secondarily, according to certain risky business units (e.g. e-commerce or handling of sensitive data), where the number of questions for a candidate increases with increasing risk category.

Regarding pricing, there seem to be large differences between carriers, while surprisingly, some of the recurring themes are reliance on external sources, estimation, comparison with competitors, using underwriter's experience, and adaptation of prices from other insurance lines [15]. Similarly, respondents in Refs. [14, 58] stated that competition between carriers seemed to prevail over actuarial assessment of the cost of risk. Most examined policies in Ref. [15] multiply a base premium by variables relating to standard insurance factors and industry-related factors, where high hazard weightings are assigned to businesses that collect and store a high volume of sensitive data or operate in industries like retail, healthcare, and the financial industry. Finally, premium multipliers are commonly assigned according to the outcome of the questionnaire regarding IT security (e.g. privacy controls, network security controls, existence of an incident response plan). In conclusion, the impression manifests that while insurers are trying to get a better understanding of cyber risk and its drivers, due to the lack of ample reliable data to describe the problem with sufficient statistical precision, as of today pricing often happens on an ad-hoc basis and established quantitative models do not exist, yet.

2.2.4 The potential of cyber insurance: insurance as a service

While traditionally insurance is a means of risk transfer, cyber insurance can potentially offer more than compensation for monetary losses. Many insurers already advertise the services their cyber insurance policies include, e.g. prevention and incident response services or crisis communication support [65]. Moreover, ENISA et al. [13] highlights possible benefits of the development of a cyber insurance market such as the potential to incentivise firms to increase IT security through premium discrimination or the development of a market for security consulting firms that investigate security practices as part of the underwriting process.

Another future topic for insurers concerns arrangements and standards that facilitate sharing data and information about cyber incidents. In order to help corporations to overcome their resentments about sharing such data, it is the insurers' task to demonstrate that pooling data enables them to improve their range of services and design adequate new and transparent products that meet companies' needs [11].

Thus, despite most academic works concluding that in their theoretical frameworks cyber insurance cannot improve social welfare or network resilience, in practice the development of adequate, transparent cyber insurance products and services might entail a number of benefits transcending a mere possibility for companies' cyber risk transfer. In summary, during the last few years research on cyber risk has considerably increased and various aspects have been considered (disjointly). Our work focuses on the viewpoint of actuarial science, but we aim at providing a holistic modelling approach, taking into account both IT security and economic factors.

3 Cyber risk: a holistic view

Cyber risk as a multi-faceted and young risk still lacks an established definition in the (insurance) literature. We therefore introduce key characteristics and risk factors a cyber risk model should comprise.

3.1 Definition and key characteristics

Eling et al. [66] summarizes the origins, consequences, and key characteristics of cyber risk as follows:

> *"Any risk emerging from the use of information and communication technology (ICT) that compromises the confidentiality, availability, or integrity of data or services. [...] Cyber risk is either caused naturally or is man-made, where the latter can emerge from human failure, cyber criminality (e.g. extortion, fraud), cyberwar, and cyber terrorism. It is characterised by interdependencies, potential extreme events, high uncertainty with respect to data and modelling approach, and risk of change."*

Interpreted from the actuarial perspective, the traditional approach of quantifying risk by frequency and severity of incidents, and combining them (potentially using an appropriate dependence structure) to obtain an aggregated loss distribution is complicated for cyber risk. We follow [25, 63] in summarizing the central properties of cyber risk:

- **Absence of historical data:** The novelty of this risk and the absence of an established terminology for cyber incidents makes it difficult for insurers to create a reliable database with information on losses. This is exacerbated by a reporting bias, i.e. companies are often reluctant to reveal incidents in order to avoid reputation damages.
- **Dynamic risk type:** Cyber risk is as non-stationary as the underlying technology and legal framework, which makes the usability of past data for modelling future losses difficult. Among the main features that underscore the dynamic nature of cyber risk are the growing speed and scope of digital transformation, widening sources of vulnerability from hyperconnectivity, and the evolution of threat actors [2].
- **Strategic threat actors:** Cyber losses do not occur in a completely random fashion, as they are often caused by malicious actors with strategic (economic) motives and attack patterns. In 2018, Lewis [6] even described the trend of *cybercrime as a service (CaaS)* encompassing a large diversity and volume of cybercrime offerings, including products (e.g. exploit kits, custom malware) and services (e.g. botnet rentals). Around this, a thriving cybercrime economy has emerged from the related communities, offering for instance product development and technical support.
- **Interdependence/Accumulation risk:** The interconnectedness of IT-systems and the often systemic nature of vulnerabilities induce a dependence structure within and across company networks and the potential for loss accumulation.
- **Interdependence of security:** Another result of the network interdependence are negative externalities regarding security, which within a game-theoretical context might lead to an equilibrium in which all companies underinvest in security and, therefore, the overall network is not sufficiently protected.
- **Difficult impact determination:** Due to the intangible nature of information assets, it is often difficult to quantify the economic consequences of a cyber incident.
- **Information asymmetry:** Cyber insurance exhibits two sorts of information asymmetry: Adverse selection and moral hazard. The former refers to the challenge for an insurer to reliably determine a company's risk exposure, the latter refers to the difficulty of ensuring the risk exposure to be maintained throughout the entire contract period.

As we focus on actuarial questions, we refrain from considering in more detail technological aspects of information security, the economics of cyber security and cybercrime, or the legal framework.

However, one important aspect to be mentioned concerns the role of governments and legislation. For example, in the European Union, the *General Data Protection*

Regulation (GDPR) came into force on May 25, 2018 with fines up to 20 € million or 4% of annual global revenues, emphasizing that the respective legal framework must be considered when modelling the size of cyber insurance claims, as penalties and fines may be included in the coverage. Furthermore, besides setting the legal framework, Anchen [2] argued that the government could help to promote cyber resilience by reshaping incentives and increasing awareness of cyber threats.

3.2 Cyber risk factors

So far, the term *risk* was used informally. Going further, we disintegrate risk into a combination of *threat*, *vulnerability*, and *impact* (c.f. Ref. [25]). A threat is the underlying root cause of the risk, which itself does not necessarily manifest as an *incident*, but is only harmful if there is a corresponding *vulnerability* in the target system. If a threat and an existing vulnerability lead to the occurrence of an incident, the *impact* refers to the consequences, which can be tangible (e.g. direct financial consequences) or intangible (e.g. loss of reputation). The process of risk management classically consists of identifying risks by characterising threats, vulnerabilities, and impacts, analysing risks with regards to the probability and impact of an incident and treating the estimated risks by selecting and applying adequate measures. As outlined in Ref. [25], there are four classical ways of dealing with risks: risk reduction, risk transfer, risk avoidance, and risk acceptance. Clearly, cyber insurance is a tool for risk transfer and a potential incentive for risk reduction.

3.2.1 Threats

In order to assign cyber incidents to a few distinct classes, we recall a quite concise definition of cyber risk originally motivated by the study of operational risk management, namely *"operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems."* [38].

We follow [37] in applying this definition to classify cyber incidents according to three classical information security protection goals: *confidentiality, integrity, and availability* of information assets [67]. Table 1 gives an overview of their definitions and the incident types that compromise each goal.

Of course, these categories are not mutually exclusive; an example combining features of fraud and business interruption is a *Ransomware* attack, i.e. extortion for temporarily withheld data. We nevertheless implement the above distinction, as it is known from data breaches that incidents of different kinds typically show a different statistical nature [68] and, moreover, the economic consequences vary across the incident categories [55]. An incident falling into more than one class could e.g. be assigned partially to both of them according to the losses it entails, e.g. for the Ransomware case, losses from the interruption of operations under BI and losses from ransom payments under FR. Furthermore, we can understand FR as a general class of incidents that cannot be distinctly classified as DB or BI.

Table 1 Classification of three main types of cyber incidents according to the basic information security protection goal they compromise

Type of cyber incident	Abbreviation	Information security goal compromised by this incident type	Definition of information security goal [67]
Data breach or data loss	DB	Confidentiality	Prevention of *unauthorized disclosure* of information
Business interruption	BI	Availability	Prevention of *unauthorized withholding* of information or service
Fraud (or general incident)	FR	Integrity	Prevention/detection of *unauthorized modification or deletion* of information

Until a few years ago, data breaches have been the most observed type of incident, see Sect. 2.1. Recently, however, the potential impact from cyber-related BI has become a major concern [4] whose financial consequences could equal or surpass losses from a data breach. Vice versa, cyber incidents have become the most feared BI trigger [12]. Our classification is quite similar to the definition of a *cyber attack* used in Ref. [13] which, however, only focuses on malicious cyber attacks. In our view, to capture the whole scope of cyber incidents, a second distinction along another dimension, namely the *root cause*, should be made.[5] Here, the following should be distinguished:

- **Targeted attacks**: Malicious attacks that target one firm specifically due to its characteristics and assets. Usually, the attack vector is tailor-made to circumvent the company's defense strategies.
- **Individual failures**: Non-malicious incidents at single firms that happen due to internal or external machine or system malfunction or human error.
- **Untargeted attacks**: Malicious attacks (from an external source) that do not target one firm specifically because of its characteristics, but are opportunistic in the sense that they attack many available targets—usually simultaneously.
- **Mass failures**: Non-malicious events that affect multiple entities simultaneously, such as the failure of a cloud service provider.

Combining incident types and root causes yields the partition of cyber incidents as shown in Table 2.[6] Note that we use terminology that is common in the natural catastrophe context and is applied in the cyber context in Ref. [70]: an incident refers to a single loss, whereas an event can cause many related incidents.[7]

One can further scrutinize motives of individuals or groups for targeting companies via cyber attacks. CRO Forum [69] defines five types of *threat actors* (with corresponding motivation): nation states (strategic), organised criminals (economic), hackers (reputational), hacktivists (political), and insiders. The last group includes *unintentional* insiders, emphasizing that, although malicious attacks are more publicly present, a large share of cyber incidents stems from human error or technical

[5] To avoid confusion, the well-known classification of cyber risk by CRO Forum [69], which distinguishes four types of cyber incidents and four potential root causes, should be mentioned. In this work, we consider their classification's *root causes* in the context of vulnerabilities and denote as *root cause* the actual origin of the incident.

[6] This categorisation also comprises classifications by other sources, e.g. Refs. [51, 55], the *PRC* database, the database of *Advisen* (https://www.advisenltd.com/data/cyber-loss-data/) and the four incident types of Ref. [69].

[7] Note that the common IT terminology of *systemic* vulnerabilities introduced in Sect. 3.2.2 is transferred directly to the terminology of *systemic events* used throughout this work. As this might be reminiscent of the term *systemic risk* used in the finance literature, let us already emphasize that we understand the risk from systemic events in the cyber context as neither the risk of a cascading failure of a whole industry nor a mixture of underlying, non-diversifiable market factors. Rather, we understand that systemic vulnerabilities create common entry points for external threats to the system and therefore introduce the potential for common external shocks to the whole portfolio or parts of it and thus multiple dependent, simultaneous loss occurrences.

Table 2 Examples of cyber incidents/events according to the classification by incident type and root cause

	Idiosyncratic incidents		Systemic events	
	Targeted attack	Individual failure	Untargeted attack	Mass failure
Data breach (DB)	Targeted data theft	Individual unintended data disclosure	Data theft through widespread malware/phishing	Unintended data disclosure at cloud service provider
Business interruption (BI)	Targeted (D)DoS/ransomware attack	Disruption of IT system or process through accidental malfunction	Widespread ransomware attack	Cloud service outage disrupting business services
Fraud/general (FR)	CEO fraud through targeted (spear-)phishing attack	Accidental compromise of database by employee	Widespread ransomware attack or social engineering fraud	Accidental compromise of data stored at cloud service provider

Note that targeted attacks include the special case of supplier attacks and we again understand the category *FR* generally as any incident that compromises data integrity

problems. This applies to cyber-related BI [4, 12], data breaches [5, 12], and general cyber incidents [3, 55, 56].

One peculiar type of targeted attacks not yet explicitly mentioned are so-called *supplier attacks*, where a company is not attacked directly but through attacks on supply-chain partners (with potentially weaker defenses). Although this so far only accounts for a minority of incidents, studies have identified a trend of attackers slowly shifting their attack patterns to exploit supply chain partner environments, particularly for industries with mature cybersecurity standards [3], and thus many companies will increasingly seek to extend insurance cover to their supply chains [4].

3.2.2 Vulnerabilities and controls

Threats only manifest as *successful* incidents if there exists an exploitable *vulnerability* in the target system [36]. We distinguish between *symptomatic* and *systemic* vulnerabilities (c.f. Ref. [36, 71]), where the former only affect single firms (e.g. via custom software), while the latter can affect many firms simultaneously (e.g. via a vulnerability in standard software). Especially the second kind is worrisome, as it exposes many potential targets to the same threat and thus could lead to highly correlated and simultaneous losses [36]. From the viewpoint of a company, a vulnerability can be mitigated by establishing adequate *controls*, both technical (e.g. antivirus software) and non-technical (e.g. awareness campaigns [36]).

Investments in cyber security require strategic decisions and cannot be limited to the prevention of cyber incidents, but must also take into account the discovery, investigation, and containment of an attack and the fast recovery of systems to a working state [3]. Many academic works have studied the problem of finding an optimal security level, balancing the cost of controls against the benefits from reduced losses (see Sect. 2.1). We do not further study this problem here, but rather conclude that a firm's IT security level must be a central parameter for an insurance company's risk assessment (as it already is in practice [15]).

Besides *opportunistic* attacks that stem from the opportunity of exploiting an existing vulnerability, we also consider targeted attacks on a specific victim. Thus, further firm characteristics that incentivise such attacks need to be identified. Considering the list of threat actors in the previous section, the following characteristics arise:

- **Industry sector**: Previous studies indicate that both the number and cost of cyber incidents depend on the industry [3, 5, 51, 52, 54, 55], with regulated industries such as healthcare and financial services suffering most. Wheatley et al. [54] mention that the industrial sector as a risk factor may serve as a proxy to identify relatively homogeneous subgroups of companies with respect to their frequency of interaction with consumers and the total volume of personal data they guard.
- **Data**: It is intuitive that indeed the *amount and sensitivity of data* handled by the company is a factor, as especially actors with economic motives will target companies with a high amount of valuable data in order to maximize their economic

gain. In practice, this is already incorporated into insurance pricing via hazard weightings [15].

- **Company size**: Regarding the size of a company, there are different aspects to be considered: Large, publicly known companies are prime targets for threat actors with reputational motives, whereas SMEs are often worse protected due to budget constraints or their smaller awareness for cyber risks.

Eling and Wirfs [56] considered, among others, the company-specific covariates *industry sector* and *size* and found both of them to be highly significant for the frequency of all kinds of cyber incidents in their model.

3.2.3 Impact

Parallel to increasing occurrence rates, the economic consequences of various cyber incidents have recently become more severe, with BI and information loss having the highest monetary impact [3]. For data breach incidents, the average cost could be up to several million USD [5, 10], where the biggest financial consequence is found to be lost business. Quantifying the consequences of cyber incidents is difficult due to the scarcity of historical data and the various (intangible) types of costs. Nevertheless, earlier studies give some indications of cost drivers.

For data breaches, Ponemon Institute LLC [5] find the average *cost per record* to depend on the root cause (malicious attacks vs. system failures and human error) and the industry sector. The latter could be explained by the fact that the rate of lost customers and business depends on the industry, but also by considering the impact of regulation and litigation on breach cost causing highly regulated industries to suffer larger losses [12]. An effect of the company size on the breach cost was reported in Refs. [53] and [55], who developed a model for the log-cost of a data breach depending on the firm's revenue (as a proxy for size) and the number of compromised records. This is more comprehensive than the well-known *Jacob's formula* [72], which simply links the log-cost of a data breach to the (log-)number of compromised records. Another amendment was proposed in Ref. [52], who argue that [72] did not yet take into account the cost of *mega data breaches* observed in future years. Finally, adequate controls can not only decrease the probability of a breach, but also its potential consequences: Improvements in data governance programs, presence of incident response plans, and employee training all result in average cost savings in case of a breach [5, 60].

Concluding, there is evidence that for data breaches the cost of an incident depends on the industry sector, the size of the company, the amount of data affected, potentially the type of attack, and controls in place. The statistical findings and distributions used to model the severity of data breaches found in investigations of available databases have been summarized in Sect. 2.1. Note that these findings for data breaches might not necessarily translate to the other incident types, as different types of cyber incidents (e.g. data breaches and privacy violations) are found to display large median cost differences [55].

It is hard to find information on the economic impact of the other two types of incidents studied here, namely BI and fraud. For the former, some sources from the

non-cyber domain are available [73–77]. The only sources including indications of which distributions are useful to model economic loss from BI are [77], who finds that the size of yearly BI insurance claims follows a Pareto distribution with an extremely heavy tail and infinite expected claim size, and [75], who suggests modelling BI loss by a *PERT* distribution.

For fraud one might hope to find information in studies on the cost of cyber crime but, unfortunately, the data is usually either aggregated over all types of cyber incidents from malicious sources or focuses on information loss/theft. Thus, there is very little reliable evidence on the actual cost of cyber fraud. Despite indications that cyber risk is quite different from other types of operational risk [56], one way might be to draw on knowledge about the modelling of operational risk as, e.g. the Basel II framework [78] includes *internal fraud* and *external fraud* as event-type categories.

Another option is to refer to the recent work of [56], who study all kinds of cyber incidents (including data breaches as a subset) using a model where the parameters of the distribution of both frequency and severity of cyber incidents might depend on firm-specific and incident-specific covariates as well as time. They resort to an EVT approach to model the severity of events, using the *generalized Pareto distribution (GPD)* to model excesses over a high threshold (the tail of the distribution) and a series of simple parametric distributions (e.g. exponential, Gamma, log-normal) for the body. The GPD with *shape parameter* ξ and *scale parameter* β is of the form

$$GPD_{\xi,\beta}(x) = \begin{cases} 1 - \left(1 + \frac{\xi}{\beta}x\right)^{-1/\xi}, & \text{if } \xi \neq 0, \\ 1 - \exp\left(-\frac{x}{\beta}\right), & \text{if } \xi = 0, \end{cases}$$

for $x \geq 0$ if $\xi \geq 0$ and $x \in [0, -\beta/\xi]$ if $\xi < 0$. They build on the work of [57] to fit a model where the parameters of the GPD may depend on covariates (including time). To the best of our knowledge, their work is the first to model the actual economic loss and to consider general types of cyber incidents instead of only data breaches, thus we incorporate their approach in our framework.

3.3 Properties of a cyber risk model

Before proposing a model for cyber risk, we shortly summarize the properties/stylized facts it should possess given the findings from this chapter:

- Different types of incidents (DB, BI, and FR/general incidents) should be distinguished.
- The model should include idiosyncratic incidents and systemic events, where both categories can include malicious and non-malicious causes. Systemic events stemming from common vulnerabilities are particularly worrisome as they entail accumulation risk.
- Companies should be viewed as heterogeneous, as their exposure and resilience to cyber threats depends on their characteristics. The most relevant such charac-

teristics are the industry sector, the company size, the data handled by the company, and its IT security level.
- The model should be able to capture the dynamic nature of cyber risk, as occurrence rates as well as impact of cyber incidents may change over time.

4 Actuarial model

Considering cyber risk a combination of threat, vulnerability, and impact, from an actuarial viewpoint it remains to translate this understanding into modelling *frequency* and *severity* of losses within a portfolio. After doing so in Sects. 4.2 and 4.3, in Sect. 4.4 we address actuarial questions, before illustrating the model in a simulation study in Sect. 5. Note that the proposed model is purposefully constructed in a modular way, as some of the assumptions and parameter choices might be updated in the future once suitable data is available. Moreover, a user who wants to incorporate properties of an internal data set can refine individual features of the model (or replace parts) without changing the overall structure.

4.1 Insurance portfolio

Consider K firms, labeled $\{1, \dots, K\}$, constituting the portfolio of an insurance company exposed to losses due to cyber incidents (idiosyncratic or caused by systemic events). This typically refers to losses covered by stand-alone cyber policies, but might in some cases include losses that still fall under traditional policies for some insurers (note that a trend towards the elimination of cyber exposure in traditional business is observed, hopefully leading to a clear-cut distinction in the future). Following the findings of Sect. 3, we assume that for each company included into the insurer's portfolio, information about relevant covariates is collected via a questionnaire and public information. Table 3 gives an overview of the characteristics we identified as relevant, the potential to elicit the necessary information from public data or a firm's voluntary disclosure, and a suggestion for their inclusion in a mathematical model.[8] Thus, for each firm $j \in \{1, \dots, K\}$, the vector of covariates

$$x_j = (x_{j1}, \dots, x_{j5})' = (b_j, s_j, d_j, c_j, nsup_j)', \tag{1}$$

is known, yielding a $K \times 5$ *covariate matrix*

[8] We do not claim this list to be exhaustive but stress that all required information can be objectively collected by an insurer. For example, one could argue that for an insurer with a world-wide portfolio, information on a firm's location (jurisdiction) should be added as it might influence the severity (e.g. via fines to be paid following a data breach) as well as, for targeted attacks, the frequency (as data from some countries might be more valuable and therefore a more frequent target) of cyber losses.

$$\mathbf{X} = \begin{pmatrix} x_1' \\ \vdots \\ x_K' \end{pmatrix} = \begin{pmatrix} x_{11} & \cdots & x_{15} \\ \vdots & \ddots & \vdots \\ x_{K1} & \cdots & x_{K5} \end{pmatrix},$$

where each row corresponds to one firm in the portfolio and each column to one of the above covariates in the order given in Eq. (1). We assume for notational convenience that all firms are ordered by sector, i.e. suppose there are B sectors and $K_{\hat{b}}, \hat{b} \in \{1, \dots, B\}$, such that firms in sector $\hat{b}$ exactly correspond to indices $i \in \mathcal{I}_{\hat{b}} := \{1 + \sum_{\ell=1}^{\hat{b}-1} K_\ell, \dots, K_{\hat{b}} + \sum_{\ell=1}^{\hat{b}-1} K_\ell = \sum_{\ell=1}^{\hat{b}} K_\ell\} \subseteq \{1, \dots, K\}$, where $\sum_{\ell=1}^{0} = 0$. This implies that there are exactly $K_{\hat{b}}$ firms in each sector $\hat{b}$ and $K = \sum_{\hat{b}=1}^{B} K_{\hat{b}}$. Additionally, we denote the ordered values of the fourth column of $\mathbf{X}$ as $(c_{[k]})_{k \in \{1, \dots, K\}}$ and additionally define $c_{[0]} = 0$ and $c_{[K+1]} = 1$.[9] Analogously, for each sector $\hat{b} \in \{1, \dots, B\}$, denote the $K_{\hat{b}}$ ordered values of $(c_i)_{i \in \mathcal{I}_{\hat{b}}}$ as $(c^{\hat{b}}_{[k_{\hat{b}}]})_{k_{\hat{b}} \in \{1, \dots, K_{\hat{b}}\}}$, and additionally set $c^{\hat{b}}_{[0]} = 0$ and $c^{\hat{b}}_{[K_{\hat{b}}+1]} = 1$. Thus, on the whole portfolio

$$0 = c_{[0]} \leq c_{[1]} \leq \ldots \leq c_{[K]} \leq c_{[K+1]} = 1,$$

and on each sector $\hat{b} \in \{1, \dots, B\}$

$$0 = c^{\hat{b}}_{[0]} \leq c^{\hat{b}}_{[1]} \leq \ldots \leq c^{\hat{b}}_{[K_{\hat{b}}]} \leq c^{\hat{b}}_{[K_{\hat{b}}+1]} = 1.$$

4.2 Loss frequency

We will use the framework of point processes to model the arrival of cyber incidents. This allows to naturally incorporate time- and covariate-dependence of the incident frequency and to distinguish between different types of incidents. A comprehensive overview on point processes is given in Refs. [79, 80], whose notation we use. In the following, all random variables are defined on a suitable probability space $(\Omega, \mathcal{F}, \mathbb{P})$, where Ω is the state space, $\mathcal{F}$ a σ-algebra on Ω, and $\mathbb{P}$ a probability measure on $(\Omega, \mathcal{F})$. For our purposes, we focus on simple point processes on the non-negative real line, i.e. processes on the state space $[0, \infty)$ interpreted as time, whose corresponding counting process $(N(t))_{t \geq 0} = \left(|\{i \in \mathbb{N} : t_i \in [0, t]\}| \right)_{t \geq 0}$ has unit increments, where $|\cdot|$ denotes the cardinality, i.e. the number of elements, of a set.

We recall Table 2 for a classification of cyber incidents according to their incident type and root cause: *Idiosyncratic incidents* (targeted attacks and individual failures) are discussed in the next section, *systemic events* (untargeted attacks and mass failures) are addressed subsequently.

[9] Ties can be ordered arbitrarily.

4.2.1 Idiosyncratic incidents

Idiosyncratic incidents are assumed to occur at each firm independently (from incidents at other firms as well as between types of incidents at the same firm). For these types of incidents, we assume that any incident is *successful* in the sense that it breaches the firms IT security measures and causes a loss. This is reasonable, given that targeted attacks are usually tailor-made against one company and furthermore, the majority of non-successful incidents (*near misses*) of this type might not be monitored or recognized.[10]

We assume the arrival of such incidents of each type {DB, BI, FR} at each firm $j \in \{1, \dots, K\}$ to follow an inhomogeneous Poisson process with time- and covariate-dependent rate

$$\lambda^{\cdot,idio}(x_j, t) = \exp\left(f_\cdot(x_j) + g_\cdot(t)\right), \tag{2}$$

where the super-/subscript $\cdot$ stands for one of the incident types $\cdot \in \{DB, FR, BI\}$, the functions $f_\cdot$ additively map (a relevant subset of) the covariates, i.e. $f_\cdot(x) = \alpha_{\lambda,\cdot} + \sum_k f_{\lambda,\cdot,k}(x_{jk})$ for some constant $\alpha_{\lambda,\cdot}$ and $g_\cdot : [0, T] \to \mathbb{R}$ is a measurable function describing the time dependence. The explicit form of the functions $f_\cdot$ and $g_\cdot$ is of course unknown but can be estimated from a suitable data set.[11] The dependence on covariates and time can differ for the three incident types. As an example, if one assumes the rate of data breaches to depend on the covariates x_{j3} (*data*; for targeted attacks), x_{j4} (*IT security*; for failures), and x_{j5} (*number of suppliers*; for supplier attacks) only, this would yield

$$\begin{aligned}\log\left(\lambda^{DB,idio}(x_j, t)\right) &= f_{\lambda^{DB,idio}}(x_{j3}, x_{j4}, x_{j5}) + g_{\lambda^{DB,idio}}(t) \\ &= \alpha_{\lambda,DB} + \sum_{k=3,4,5} f_{\lambda,DB,k}(x_{jk}) + g_{\lambda^{DB,idio}}(t),\end{aligned} \tag{3}$$

where the functions $f_{\lambda,DB,k}$ map factor levels to constants for the ordinal covariates indexed $k \in \{3, 5\}$ (i.e. are naturally measurable) and $f_{\lambda,DB,4}$ is any measurable function of the numerical covariate x_{j4}.

It is clear that for any interval $[\tau_1, \tau_2] \subseteq [0, \infty)$ (set for now $\tau_1 := 0$ and $\tau_2 =: T$), given the covariate matrix $\mathbf{X}$, the number of idiosyncratic incidents of each type arriving at firm j follows a Poisson distribution:

[10] As we assume these attacks to occur due to the firm's characteristics, one might ask if a firm has to simply take its exposure to these types of threats as given. For the occurrence rate of malicious targeted attacks this might be true, but we assume that the impact of a successful attack can be limited by adequate measures (see Sect. 4.3). Furthermore, putting security measures in place mitigates the occurrence of individual failures and potentially implicitly deters targeted attacks as attackers would have to invest more resources to devise an attack vector.

[11] As this ansatz constitutes a standard *generalized additive model*, techniques for parameter estimation are readily available, see, e.g. Ref. [81]. Using the statistical software R, such models can be fit with the function `gam(...,family=poisson)` from the package `mgcv`.

$$\forall j \in \{1, \dots, K\} : N_j^{\cdot,idio}(T) \sim Poi\left(\Lambda_j^{\cdot,idio}(T)\right),$$

where $\Lambda_j^{\cdot,idio}(T) = \int_0^T \lambda_j^{\cdot,idio}(t)\mathrm{d}t$ is the mean measure of the inhomogeneous Poisson process.

As the processes are assumed independent between firms, it follows by superposition that the number of idiosyncratic incidents on the whole portfolio is also Poisson distributed:

$$\sum_{j=1}^{K} N_j^{\cdot,idio}(T) = N^{\cdot,idio}(T) \sim Poi\left(\Lambda^{\cdot,idio}(T)\right), \text{ where } \Lambda^{\cdot,idio}(T) = \int_0^T \Big(\sum_{j=1}^{K} \lambda_j^{\cdot,idio}(t)\Big)\mathrm{d}t.$$

4.2.2 Systemic events

Systemic events cause incidents at multiple firms at the same time and, if of malicious origin, are typically of an opportunistic nature, i.e. a set of firms is affected not because of their specific features or the economic gain attainable from attacking them, but rather due to the availability of an exploitable attack vector against them. This often stems from a common vulnerability, for example a list of bought e-mail-addresses that allows a threat actor to send ransomware to employees of certain firms. In many cases, a common vulnerability would likely affect firms within one industry sector (e.g. if custom software is vulnerable), but of course the common factor can also be unobservable. In any case, to model incidents from systemic events, an extension of the simple point process framework of the previous section is needed. We use the framework of marked point processes, where the process of locations (arrival timepoints of events), now called the *ground process* $N^g(\cdot)$, is a simple[12] point process $\{t_i\}_{i\in\mathbb{N}}$ on the non-negative real line as above, more specifically a non-homogeneous Poisson process with log-rate[13]

$$\log\left(\lambda^{\cdot,g}(t)\right) = g_{\lambda^{\cdot,g}}(t), \tag{4}$$

where the super-/subscript $\cdot$ indicates the event type $\cdot \in \{DB, FR, BI\}$, and again $g_\cdot$ is a measurable function of time. Each arrival of the ground process $\{t_i\}_{i\in\mathbb{N}}$ is then equipped with a mark $(m_i, S_i) \in \mathcal{M} \times \mathcal{S}$ consisting of realisations of components $m_i \in \mathcal{M} := [m_{\min}, m_{\max]} \overset{\text{w.l.o.g.}}{=} [0, 1]$ and $S_i \in \mathcal{S} := \mathcal{P}_K$, such that the resulting process is a marked point process $\left\{t_i, (m_i, S_i)'\right\}_{i\in\mathbb{N}}$ on $[0, \infty) \times (\mathcal{M} \times \mathcal{S})$, where $\mathcal{M} \times \mathcal{S}$ is called the mark space (for a rigorous definition, see Definition 1 in Online Appendix A.1).

[12] As remarked in Ref. [79], by suitably redefining the marks, any marked point process can be represented as a marked point process on the same state space with a simple ground process N^g.

[13] Of course, the log-link is superfluous in this case and might even seem a bit artificial. However, we decide to use this formulation in order to keep consistent with the previous section, especially as we will see the results from both sections being treated jointly later on.

Remark 1 (Interpretation of mark components)

1. $m_i \in \mathcal{M} = [0, 1]$ describes the strength of an event, where strength can be understood e.g. as effectiveness to overcome IT security measures.[14] This is useful to include, as in reality a wide range of sophistication of attacks exists and capturing their strength allows to quantify the effectiveness of IT security measures and the sensitivity of the expected loss to their improvement.
2. $S_i \in \mathcal{S} = \mathcal{P}_K$ encodes the subset of the portfolio affected by an event.

The two components of the mark are used jointly to determine which firms suffer a loss from a given event, namely those firms included in the affected subset whose security level is lower than the strength of the event. With the above notation, an event $\left(t_i, (m_i, S_i)'\right)$

– arrives at time t_i,
– reaches exactly the firms $\left\{j \in S_i\right\}$, and
– causes a loss in exactly the firms $\left\{j \in S_i^*\right\} := \left\{j \in S_i, c_j < m_i\right\}$.

To characterize a marked point process completely, it remains to specify the conditional distribution of the marks, given the locations of the Poisson ground process N_g (see Proposition 6 in Online Appendix A.1). This is done in the following assumptions whose rationality will be detailed below:

Assumption 1 (Conditional mark distribution)

(A1) The joint mark distribution is independent of the location $t \in [0, \infty)$ and the marks $\{(m_i, S_i)'\}_{i\in\mathbb{N}}$ are independent and identically distributed (iid.).
(A2) The two mark components $\{m_i\}_{i\in\mathbb{N}}$ and $\{S_i\}_{i\in\mathbb{N}}$ are independent, where the distribution of m_i is given by the cdf F_M (with pdf f_M) and the distribution of S_i is given by a (discrete) pmf f_S.
(A3) m_i follows a continuous Uniform distribution on $\mathcal{M} = [0, 1]$.
(A4) The distribution of S_i is generated by distinguishing between general and sector-specific events. Given the event type, firms in the relevant subset are affected with identical probability and independently from each other. More specifically, assume there are r.v. $Z_{ij} \in \{0, 1\}$ – such that $\{j \in S_i\} \iff Z_{ij} = 1$ – whose distribution depends on independent r.v. $G_i \sim Ber(p_G)$ and B_i following some categorical distribution on $\{1, \ldots, B\}$ with probability $\{p_1, \ldots, p_B\}$ (G_i determines whether the event is sector-specific ($G_i = 1$) or general ($G_i = 0$); B_i determines the affected sector in the former case). Then let

[14] For example, a simple phishing e-mail that would immediately be classified spam is rather weak, whereas a sophisticated exploit designed to circumvent state-of-the-art security systems is rather strong.

$$\mathbb{P}(Z_{ij} = 1 \mid G_i = 0) = p_{gen} \quad \text{iid. } \forall j \in \{1, \dots, K\},$$
$$\mathbb{P}(Z_{ij} = 1 \mid G_i = 1, B_i = \hat{b}) = \begin{cases} p_{sec} & \text{iid. } \forall j \in \mathcal{I}_{\hat{b}}, \\ 0 & \text{else.} \end{cases}$$

Of course, p_G, p_{sec}, $p_{gen} \in [0,1]$ and $p_b \in [0,1]$, $\forall b \in \{1, \dots, B\}$, s.t. $\sum p_b = 1$. We exclude the cases $p_G = p_{gen} = 0$ and $(1 - p_G) = p_{sec} = 0$, which lead to the uninteresting case $\mathbb{P}(S_i = \emptyset) = 1$.

A concrete distributional assumption for a model should ideally be backed by empirical evidence. As this is currently not possible due to data scarcity in the cyber domain, we stick to the principle of imposing as little (unknown) prior information as possible. This justifies (A1) and (A2), as we do not have any evidence that would suggest deviating from iid., to introduce any particular dependence, neither between locations and marks, nor between the components of the mark. Similarly, regarding (A3), one might intuitively rather assume the number of very weak attacks (such as easily recognizable spam e-mails) to be higher than the number of very sophisticated attacks. However, as we do not have statistical evidence that would allow to choose a particular distribution, we use a Uniform distribution (maximum entropy distribution among all continuous distributions on a bounded interval [82]). Considering (A4), several industry experts have highlighted in conversations with us the importance of industry sector-specific systemic events. Thus, we incorporate this idea in our model, while again leaving the distribution as simplistic as possible (conditionally iid. Bernoulli draws). Furthermore, note that due to the modular structure of the model, each assumption can be altered or replaced individually if suitable data indicates the necessity, without compromising the general model structure.

4.2.3 Properties of the model

In the following, we detail properties of the model and their interpretation in the cyber insurance context. As proofs mostly rely on standard techniques, they are given in Online Appendix A.3.

Proposition 1 (Distribution of number of incidents and losses) *Under* (A4)*, the number of incidents per event* $\{|S_i|\}_{i \in \mathbb{N}}$ *follows a Binomial mixture distribution, i.e.* $f_{|S_i||n,p}(k) = Binom(n, p, k)$ *with*

$$(n, p) = \begin{cases} (K, p_{gen}) \text{ with weight } (1 - p_G), \\ (K_{\hat{b}}, p_{sec}) \text{ with weight } p_G\, p_{\hat{b}}, \quad \hat{b} \in \{1, \dots, B\}. \end{cases} \tag{5}$$

Similarly, under (A3) *and* (A4)*, the number of losses per event* $\{|S_i^*|\}_{i \in \mathbb{N}}$ *follows a Binomial mixture distribution, i.e.* $f_{|S_i^*||n,p}(k) = Binom(n, p, k)$ *with*

$$(n, p) = \begin{cases} (K^*, p_{gen}) & \text{with weight } (1 - p_G)\,(c_{[K^*+1]} - c_{[K^*]}), \quad K^* \in \{0, \dots, K\}, \\ (k^*_{\hat{b}}, p_{sec}) & \text{with weight } p_G\, p_{\hat{b}}\,(c^{\hat{b}}_{[k^*_{\hat{b}}+1]} - c^{\hat{b}}_{[k^*_{\hat{b}}]}), \quad k^*_{\hat{b}} \in \{0, \dots, K_{\hat{b}}\},\ \hat{b} \in \{1, \dots, B\}. \end{cases} \tag{6}$$

Notice that the distribution of $\{|S_i^*|\}_{i\in\mathbb{N}}$ implies the distribution of $\{|S_i|\}_{i\in\mathbb{N}}$ as the special case where $c_{[k]} = 0, \forall k \in \{1,\dots,K\}$, i.e. the worst-case scenario where no firm has any IT security measures in place and thus the number of incidents and losses is equivalent.

Proposition 2 (Conditional incident and loss probability) *For a firm $j_1 \in \{1,\dots,K\}$ in sector b_{j_1}, the probability of being affected by an event, given the information that another firm $j_2 \in \{1,\dots,K\}$ in sector b_{j_2} has been affected (i.e. the conditional incident probability), is given by*

$$\mathbb{P}(j_1 \in S_i \mid j_2 \in S_i) = \begin{cases} \dfrac{p_{sec}^2\, p_{b_{j_2}}\, p_G + p_{gen}^2\,(1-p_G)}{\tilde{p}(b_{j_2})}, & b_{j_1} = b_{j_2}, \quad (7a) \\ \dfrac{p_{gen}^2\,(1-p_G)}{\tilde{p}(b_{j_2})}, & b_{j_1} \neq b_{j_2}, \quad (7b) \end{cases}$$

where

$$\tilde{p}(b_j) := \mathbb{P}(j \in S_i \mid b_j) = p_G\, p_{b_j}\, p_{sec} + (1-p_G)\, p_{gen} \tag{8}$$

is the (unconditional) incident probability for each firm, given its industry sector.

Likewise, for the conditional loss probabilities,

$$\mathbb{P}(j_1 \in S_i^* \mid j_2 \in S_i^*) = \begin{cases} \dfrac{p_{sec}^2\, p_{b_{j_2}}\, p_G + p_{gen}^2\,(1-p_G)}{\tilde{p}(b_{j_2})}, & b_{j_1} = b_{j_2},\ c_{j_1} \le c_{j_2}, \quad (9a) \\ \dfrac{p_{gen}^2\,(1-p_G)}{\tilde{p}(b_{j_2})}, & b_{j_1} \neq b_{j_2},\ c_{j_1} \le c_{j_2}, \quad (9b) \\ \dfrac{\bar{F}_M(c_{j_1})}{\bar{F}_M(c_{j_2})}\Big(\dfrac{p_{sec}^2\, p_{b_{j_2}}\, p_G + p_{gen}^2\,(1-p_G)}{\tilde{p}(b_{j_2})}\Big), & b_{j_1} = b_{j_2},\ c_{j_1} > c_{j_2}, \quad (9c) \\ \dfrac{\bar{F}_M(c_{j_1})}{\bar{F}_M(c_{j_2})}\Big(\dfrac{p_{gen}^2\,(1-p_G)}{\tilde{p}(b_{j_2})}\Big), & b_{j_1} \neq b_{j_2},\ c_{j_1} > c_{j_2}, \quad (9d) \end{cases}$$

where the unconditional loss probability is given by

$$\mathbb{P}(j \in S_i^* \mid b_j) = \bar{F}_M(c_j)\,\big(p_G\, p_{b_j}\, p_{sec} + (1-p_G)\, p_{gen}\big) = \bar{F}_M(c_j)\,\tilde{p}(b_j). \tag{10}$$

The above results are interesting from a practical viewpoint: If an insurer is notified about a cyber incident by one of its policyholders (many policies include mandatory immediate notification or even the provision of an immediate-response-team

by the insurer), it is worthwhile to find (and warn!) firms with a high conditional probability of having been affected by the same event, thus potentially giving them the chance to avert the actual manifestation in their firm (e.g. by warning employees about a phishing threat or updating vulnerable software). The information about an incident in one firm always has a non-negative effect on the incident probabilities for other firms of the same sector ((7a) vs. (8); a formal proof of this statement is given in Online Appendix A.3), while the effect can go in either direction for firms of different sectors ((7b) vs. (8)). For a detailed illustration, see Fig. 1. The same holds for the information of a suffered loss, i.e. the probability of suffering a loss increases with the knowledge that another firm of the same sector has suffered a loss, and the increase is larger if the harmed firm's IT security level exceeds the one of the firm under consideration.

Analogously to the notation in the previous section, for any interval $[0, T] \subseteq [0, \infty)$, given the arrival process $\{t_i, (m_i, S_i)'\}_{i\in\mathbb{N}}$ and the covariate matrix $\mathbf{X}$, the number of incidents $\bar{N}_j^{\cdot,syst}$ resp. losses $N_j^{\cdot,syst}$ at each firm follows a Poisson process, where the rate can be obtained by thinning the ground process $N^{\cdot,g}$ of arrivals $\{t_i\}_{i\in\mathbb{N}}$ appropriately (see Ref. [83] and Proposition 5 in Online Appendix A.1). In particular

$$\bar{N}_j^{\cdot,syst}(T) = \sum_{i=1}^{N^{\cdot,g}(T)} \mathbb{1}_{\{j\in S_i\}} \sim Poi\big(\tilde{p}(b_j)\Lambda^{\cdot,g}(T)\big),$$

$$N_j^{\cdot,syst}(T) = \sum_{i=1}^{N^{\cdot,g}(T)} \mathbb{1}_{\{j\in S_i^*\}} \sim Poi\big(\tilde{p}(b_j)\bar{F}_M(c_j)\Lambda^{\cdot,g}(T)\big).$$

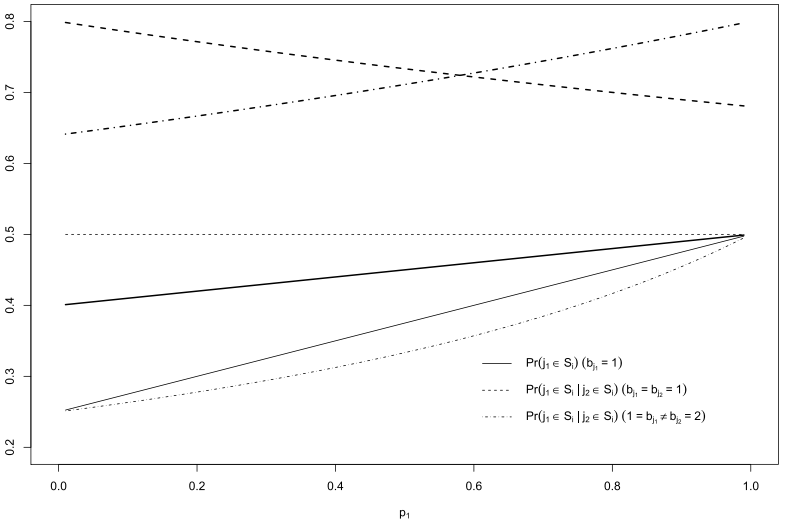
Contrary to the previous section, we cannot transition to the portfolio level by simple superposition due to lack of independence between firms. Instead, we express the cumulative number of incidents $\bar{N}^{\cdot,syst}(T)$ resp. losses $N^{\cdot,syst}(T)$ across the entire portfolio for fixed $T > 0$ as a *compound Poisson* distributed r.v.

$$\bar{N}^{\cdot,syst}(T) = \sum_{i=1}^{N^{\cdot,g}(T)} |S_i| \quad \text{and} \quad N^{\cdot,syst}(T) = \sum_{i=1}^{N^{\cdot,g}(T)} |S_i^*|,$$

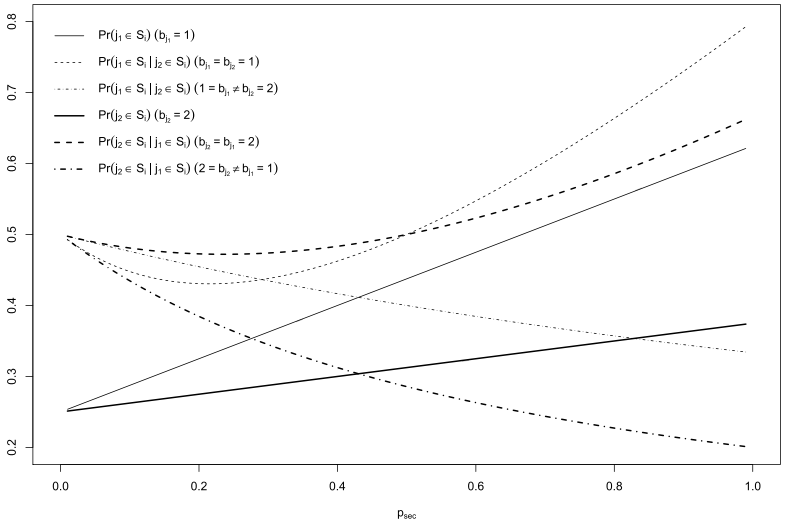
where $N^{\cdot,g}(T) \sim Poi\Big(\int_0^T \lambda^{\cdot,g}(t)\mathrm{d}t\Big)$ and $\{|S_i|\}_{i\in\mathbb{N}}$ resp. $\{|S_i^*|\}_{i\in\mathbb{N}}$ are iid. mixed Binomial and independent from $N^{\cdot,g}(T)$.[15] Using well-known results for the calculation of the expectation and variance of a compound Poisson r.v. (details in Refs. [84, 85] and Online Appendix A.2), this yields:

Proposition 3 (Overdispersion of systemic incident/loss numbers) *Assume* $K > 1$ *and* $K_{\hat{b}} > 1$ *for at least one* $\hat{b} \in \{1, \dots, B\}$ *with* $p_{\hat{b}} > 0$. *Then, the cumulative number*

[15] The notation $\bar{N}$ and N alludes to the fact that the number of incidents can always be considered a worst-case bound for the number of losses (counterfactual analysis: what had happened if no security was in place at all); in particular, for a given realisation $\{t_i, (m_i, S_i)\}_{i:t_i\in[0,T]}$ always $\bar{N}^{\cdot,syst}(T) \geq N^{\cdot,syst}(T)$.



(a)



(b)

Fig. 1 We illustrate the effect of the information that a firm of the same (resp. a different) sector has been affected by an event on the incident probability for just two sectors. (**a**) shows the (un) conditional probabilities for a firm from sector 1 dependent on p_1. The other parameters are chosen as $p_G = p_{sec} = p_{gen} = 0.5$ (thin lines) or $p_G = 0.5, p_{sec} = 0.2, p_{gen} = 0.8$ (thick lines), such that one observes that for $b_{j_1} \neq b_{j_2}$, the conditional probabilities can be above or below the unconditional one (solid line), whereas for $b_{j_1} = b_{j_2}$, the conditioning has a non-negative effect in both cases. Likewise in (**b**), for $p_G = 0.5, p_{gen} = 0.5, p_1 = 1 - p_2 = 0.75$, probabilities for all cases are shown dependent on p_{sec}. Observe again that conditioning on the same sector has a non-negative effect, whereas when conditioning on the other sector, there is an intersection $\mathbb{P}(j_1 \in S_i) = \mathbb{P}(j_1 \in S_i \mid j_2 \in S_i)$ (and $\mathbb{P}(j_2 \in S_i) = \mathbb{P}(j_2 \in S_i \mid j_1 \in S_i)$) at $p_{sec} = 0.4305$

of incidents resp. losses from systemic events is overdispersed, i.e. has a dispersion index (DI = variance-to-mean ratio) exceeding 1.

$$DI\big(\bar{N}^{\cdot,syst}(T)\big) := \frac{\mathbb{V}ar\big[\bar{N}^{\cdot,syst}(T)\big]}{\mathbb{E}\big[\bar{N}^{\cdot,syst}(T)\big]} = 1 + \frac{(1-p_G)\,p_{gen}^2\,(K^2-K) + p_G\,p_{sec}^2\,\sum_{\ell=1}^{B} p_\ell (K_\ell^2 - K_\ell)}{(1-p_G)\,K\,p_{gen} + p_G\,p_{sec}\,\sum_{\ell=1}^{B} p_\ell\,K_\ell} > 1,$$

$$DI\big(N^{\cdot,syst}(T)\big) = 1 + \frac{(1-p_G)\,\sum_{k^*=0}^{K} p_{gen}^2((k^*)^2-k^*)(c_{[k^*+1]}-c_{[k^*]}) + p_G\,\sum_{\ell=1}^{B}\sum_{k_\ell^*=0}^{K_\ell} p_{sec}^2 p_\ell((k_\ell^*)^2-k_\ell^*)(c^\ell_{[k_\ell^*+1]}-c^\ell_{[k_\ell^*]})}{(1-p_G)p_{gen}\,\sum_{k^*=0}^{K} k^*(c_{[k^*+1]}-c_{[k^*]}) + p_G p_{sec}\,\sum_{\ell=1}^{B}\sum_{k_\ell^*=0}^{K_\ell} p_\ell k_\ell^*(c^\ell_{[k_\ell^*+1]}-c^\ell_{[k_\ell^*]})} > 1.$$

It is well-known that the Poisson distribution exhibits equidispersion ($DI = 1$), while empirical studies in non-life insurance often report overdispersed claim count data and therefore recommend to use alternative distributions (e.g. negative Binomial) to model claim counts. Proposition 3 shows that our construction using a marked Poisson process to allow simultaneous arrivals of several incidents (resp. losses) due to one systemic event likewise is able to introduce overdispersion.

4.2.4 Summary: loss frequency model

Recall that idiosyncratic incidents arrive to each firm $j \in \{1, \dots, K\}$ independently as inhomogeneous Poisson processes with rates $\lambda_j^{\cdot,idio}(t)$, $\cdot \in \{DB, FR, BI\}$. Each incident is assumed to cause a loss. For a fixed time $T > 0$, the overall number of losses caused by idiosyncratic incidents up to this time $N^{\cdot,idio}(T)$ follows a Poisson distribution with rate $\Lambda^{\cdot,idio}(T) = \int_0^T \Big(\sum_{j=1}^{K} \lambda_j^{\cdot,idio}(t)\Big)\mathrm{d}t$.

Systemic events arrive to the portfolio with overall rates $\lambda^{\cdot,g}(t)$. Each arrival t_i carries a mark including the strength of the event m_i and the affected subset S_i. An event at time t_i thus causes incidents in all firms in the set $\{j \in S_i\}$ and causes losses in its subset $\{j \in S_i^*\} = \big\{j \in S_i, c_j < m_i\big\}$. The total number of incidents and losses from systemic events up to time $T > 0$, $\bar{N}^{\cdot,syst}(T)$ resp. $N^{\cdot,syst}(T)$, follow a compound Poisson distribution with mixed Binomial jump sizes.

Aggregating the number of incidents and losses from both root causes on the level of each individual firm translates to aggregating two independent Poisson r.v.

$$N_j^{\cdot}(T) := N_j^{\cdot,idio}(T) + N_j^{\cdot,syst}(T) \sim Poi\big(\Lambda_j^{\cdot,idio}(T) + \tilde{p}(b_j)\bar{F}_M(c_j)\Lambda^{\cdot,g}(T)\big) =: Poi\big(\Lambda_j^{\cdot}(T)\big). \tag{11}$$

On the portfolio level, we aggregate two independent compound Poisson r.v. (one with jumps of constant size 1 and one with mixed Binomial jump sizes), which yields (see Proposition 7 in Online Appendix A.2):

$$N^{\cdot}(T) := N^{\cdot,idio}(T) + N^{\cdot,syst}(T) \overset{d}{=} \sum_{i=1}^{N(T)} Y_i, \tag{12}$$

where $N(T) \sim Poi\big(\Lambda^{\cdot,idio}(T) + \Lambda^{\cdot,g}(T)\big)$ and $\{Y_i\}_{i\in\mathbb{N}}$ are iid., independent of $N(T)$, with mixture distribution

$$F_{Y_i}(n) = \frac{\Lambda^{\cdot,idio}(T)}{\Lambda^{\cdot,idio}(T) + \Lambda^{\cdot,g}(T)} \mathbb{1}_{[1,\infty)}(n) + \frac{\Lambda^{\cdot,g}(T)}{\Lambda^{\cdot,idio}(T) + \Lambda^{\cdot,g}(T)} F_{|S_i^*|}(n), \ n \in \mathbb{N}_0.$$

Note that so far, we have kept the numbers of losses of different types {DB, FR, BI} separate. In general, assuming independence between them, they could be aggregated into one arrival process, but this may not be desirable as also the loss severity distributions might be different (see Sect. 3.2.3), and therefore for the determination of the portfolio loss their numbers have to be taken into account separately.

4.3 Loss severity

After describing the model of the cumulative number of cyber incidents and losses in the last section, we now turn to their impact, i.e. let $L_{ij} := L_j(t_i)$ be a r.v. describing the non-negative monetary loss caused by a cyber incident reaching firm $j \in \{1, \dots, K\}$ at time $t_i \in [0, T]$. Based on previous findings from academic literature and the arguments in Sect. 3.2.3, we model the body and tail of the loss severity distribution separately and allow the parameters of the distributions to exhibit time- and covariate-dependence. Specifically, for all types of incidents, we suggest using a combination of log-normal and generalized Pareto distribution based on the findings of Ref. [56]. Other promising approaches (e.g. based on Refs. [49] and [72] for DBs or based on Ref. [75] for BIs) are detailed in Online Appendix A.4.

As we do not rely on empirical data, we first need to set a threshold between body and tail of the to-be-constructed distribution. Therefore, we first assume an underlying log-normal distribution $\widetilde{L}_{ij}^{\cdot} \sim LN(\mu_{ij}^{\cdot}, \sigma^{\cdot})$ and select a high quantile as threshold, e.g. set $u_{ij}^{\cdot} = q_z(\widetilde{L}_{ij}^{\cdot})$ with e.g. $z = 0.95$. Given the threshold, construct the density $f_{L_{ij}}$ of the loss distribution as[16]

$$\begin{aligned} f_{L_{ij}^{\cdot}}(l) &= \begin{cases} z\, f_{TruncLN}(l; \mu_{ij}^{\cdot}, \sigma^{\cdot}, 0, u_{ij}^{\cdot}), & l \in [0, u_{ij}^{\cdot}], \\ (1-z)\, f_{GPD}(l; u_{ij}^{\cdot}, \xi_{ij}^{\cdot}, \beta_{ij}^{\cdot}), & l \in (u_{ij}^{\cdot}, \infty), \end{cases} \\ \mu_{ij}^{\cdot} &= \alpha_{\mu,\cdot} + \sum_k f_{\mu,\cdot,k}(x_{jk}) + g_{\mu,\cdot}(t_i), \\ \xi_{ij}^{\cdot} &= \alpha_{\xi,\cdot} + \sum_k f_{\xi,\cdot,k}(x_{jk}) + g_{\xi,\cdot}(t_i), \\ \beta_{ij}^{\cdot} &= f_{\beta,\cdot}(x_j, t_i), \end{aligned} \tag{13}$$

where $TruncLN(\mu, \sigma, x_{\min}, x_{\max})$ denotes a truncated log-normal distribution on the interval $[x_{\min}, x_{\max}]$ and $GPD(u, \xi, \beta)$ denotes a generalized Pareto distribution with

[16] Note that when fitting a spliced severity distribution as below, in order to apply established fitting procedures, one would usually select a global, non-covariate-dependent threshold u and fit each distribution onto the data that fall into the "globally" specified regions. As we do not address the question of model fitting here, we stick to the more general formulation, as it is interesting to assume that depending on the covariates, the classification of a severity as *extreme* should start at different levels.

location u, shape ξ, and scale β.[17] As for the idiosyncratic frequency modelling illustrated in Sect. 4.2.1, the sum might run over different subsets of covariates for different incident types (see e.g. Eq. (3)).

Next, we combine the concepts for frequency and severity modelling to study some questions that arise from an actuarial viewpoint.

4.4 Insurance pricing and risk measurement

Recall that we take the perspective of an insurer, whose portfolio consists of K firms exposed to cyber losses whose frequency and severity are modelled as detailed in Sects. 4.2 and 4.3. Questions of interest for the insurer when setting up a portfolio of cyber insurance policies typically include:

1. Contract design (deductibles, cover limits, coverage period);
2. Pricing of individual policies given an applicant's characteristics;
3. Estimation and quantification of the portfolio risk.

In this work, we do not elaborate in detail on the first question and for now assume no deductible, no cover limit, and a standard policy duration of one year. These assumptions imply that for each incident, the loss suffered by the insured firm and the claim size faced by the insurer are equal and the terms will be used interchangeably. To study the latter two questions, the *total claim amount process* is denoted

$$L(t) = \sum_{i=1}^{N(t)} Y_i, \quad t \geq 0,$$

where it is assumed that the claim number process $(N(t))_{t\geq 0}$ is independent of the iid., a.s. positive, claim size sequence $\{Y_i\}_{i\in\mathbb{N}}$. We restrict our focus to the case of fixed $T > 0$, i.e. instead of studying the process $(L(t))_{t\geq 0}$, study the random variable $L(T)$. In general, it is very hard to make statements about the exact distribution of L and one has to resort to Monte Carlo methods or, if applicable, a numerical routine like the *Panjer recursion*.

In our context, the loss for a firm $j \in \{1, \ldots, K\}$ up to time $T > 0$ from one type of cyber incidents (e.g. data breaches) can be expressed as

$$L_j^{\cdot}(T) = \sum_{i=1}^{N_j^{\cdot}(T)} L_i^{\cdot,(j)},$$

[17] Note that when fitting a GPD with covariate-dependent parameters using the method developed in Ref. [57], an orthogonal reparametrization $(\xi(x_j,t), \nu(x_j,t)) := (\xi(x_j,t), \log(\beta(x_j,t)(1+\xi(x_j,t))))$ is chosen. The resulting MLE $\hat{\nu}$ can be transformed back directly to an estimator $\hat{\beta}$, but the dependence of β on the covariates does then not follow a GAM structure anymore. Therefore, a more general functional relationship is stated above.

where $N_j^{\cdot}(T) \sim Poi\big(\Lambda_j^{\cdot}(T)\big)$ as given in Eq. (11) and $\{L_i^{\cdot,(j)}\}_{i\in\mathbb{N}} := \{Y^{\cdot,(j)}(t_i)\}_{i\in\mathbb{N}}$ with pdf. $f_{L_{ij}^{\cdot}}$ as given in Eq. (13). Note that in general the sequence $\{L_i^{\cdot,(j)}\}_{i\in\mathbb{N}}$ is not iid. (due to time-dependence). However, if we drop time-dependence, which in practice could mean assuming constant severity distributions on one-year intervals considered separately, $L_j^{\cdot}(T)$ is again compound Poisson, and the total cyber loss incurred by firm $j \in \{1, \dots, K\}$ is given by

$$L_j(T) = \sum_{i=1}^{N_j(T)} L_i^{(j)}, \text{ where } N_j(T) \sim Poi\big(\Lambda_j^{DB}(T) + \Lambda_j^{FR}(T) + \Lambda_j^{BI}(T)\big),$$

$$\text{and } F_{L_i^{(j)}} = \sum_{y\in\{DB,FR,BI\}} \frac{\Lambda_j^{y}(T)}{\Lambda_j^{DB}(T) + \Lambda_j^{FR}(T) + \Lambda_j^{BI}(T)} F_{L_i^{y,(j)}}.$$

The portfolio loss is simply given by the sum of (dependent) firm losses, i.e.

$$L^{\cdot}(T) = \sum_{j=1}^{K} L_j^{\cdot}(T) \text{ and } L(T) = \sum_{j=1}^{K} L_j(T).$$

Regarding the second question of finding a premium $\Pi(T)$ for an individual insurance policy on $[0, T]$, we recall the well-known premium calculation principles listed below [86]. As it is often impossible to find the exact distributional properties of the total claim amount process, the ones based on the first two moments are popular in practice.

- Expected value principle: $\Pi_j(T) = (1+\rho)\mathbb{E}\big[L_j(T)\big]$, with safety loading $\rho > 0$.
- Standard deviation principle: $\Pi_j(T) = \mathbb{E}\big[L_j(T)\big] + \rho\sqrt{\mathbb{V}ar\big(L_j(T)\big)}$, where $\rho > 0$.
- Exponential principle: $\Pi_j(T) = \frac{1}{\gamma}\log\big(\mathbb{E}[e^{\gamma L_j(T)}]\big)$, with risk aversion $\gamma > 0$.

Concerning the question of quantifying the risk of the overall portfolio loss, the two most common tail risk measures are the *Value-at-Risk (VaR)* at a given confidence level $1-\alpha$ and, if applicable, the corresponding *Average Value-at-Risk (AVaR)*. Theoretically, for a positive loss r.v. L with cdf F_L, they are given by

$$VaR_{1-\alpha}(L) := \inf\big\{l \in \mathbb{R} : \mathbb{P}(L \le l) \ge 1-\alpha\big\} = F_L^{-1}(1-\alpha),$$

$$AVaR_{1-\alpha}(L) := \mathbb{E}\big[L \big| L \ge VaR_{1-\alpha}(L)\big] \overset{(*)}{=} \frac{1}{1-\alpha}\int_0^{1-\alpha} VaR_{\gamma}(L)\mathrm{d}\gamma,$$

where F_L^{-1} denotes the generalized inverse of F_L and $(*)$ requires F_L to be continuous. Note that in cases with very heavy-tailed loss severities (as e.g. observed in some of the previous works on cyber risk), $AVaR(L)$ cannot be computed as it relies on L to have finite expectation.

5 An example of an actuarial application via a simulation study

The aim of the following section is to illustrate the application of the proposed modelling approach to pricing and risk measurement in an actuarial context. To this end, a fictitious insurance portfolio is constructed and parameters for the frequency and severity distributions as given in the previous sections are proposed based on previous academic literature and expert judgement. Based on the resulting simulated portfolio loss distribution, the effect of interdependent losses and the introduction of cover limits is highlighted. Due to the scarcity of available empirical data, the parameters and model assumptions could not yet be fit to (resp. challenged on) a real dataset; this remains an important task for future research.

5.1 Portfolio composition and company covariates

We first construct a (fictitious) insurance portfolio consisting of $K = 50$ firms from $B = 6$ sectors, all details are listed in Table 3. A bigger portfolio, which is used in our simulation study, is then obtained by copying each firm 10 times with IT security levels varying from 0.05 to 0.95 (stepsize 0.1). This enables us to compare the results of the entire portfolio ($K = 500$) with sub-portfolios ($K = 50$) of different security level (denoted sub-portfolio 1 – 10), and for each individual firm with varying security level. Table 4 gives an overview of the relative and absolute frequencies for each covariate in each sub-portfolio.

5.2 Frequency distribution

We require our simulation to adhere to the following stylized facts (F1)–(F5) for the frequency of idiosyncratic incidents:

(F1) Consider a $T = 5$-year observation period, during which the frequency increases by around 67% [3]. The increase is realized in yearly (log-linear) steps; within each year the frequency is assumed constant.

(F2) During the first year ($t \in [0, 1)$) and for baseline covariate levels $s_j = d_j = nsup_j = 1, c_j = 0.5$, the incident (loss) probability is 0.01 (this is a conservative estimate).

(F3) Incidents are distributed into 25% DBs [56], 25% BIs, and 50% FR (or *other*).
(F4) An increase of either of the categorical covariates s_j, d_j, and $nsup_j$ by one (two) level(s) from the baseline implies an increase of the incident rate by 10% (20%).
(F5) Assume a log-linear influence of the security level such that increasing it to the maximum ($c_j = 1$) yields a halved rate of cyber incidents (and thus lowering it to the minimum ($c_j = 0$) leads to a doubled rate), compared to the baseline.

These assumptions imply the parameters for the covariate-dependent rates of idiosyncratic incidents (c.f. Eq. (2)) in the upper panel of Table 5.[18] For systemic events, we follow Sect. 4.2.2, where the assumed parameters for the ground process (c.f. Eq. (4)) and the mark distribution are given in the lower panel of Table 5. Although it is difficult to make assumptions, as none of the existing studies explicitly distinguish systemic events, Table 5 reflects the following simplifying assumptions (F6), (F7) (as before, we do not have any information to justify any more complex assumptions):

(F6) The mark distribution is equal for DB, BI, and FR. Sector-specific events are (discretely) uniformly distributed over all sectors.
(F7) The number of incidents from systemic events is similar to the number of idiosyncratic incidents for baseline covariate levels, which implies a doubled overall incident frequency (and a 50% increased loss frequency).

5.3 Severity distribution

For this study, we deviate from the very high mean (resp. median) severity estimates given in the existing literature (several million US$ for a single incident) for two reasons: First, it is reasonable that events listed in public databases exhibit much higher losses than the average *daily-life* cyber incident that goes unnoticed by the public and second, insurance policies currently offered on the market (especially policies for SMEs) usually have cover limits of up to 5 million US$, therefore it would not be reasonable to assume mean claim severities that already exhaust the policy limit.[19] Recall that this study is intended as a prototype to show the general behaviour of the model; absolute numbers given should not be interpreted as representative of

[18] To illustrate how these parameters relate to the assumptions, take the example of (F4): The increase of the idiosyncratic rate of some type of incident when increasing a categorical covariate by one level from the benchmark (where the benchmark is represented by the intercept) is given by $\lambda^{\cdot,idio}((x_{j1}, 2, x_{j3}, x_{j4}, x_{j5}), t)/\lambda^{\cdot,idio}((x_{j1}, 1, x_{j3}, x_{j4}, x_{j5}), t) = \exp(f_{\lambda,\cdot,2}(2))$. Equating this ratio to 1.1, i.e. assuming a c.p. 10% increase, yields $f_{\lambda,\cdot,2}(2) = 0.095$. Likewise, equating $\lambda^{\cdot,idio}((x_{j1}, 3, x_{j3}, x_{j4}, x_{j5}), t)/\lambda^{\cdot,idio}((x_{j1}, 1, x_{j3}, x_{j4}, x_{j5}), t) = \exp(f_{\lambda,\cdot,2}(3))$ to 1.2, i.e. assuming a c.p. 20% increase, yields $f_{\lambda,\cdot,2}(3) = 0.18$.

[19] Note that as the existing studies do not state whether the recorded cyber losses were fully or partly insured, it is not possible to make statements about the relationship between those losses and the size of potentially corresponding insurance claims.

a real-world portfolio. The following assumptions (S1)–(S7) lead to the choice of parameters given in Table 6:

(S1) During the first year and for baseline covariate levels, for all types of incidents the expected claim size of the underlying log-normal distribution is given by $\mathbb{E}[\widetilde{L}_{ij}] = 50$.

(S2) The standard deviation of the underlying log-normal cost distribution is constant and consistent with the results for (negligent) data breaches in Refs. [49] and [72].

(S3) The expected claim size $\mathbb{E}[\widetilde{L}_{ij}]$ increases by 10% (20%) for a one (two) level increase of either s_j or d_j relative to the benchmark. The influence of c_j on $\mathbb{E}[\widetilde{L}_{ij}]$ is log-linear, where $c_j = 1$ results in a halved expected claim size.

(S4) Over the $T = 5$-year observation period, $\mathbb{E}[\widetilde{L}_{ij}]$ increases (in yearly log-linear steps) by 60%.

(S5) For *large claims*, the shape parameter ξ of the GPD is constant and close to 1 [56] to model heavy-tailed behaviour while avoiding a switch from a finite-mean to an infinite-mean scenario.

(S6) The expected threshold exceedance (relative to the corresponding threshold, dependent on the underlying log-normal distribution) $\mathbb{E}[L_{ij} - u_{ij} \mid L_{ij} > u_{ij}]/u_{ij} = \beta_{ij}\,(u_{ij}(1-\xi_{ij}))^{-1}$ equals 0.5 for baseline covariate levels, i.e. the expected size of a claim exceeding the threshold is given by 1.5 times the threshold.

(S7) The same assumptions regarding covariate- and time-dependence as for small claims are made, referring to the expected relative threshold exceedance (e.g. a one-level increase of s_j leads to a 10% increase) instead of the expected claim size. In this case, the influence of c_j is linear and such that $c_j = 1$ results in a halved expected relative threshold exceedance.[20]

5.4 Results of the simulation study

The following results are based on 50.000 simulation runs on a grid of 5 years, reported values refer to the first year unless stated otherwise. For each run, the arrival times of idiosyncratic incidents (at each firm) and systemic events are generated using the rates in Eqs. (2) and (4), respectively. For each systemic event, the affected subset S_i is generated as described in (*A*4) using r.v. G_i, B_i, and Z_{ij} from their respective distributions. Furthermore, m_i is drawn and the set S_i^* deduced from the realisations of S_i and m_i. This

[20] Assumptions (S6) and (S7) result in equations for β of the type $\beta_{ij}^{\cdot} = u_{ij}^{\cdot}\,(1-\xi^{\cdot})\,(\alpha_{\beta,\cdot} + \sum f_{\beta,\cdot,k}(x_{jk}) + g_{\beta,\cdot}(t))$ with coefficients given in Table 6 which do not strictly fit into the framework of [57] for fitting a covariate-dependent GPD. When calibrating the model to data, it is not required to make any such assumption. Note, however, that due to the reparametrization in the framework of [57], the covariate dependence of β is not intuitive. Therefore, we stick to intuitively interpretable assumptions.

Table 3 List and modelling framework of company covariates to be included in a cyber risk model

Covariate	Abbreviation	Type	Scope	Information availability	Comment
Industry sector	*b*	Categorical	FI: finance and insurance BR: businesses (retail) HC: healthcare EDU: education GOV: government and military MAN: manufacturing	Public data	All but the last sector are covered in the PRC dataset and therefore used in the works using that data (e.g. Refs. [50–52]) Sector found as relevant covariate in Refs. [3, 5, 51, 52, 54, 55].
Size	*s*	Ordinal	1 Small 2 Medium 3 Large	Public data or questionnaire	Usually, for the size determination of an enterprise, revenue and number of employees should be used jointly. For details, see Table 11 in Online Appendix A.7. Size found as relevant covariate in Refs. [53–55].
Data	*d*	Ordinal	1 Low risk 2 Medium risk 3 High risk	Self-report via questionnaire, otherwise approximate using public data about industry sector and size	Data found as relevant covariate in Refs. [52, 55, 72]. Usually considered for insurance pricing [15]. Risk classification should take into account number of records and type of data (e.g. PII, PHI, credit card data is more sensitive), see Table 12 in Online Appendix A.7.

Table 3 (continued)

Covariate	Abbreviation	Type	Scope	Information availability	Comment
IT security level	c	Numerical	$[c_{min}, c_{max}] \overset{\text{w.l.o.g.}}{=} [0, 1]$	Self-report via questionnaire or e.g. scrutiny by a service provider hired by the insurer	Relevance is clear, but e.g. emphasized in Refs. [5, 60]. Usually taken into account for insurance pricing [15].
Number of suppliers	*nsup*	Ordinal	1 Low 2 Medium 3 High	Hard to elicit, could be estimated from industry sector and size, or via questionnaire	Depends on sector and number of employees. For details, see Table 13 in Online Appendix A.7. Relevant for exposure to supplier attacks.

yields an overall number of losses and incidents for each firm on each step of the grid, such that the corresponding severities can be drawn from the appropriate (time- and covariate-dependent) distribution.

5.4.1 Cumulative loss distribution

First, we examine the number of incidents/losses and the distribution of cumulative losses in the full portfolio ($K = 500$) in Fig. 2a and b. We compare the case where only actual losses are counted with the case where all incidents are counted (i.e. the *worst case* where all incidents cause a loss). At first glance, the two cases appear to be surprisingly similar. Notice, however, that due to the assumptions above, for most firms the rate of idiosyncratic incidents outweighs the rate of incidents from systemic events. Furthermore, the lower the security level for a given firm, the higher its contribution to the overall number of incidents, and simultaneously the lower the effect of distinguishing losses and incidents. Conversely, the higher the security level of a given firm, the less likely it is to be affected at all. Therefore, when only few cases are registered at all, these cases are likely to have occurred at firms with low security and are therefore unlikely to be filtered. The cases where most filtering occurs are large systemic events whose effect is clearly reduced (consider the range around [45, 65] on the x-axis of Fig. 2b). Of course, this translates analogously to Fig. 2a, where particularly the tail of the distribution is altered (x-axis-range around [2500, 4000] in Fig. 2a). In this case, it additionally has to be kept in mind that incidents at well-protected firms—which are mostly filtered—are assumed to typically cause below-average losses. In both figures, one observes the difference in mean between counting losses and incidents, and that the mean is shifted clearly to the right from the mode of the body of the distribution. As expected from the assumptions above, we observe a shift of the cumulative loss distribution to the right as time progresses. To corroborate the simulation results, we generate 50.000 samples of incident/loss numbers following Proposition 1 and Eq. (12) and compare them in Fig. 2d. The simulation via Eq. (12) is much faster, but cannot be directly used to generate the cumulative loss distribution, as only samples of the *total number* of incidents/losses are drawn without information as to which firms they affect (and severity differs between firms).

Furthermore, we compare the cumulative loss distribution for selected sub-portfolios in Fig. 2c, taking into account only simulation runs where a non-zero loss has been observed. As to be expected, we observe a shift of the body and tail of the loss distribution to the left as the security level increases. Understanding the cumulative loss distribution—especially in the tail—is particularly interesting in the context of reinsurance, where common contract design involves so-called *excess-of-loss* reinsurance, meaning that (portfolio) losses exceeding a pre-specified limit are ceded. For this case, an accurate understanding of the portfolio loss distribution and its tail

Table 4 Occurrence frequencies of covariate values in the toy portfolio

Covariate	Scope	Frequency
Sector b_j	FI: finance and insurance	0.30 (15)
	HC: healthcare	0.30 (15)
	BR: businesses (retail)	0.10 (5)
	EDU: education	0.10 (5)
	GOV: government and military	0.10 (5)
	MAN: manufacturing	0.10 (5)
Size s_j	1 Small	0.60 (30)
	2 Medium	0.30 (15)
	3 Large	0.10 (5)
Data d_j	1 Low risk	0.20 (10)
	2 Medium risk	0.28 (14)
	3 High risk	0.52 (26)
Number of suppliers $nsup_j$	1 Low	0.74 (37)
	2 Medium	0.20 (10)
	3 High	0.06 (3)

This dataset is copied ten times with varying IT security level ranging from 0.05 to 0.95

Table 5 Chosen parameter assumptions for frequencies (based on (F1)–(F7))

Idiosyncratic incidents		
Intercept	$(\alpha_{DB}, \alpha_{FR}, \alpha_{BI})$	$(-6, -5.3, -6)$
Data factor levels	$f_{DB,3}(x_{j3})$	(0, 0.095, 0.18)
Size factor levels	$f_{FR,2}(x_{j2}), f_{BI,2}(x_{j2})$	(0, 0.095, 0.18)
Supplier factor levels	$f_{DB,5}(x_{j5}), f_{FR,5}(x_{j5}), f_{BI,5}(x_{j5})$	(0, 0.095, 0.18)
IT security dependence	$f_{DB,4}(x_{j4}), f_{BI,4}(x_{j4})$	$1.39\ (0.5 - x_{j4})$
Time dependence	$g_{\lambda^{DB,idio}}(t), g_{\lambda^{FR,idio}}(t), g_{\lambda^{BI,idio}}(t)$	$0.128\ \lfloor t \rfloor$
Ground process of systemic events		
$\lambda^{DB,g}(t) = \exp(g_{\lambda^{DB,g}}(t))$	$\exp(-3.28 + 0.128\ \lfloor t \rfloor)$	
$\lambda^{FR,g}(t) = \exp(g_{\lambda^{FR,g}}(t))$	$\exp(-2.59 + 0.128\ \lfloor t \rfloor)$	
$\lambda^{BI,g}(t) = \exp(g_{\lambda^{BI,g}}(t))$	$\exp(-3.28 + 0.128\ \lfloor t \rfloor)$	
Distribution of S_i		
(p_G, p_{gen}, p_{sec})	(0.5, 0.1, 0.2)	
Sector distribution	$B_i \sim Unif\{1, \ldots, 6\}$, i.e. $p_b = \frac{1}{6}\ \forall b \in \{1, \ldots, B\}$	

is clearly essential. Apart from these considerations, insurers are mostly concerned with the pricing of individual policies. This is addressed next.

Table 6 Chosen parameter assumptions for severities (based on (S1)–(S7))

μ		
Intercept	$\alpha_{\mu,\cdot}$	3.91
Data factor levels	$f_{\mu,DB,3}(x_{j3})$	(0, 0.095, 0.18)
Size factor levels	$f_{\mu,FR,2}(x_{j2}), f_{\mu,BI,2}(x_{j2})$	(0, 0.095, 0.18)
IT security dependence	$f_{\mu,\cdot,4}(x_{j4})$	1.39 $(0.5 - x_{j4})$
Time dependence	$g_{\mu,\cdot}(t)$	0.1175 $\lfloor t \rfloor$
σ	$\sigma^{\cdot}$	0.076
ξ	$\alpha_{\xi,\cdot}$	0.9
β		
Intercept	$\alpha_{\beta,\cdot}$	0.5
Data factor levels	$f_{\beta,DB,3}(x_{j3})$	(0, 0.05, 0.1)
Size factor levels	$f_{\beta,FR,2}(x_{j2}), f_{\beta,BI,2}(x_{j2})$	(0, 0.05, 0.1)
IT security dependence	$f_{\beta,\cdot,4}(x_{j4})$	0.5 $(0.5 - x_{j4})$
Time dependence	$g_{\beta,\cdot}(t)$	$(0, 0.063, 0.133, 0.211, 0.3)\ \mathbb{1}_{\{\lfloor t \rfloor = i\}},\ i \in \{0, \ldots, 4\}$

5.4.2 Premium calculation

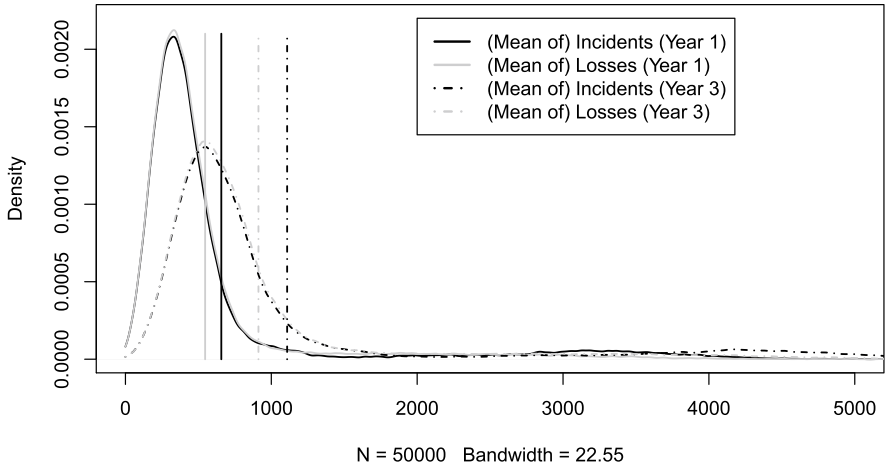
Based on the distribution of individual losses, we calculate the first-year premium based on the expected value principle given in Sect. 4.4.[21] Table 7 compares the following exemplary firms:

Firm 1: A small manufacturing business with low data and supplier risk and low IT security standards ($c = 0.15$).
Firm 2: A medium-sized company in the financial sector with medium data and supplier risk and high IT security standards ($c = 0.85$).
Firm 3: A large health care provider with high data risk, medium supplier risk, and average IT security standards ($c = 0.55$).

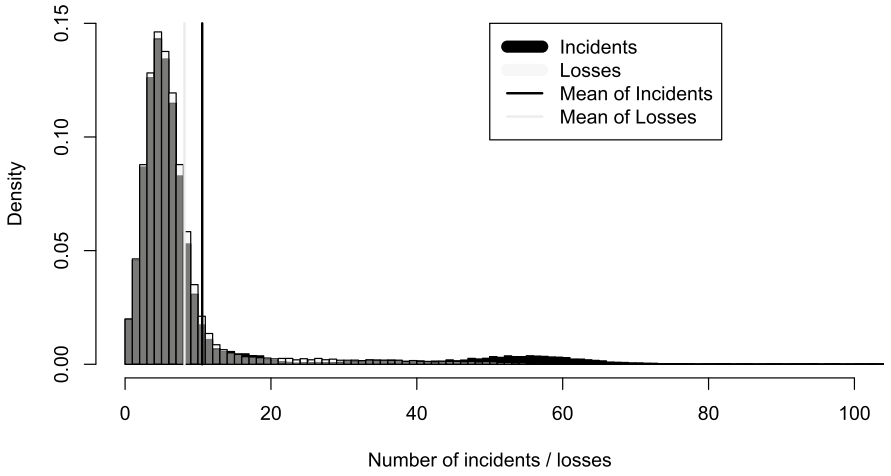
The results show that the IT security level dominates the covariate-effect on the premium, which is in line with the assumptions. As in practice, the calculation of expected losses is typically based on historically recorded (rare!) losses, only very few firms with the exact same covariate combinations might be in the portfolio and therefore, the premium is rather calculated based on all losses within a class of firms considered *homogeneous*. New firms falling into the same class are then assigned the same premium. The quite difficult task is to find an appropriate way of partitioning firms into homogeneous groups. If we partition firms according to their IT security level and calculate their premium by taking into account all firms with the same level, we obtain the results shown in Fig. 3.[22] As to be expected, the premium

[21] Note that for the chosen severity parameters, only the first moment exists ($0.5 < \xi < 1$). This prohibits the use of the exponential and standard deviation principle. We will remedy this by introducing cover limits later.

[22] *Theoretical* premiums in this figure refer to the premium that would be assigned to each firm if the expected sub-portfolio loss (the sum of the expected single losses) was allocated evenly among all firms in the sub-portfolio. This is analogous to the *simulated* approach of pricing each firm equally based on



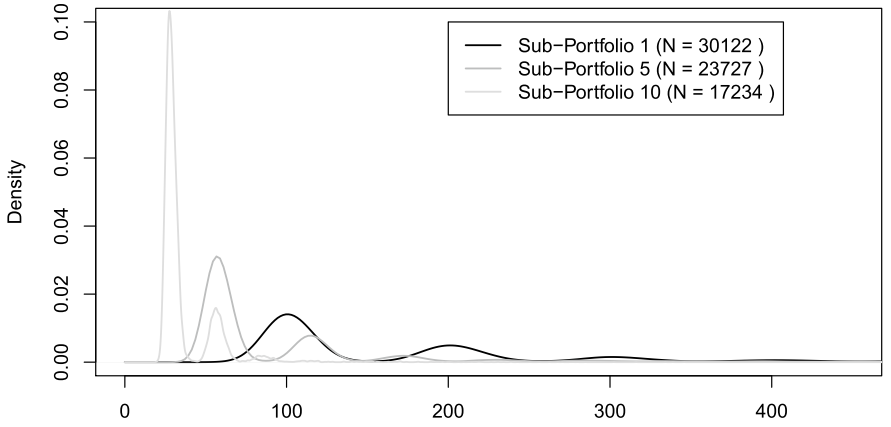
(a) Density of cumulative loss (whole portfolio).



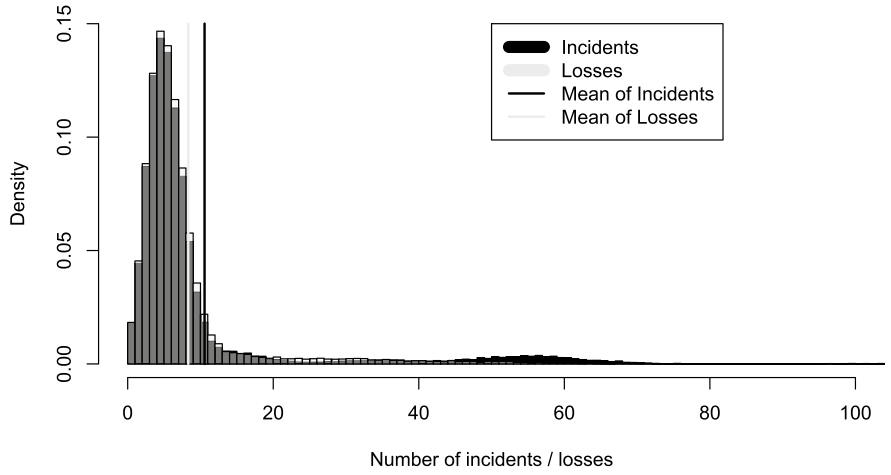
(b) Histogram of incident / loss numbers.

Fig. 2 In panels (**a**) and (**b**), for the entire portfolio ($K = 500$), the number of incidents and losses and the distribution of the cumulative portfolio loss for 50.000 runs is compared. In panel (**c**), the cumulative loss distributions for three sub-portfolios with different security levels, namely 0.05 (Portfolio 1), 0.45 (Portfolio 5), and 0.95 (Portfolio 10) are shown; here, only runs with non-zero recorded loss are taken into account, causing the sample size to vary between portfolios as to be expected. In panel (**d**), incident numbers as in Eq. (12) are simulated such that one can observe the similarity to panel (**b**)

Footnote 22 (continued)
the loss history of the—assumed homogeneous—portfolio. Combining the two "extremes" of considering only individual loss experience and only loss experience from a homogeneous group lies at the heart of *credibility theory* approaches and will not be addressed here.



(c) Density of cumulative loss (three sub-portfolios, non-zero losses only).



(d) Histogram of incident / loss numbers (based on (5), (6), and (12)).

Fig. 2 (continued)

decreases with increasing security level, while the difference between incidents and losses increases. As an alternative to (and validation for) the Monte Carlo simulation, we have furthermore implemented a *Panjer recursion scheme* using a discretized version of the severity distribution; the results are given in Online Appendix A.5 and corroborate the ones given here.

Table 7 Comparison of first-year cyber insurance premium for three selected firms, simulated numbers based on 50.000 runs

Premium based on expected value principle ($\rho = 0.2$)				
	Based on losses		Based on incidents	
	Theoretical	Simulated	Theoretical	Simulated
Firm 1	2.1665	2.0814	2.3174	2.2338
Firm 2	0.4610	0.4451	0.8107	0.7746
Firm 3	1.1777	1.1732	1.5557	1.5164

The difference between losses and incidents represents a reduction that can purely be achieved through enhanced security, as more incidents from systemic events are filtered. Note that enhanced security also decreases the frequency of idiosyncratic incidents; this is reflected in both cases

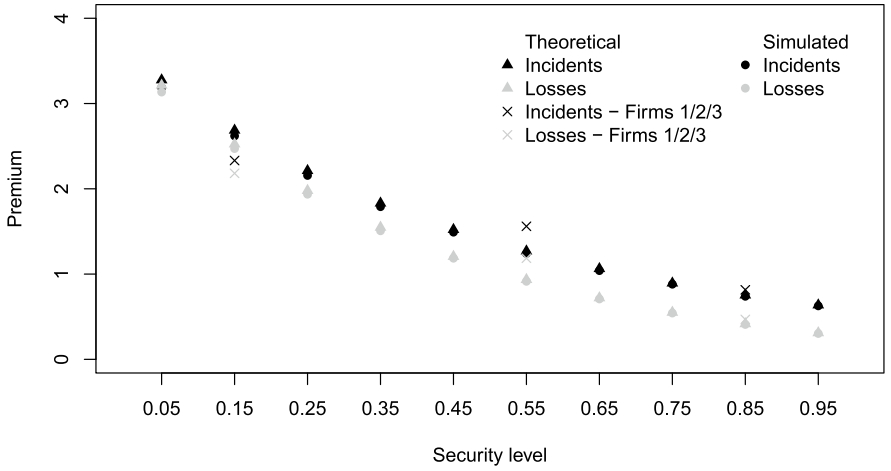


Fig. 3 We compare the premium (with loading 0.2 as above) that would be assigned to firms if they were grouped according to their IT security level. We observe that simulated values are now very close to theoretical ones, as they depend on the loss history of a sub-portfolio of 50 firms, such that Monte Carlo noise is reduced (compared to Table 7). We furthermore compare the values for the single firms from Table 7 with the portfolio they would be grouped into, and observe that e.g. firm 1, when evaluated on its own, is slightly less risky than the average firm in sub-portfolio 2

5.4.3 Risk measurement on individual and portfolio level

We compare *VaR* and *AVaR* for the three firms described above and two sub-portfolios in Table 8, as well as for all sub-portfolios in Fig. 4a and b. The *historical* estimate refers to the sample quantile from the simulation data, i.e. for a realisation of losses $\mathbf{L} = (L_1, \dots, L_n)$, let $L_{(1)} < L_{(2)} < \dots < L_{(n)}$ denote the order statistics, then for a chosen level $(1-\alpha) \in \left(\frac{i-1}{n}, \frac{i}{n}\right]$, $VaR_{1-\alpha}$ and $AVaR_{1-\alpha}$ are estimated as their empirical counterparts

$$\widehat{VaR}_{1-\alpha}(\mathbf{L}) = \hat{F}_L^{-1}(1-\alpha) = L_{(i)}, \quad \widehat{AVaR}_{1-\alpha}(\mathbf{L}) = \frac{1}{n-i+1}\sum_{j=i}^{n} L_{(j)}.$$

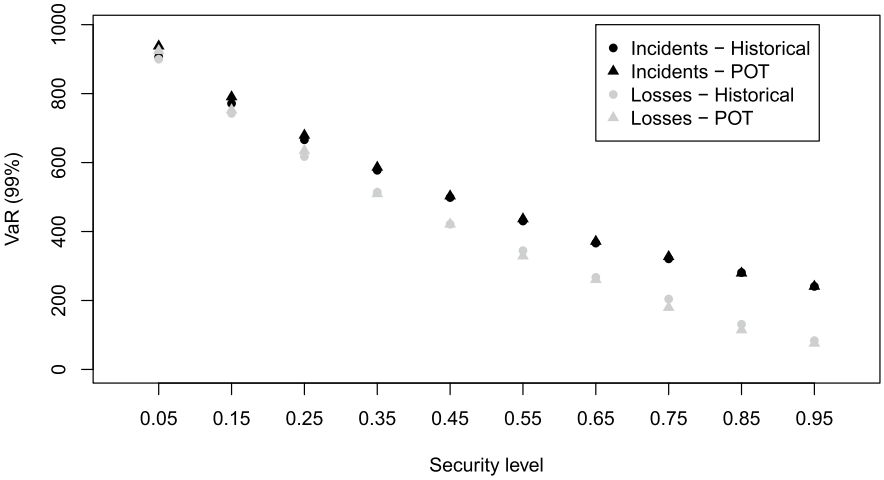
The *POT* estimate assumes that for a large threshold u, the excesses are distributed according to a generalized Pareto distribution $GPD(u, \xi, \beta)$, and thus $VaR_{1-\alpha}$ and $AVaR_{1-\alpha}$ can be estimated as (see, e.g. Ref. [57])

$$\widehat{VaR}_{1-\alpha}(\mathbf{L}) = u + \frac{\hat{\beta}}{\hat{\xi}}\left(\left(\frac{\alpha}{\frac{n'}{n}}\right)^{-\hat{\xi}} - 1\right), \quad \widehat{AVaR}_{1-\alpha}(\mathbf{L}) = \begin{cases} \frac{\widehat{VaR}_{1-\alpha}(\mathbf{L}) + \hat{\beta} - \hat{\xi}u}{1-\hat{\xi}}, & \text{if} \quad \hat{\xi} \in (0,1), \\ \infty, & \text{if} \quad \hat{\xi} \geq 1, \end{cases}$$

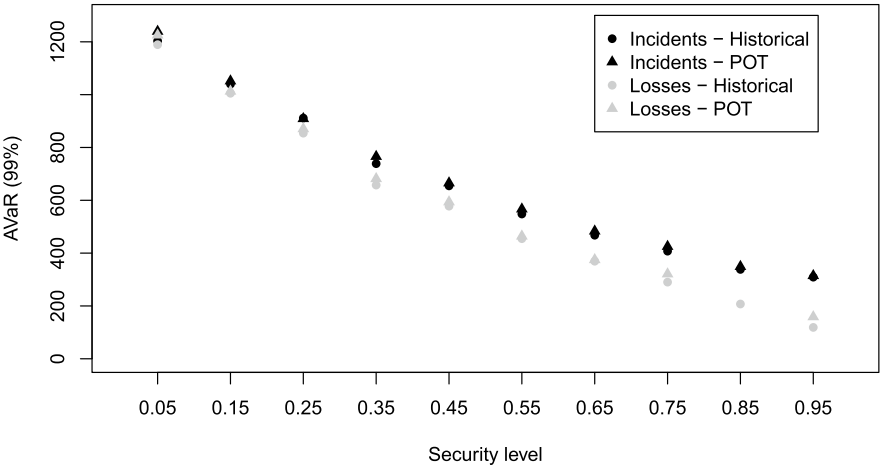
where $\hat{\beta}$ and $\hat{\xi}$ are the parameter estimates of the scale and shape of the GPD given the data $\mathbf{L}$ and n' is the number of threshold exceedances. As to be expected, both *VaR* and *AVaR* decrease with increasing security level, while the reduction when considering only losses instead of all incidents is more substantial. Note again that

Table 8 Comparison of $VaR_{0.995}$ and $AVaR_{0.995}$ for the three selected firms and two selected sub-portfolios

Risk measures	$VaR_{0.995}$				$AVaR_{0.995}$			
	Losses		Incidents		Losses		Incidents	
	Hist	POT	Hist	POT	Hist	POT	Hist	POT
Firm 1	86.46	85.86	86.73	86.27	97.18	95.73	99.40	97.57
Firm 2	34.01	33.31	35.54	35.23	36.97	37.74	39.13	39.06
Firm 3	58.28	57.68	59.01	58.81	64.61	64.23	66.96	66.22
Portfolio 1	1056.01	1041.18	1067.52	1054.67	1408.11	1379.91	1423.35	1397.02
Portfolio 6	409.87	407.52	496.96	493.88	532.67	528.27	637.25	629.33



(a) $VaR_{0.99}$



(b) $AVaR_{0.99}$

Fig. 4 Comparison of $VaR_{0.99}$ and $AVaR_{0.99}$ for all sub-portfolios

for individual firms, the numbers are based on their own loss history only and should be interpreted with care.

5.5 How relevant is accumulation risk?

We have repeatedly stressed the distinction between idiosyncratic incidents and systemic events and emphasized that the latter can lead to accumulation risk (re-)

insurers should be particularly worried about. One might now question whether the effect of including systemic events on the loss distribution warrants such a more complicated model. In order to answer this question (spoiler alert: yes!), we compare the results above with the results of a model that assumes the same marginal frequency as before for each firm, but assumes all incidents to be idiosyncratic, i.e. to occur independently from other firms. Intuitively, this should lead to the same premium for each individual contract, but decrease portfolio risk. Following Eq. (11), the overall number of incidents $\bar{N}_j^{\cdot}(T)$ at each firm $j \in \{1, \dots, K\}$ is generated using two independent Poisson r.v.

$$\bar{N}_j^{\cdot}(T) = \underbrace{N_j^{\cdot,idio}(T)}_{\sim Poi\left(\Lambda_j^{\cdot,idio}(T)\right)} + \underbrace{\bar{N}_j^{\cdot,syst}(T)}_{\sim Poi\left(\bar{p}(b_j)\Lambda_j^{\cdot,g}(T)\right)}$$

independently from all other firms. To be able to compare the two cases in each run, the number of losses $N_j^{\cdot}(T)$ at each firm $j \in \{1, \dots, K\}$ is then generated as

$$N_j^{\cdot}(T) = N_j^{\cdot,idio}(T) + \underbrace{\bar{N}_j^{\cdot,syst}(T)}_{\sim Binom\left(N_j^{\cdot,syst}(T),\bar{F}_M(c_j)\right)} .$$

With the severity distributions remaining unchanged, an analogous simulation study as above is conducted. Again, we first examine the overall distribution of the cumulative portfolio loss and number of incidents and losses in Fig. 5a and b, respectively. The difference to Fig. 2a and b is immediately evident:

- The visible heavy tails for both incident numbers and cumulative losses have vanished; thus it can be assumed they have been caused by systemic events with many firms affected simultaneously.
- In particular, the highest observed number of losses has decreased to around 17% of its previous value in both considered years, while mean losses and mean numbers of incidents/losses have stayed unaffected.
- The difference between incidents and losses is more directly visible, as in the independence case the body of the cumulative loss distribution is directly affected. This is because individual incidents are now filtered instead of the filtering impacting only systemic events, whose occurrence mostly alters the tail of the distribution.

From these findings, we conclude that incorporating systemic events into the model to capture potential accumulation risk is essential. We furthermore report $VaR_{0.99}$ and $AVaR_{0.99}$ for all sub-portfolios in Fig. 6a and b, respectively. Comparing them with Fig. 4a and b yields the same to-be-expected decreasing pattern as the security level increases, but the absolute values of the risk measures can be observed to have about halved. Perhaps it should rather be put vice versa: By including systemic events compared to complete independence, for the same expected overall

number of incidents, the risk measures $VaR_{0.99}$ and $AVaR_{0.99}$ on sub-portfolio level *double*.

As the marginal frequency and severity for each firm remain unchanged, calculated premiums should not differ from the previous simulation study; this is corroborated in Online Appendix A.5.

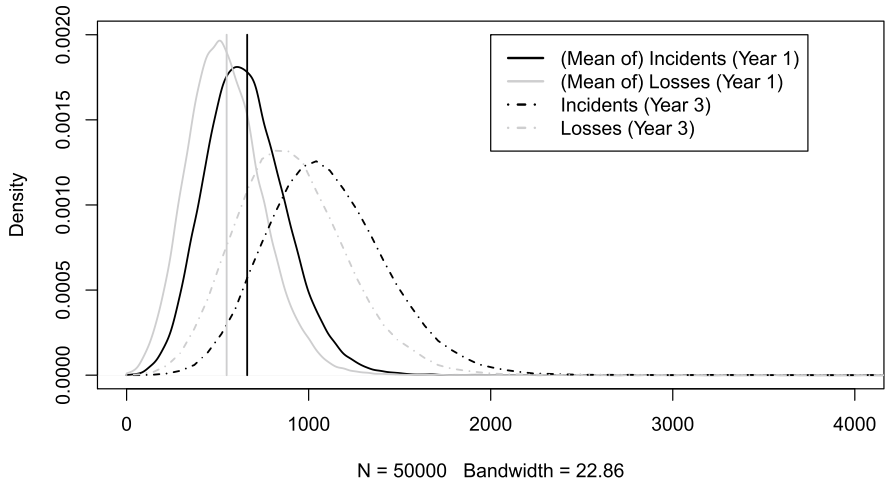
We have mentioned before that very heavy-tailed loss severities characterize cyber risk, and previous studies typically suggest such heavy tails that any moments higher than first order do not exist (and in some cases tail parameter estimates even yield infinite-mean scenarios). Even a finite-mean, infinite-variance scenario (as above, with $0.5 < \xi < 1$) is cumbersome to deal with, as e.g. only premium calculations based on the first moment can be applied. "Luckily," in the insurance context, one typically does not deal with loss severities (without upper limit) directly, but rather with claim sizes, which are typically bounded from above by the introduction of a cover limit, a maximum amount the insurer is obliged to cover for each loss. The effects of this contract design feature are examined next.

5.6 Cyber policy design: the effect of cover limits

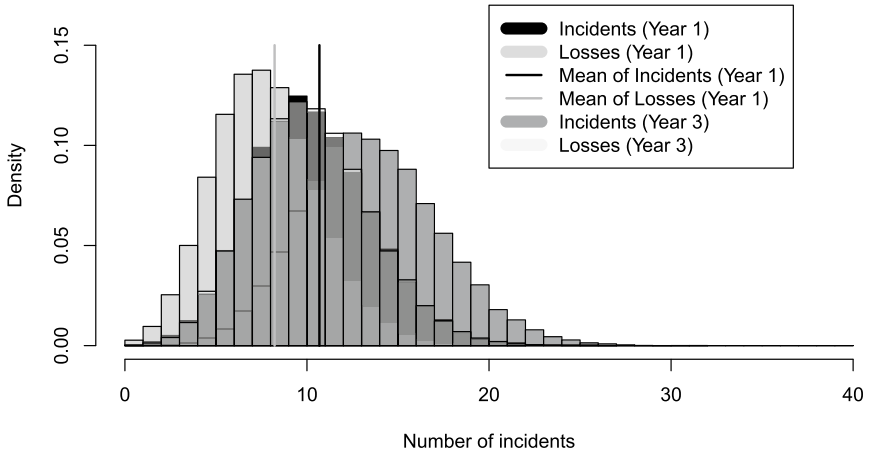
In practice, typical (primary) insurance contracts include a cover limit, as the insurer seeks to bound losses from single, extreme incidents. This, however, can lead to a supply-demand-mismatch: Insurers, still cautious of this new risk type, prefer relatively low cover limits (with a few exceptions, see the overview in Ref. [25]) that are sufficient to cover day-to-day cyber incidents, while many firms particularly seek protection for extreme scenarios such as a large data breach or long BI. [14, 58, 60] reported the non-existence of adequate cover limits as one reason for firms to refrain from purchasing cyber insurance.

Mathematically speaking, the introduction of a cover limit $\bar{M}$ corresponds to the truncation of the loss distribution, i.e. each $Y_i \in [0, \infty)$ is mapped to a claim size $\hat{Y}_i$ via $Y_i \mapsto \hat{Y}_i := \min\{Y_i, \bar{M}\} \in [0, \bar{M}]$. Note that we assume a limit on each loss; alternatives might be a limit on the total loss over the policy duration or a limit on the number of covered claims. Assuming, however, a realistically small claim frequency, this does not make a large difference, as cases of multiple losses happening at the same firm during a single policy year are extremely unlikely. Table 9 reports the probabilities of exceeding different cover limits for a large severity event and three different covariate combinations: the *baseline case* (year 1, $s = d = nsup = 1$, $c = 0.5$), the *lowest-risk case* in the portfolio (year 1, $s = d = nsup = 1$, $c = 0.95$), and the *highest-risk case* in the portfolio (year 5, $s = d = nsup = 3$, $c = 0.05$). To find the probability of an incoming claim to exceed the cover limit, we condition on observing a large claim event, i.e. in the notation of Sect. 4.3:

$$\mathbb{P}(L_{ij} > \bar{M}) = \underbrace{\mathbb{P}(L_{ij} > \bar{M} \mid L_{ij} > u_{ij})}_{\text{see Table 9}} \underbrace{\mathbb{P}(L_{ij} > u_{ij})}_{= 1-z \overset{e.g.}{=} 0.05}, \quad \bar{M} > u_{ij}.$$

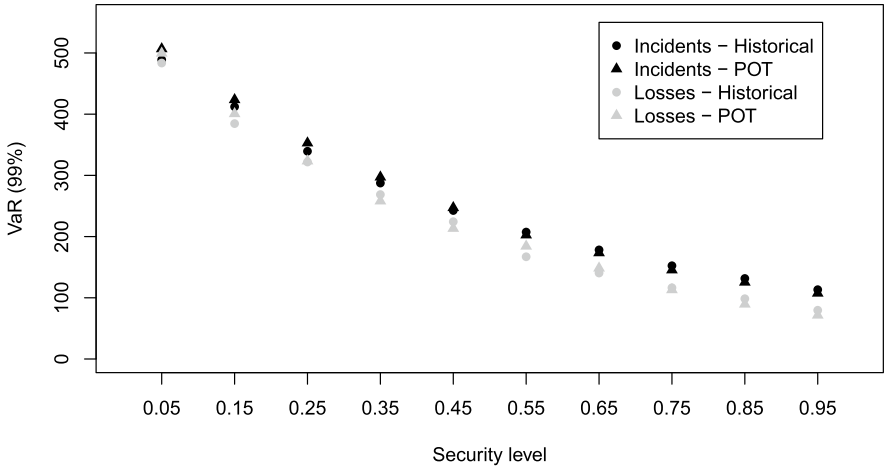


(a) Density of cumulative losses; Independence Case.

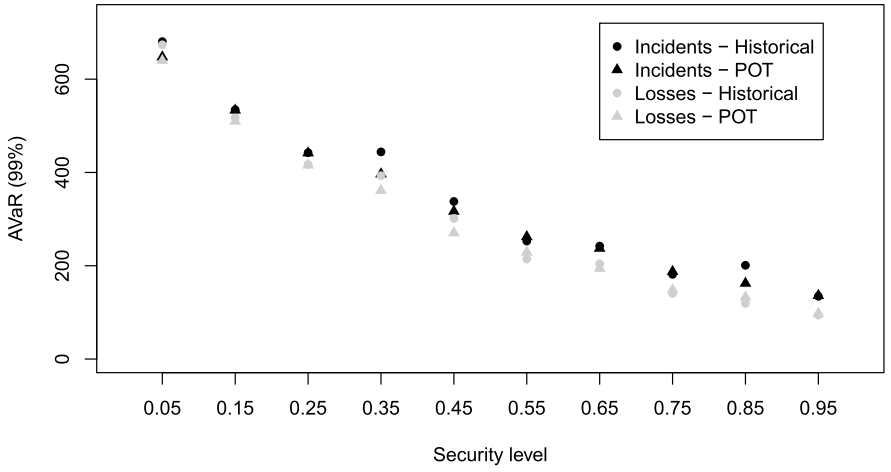


(b) Histogram of incident / loss numbers; Independence Case.

Fig. 5 For the entire portfolio ($K = 500$), the number of incidents/losses and the distribution of the cumulative portfolio loss for two different years is compared if incidents are assumed to arrive completely independently between firms



(a) $VaR_{0.99}$; Independence Case



(b) $AVaR_{0.99}$; Independence Case

Fig. 6 Comparison of $VaR_{0.99}$ and $AVaR_{0.99}$ for sub-portfolios of size $K = 50$ with varying security levels

We now assume the cover limit for all contracts to be $\bar{M}_2$ and run the same simulation as before. This could be generalized to allowing different limits depending on the insured's characteristics, e.g. a certain IT security level could be considered a prerequisite for a contract with a high limit. Similarly as above, Fig. 7 displays the (simulated) premium. While changes in the absolute numbers for the expected value principle are minor, the use of other common principles are now viable (all moments exist for the truncated losses) and deliver stable results.

Table 9 Conditional exceedance probabilities $\mathbb{P}(L_{ij} > \bar{M} \mid L_{ij} > u_{ij}) \times 10^2$ of three cover limits for large severity incidents

Cover limit	Low risk	Baseline	High risk
$\bar{M}_1 = 500$	0.0977	0.4055	5.9530
$\bar{M}_2 = 1.000$	0.0437	0.1760	2.1016
$\bar{M}_3 = 10.000$	0.0033	0.0129	0.1335

We observe that a cover limit in most cases impacts only very few (large) claims

Figures showing $VaR_{0.99}$ and $AVaR_{0.99}$ analogously to above are given in Online Appendix A.6. As to be expected, the introduction of a cover limit leads to an overall decrease in both risk measures, where the effect is higher for sub-portfolios with lower security (who tend to suffer the most severe losses and are therefore most impacted by a cover limit) and $AVaR_{0.99}$ decreases more than $VaR_{0.99}$ in absolute numbers (see Figure 9 in Online Appendix A.6).

6 Conclusion

We have presented an actuarial approach to modelling cyber risk that is consistent with the characteristics of the underlying risk factors from an economic and information-technological viewpoint. For this purpose, the existing literature on technical, statistical, economic, actuarial, and legal aspects of cyber risk was analysed in detail to identify relevant risk factors and plausible distributional assumptions within an actuarial framework. By construction, the resulting model is able to capture accumulation risk stemming from multiple firms being simultaneously affected by a cyber event; a prospect that insurers are especially worried about. Some distributional properties of the model and their relevance in the cyber context were highlighted. Moreover, we demonstrated how the model can be implemented in an insurance context using a loss distribution approach. An illustrative simulation study makes use of this implementation and derives the yearly premium for individual contracts as well as common portfolio risk measures. The model is stressed in different directions (contract design, the omission of systemic events) and the findings are analysed from the perspective of an actuary. Given the scarcity of available data on cyber losses, let us reiterate that distributional assumptions and concrete parameter choices rely on the existing literature (scattered across different disciplines) and expert judgments, hence, all quantitative findings should be interpreted with some caution in the light of model/parameter risk. Naturally, since the model presented here is not challenged on data, it is limited to its specific assumptions, e.g. using a Poisson process for arrivals; for the exemplary simulation study, these assumptions are further simplified to illustrate the actuarial exercise. However, to account for updates in the future, we consciously use a modular design that could allow to alter/replace parts of the model or to adapt it to a specific portfolio an insurance company works with.

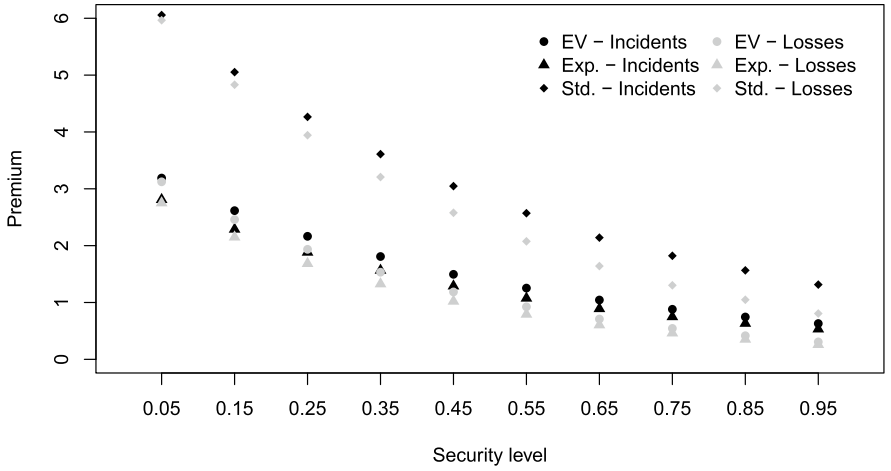


Fig. 7 We compare the premium (according to the three principles introduced in Sect. 4.4) that would be assigned to firms if they were grouped according to their IT security level and every claim in each contract had a limit of $\bar{M}_2$

Many interesting aspects, however, remain open for future research. Once sufficient cyber risk data is available, optimal estimation procedures and out-of-sample tests for the model assumptions are called for. Less theoretical, but equally important, appears the economic/legal question of categorizing cyber incidents. From the actuarial perspective, extremely interesting is the question of (optimal) cyber insurance contract design. Currently offered cyber insurance products seem to reflect the lack of an established common understanding of cyber risk and the resulting caution with which many insurers approach the topic. A better understanding of the underlying dynamics of cyber risk will in time hopefully enable product design to reflect economic optimality criteria instead of the insurers' operational limitations. Furthermore, what separates cyber from most other loss categories is the potential of designing cyber insurance products that transcend mere risk transfer, e.g. by including incident response teams or other services. To the best of our knowledge, this (non-traditional) part of cyber insurance contract design has not yet been addressed from an academic actuarial science viewpoint.

Supplementary Information The online version contains supplementary material available at https://doi.org/10.1007/s13385-021-00290-1.

Acknowledgements We have interviewed experts from different fields to gather a comprehensive understanding of cyber risk and insurance. We would especially like to thank the *Cyber-Allianz-Zentrum Bayern (CAZ) am Bayerischen Landesamt für Verfassungsschutz* (Center for Cyber Defense at the Bavarian Office for the Protection of the Constitution) and Frank Romeike for sharing their insights on cyber attacks; as well as Andreas Horn from *ERGO Insurance Group (Cyber-Insurance)* for sharing his knowledge of the current status quo of cyber insurance in Germany and the experts at *Munich Re (Corporate Underwriting Cyber)* for giving their knowledgeable feedback about the practical aspects of the model. We furthermore thank the three anonymous referees whose feedback greatly helped to improve the quality and presentation of this paper.

Funding Open Access funding enabled and organized by Projekt DEAL.

References

1. Eling M (2020) Cyber risk research in business and actuarial science. Eur Actuar J 10(2):303–333
2. Anchen J (2017) Cyber: getting to grips with a complex risk. sigma No 1/2017, Swiss Re Institute, Zurich
3. Accenture and Ponemon Institute LLC (2019) The cost of cybercrime: ninth annual cost of cybercrime study unlocking the value of improved cybersecurity protection. https://www.accenture.com/us-en/insights/security/cost-cybercrime-study
4. Allianz Global Corporate & Specialty (2015) A guide to cyber risk: managing the impact of increasing interconnectivity. https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/AGCS-Cyberrisk-report.pdf
5. Ponemon Institute LLC (2016) 2016 Cost of data breach study: global analysis. https://www.academia.edu/35179110/2016_Cost_of_Data_Breach_Study_Global_Analysis
6. Lewis J (2018) Economic impact of cybercrime – no slowing down. McAfee. https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf
7. Sandle P (2018) Ericsson sorry for software glitch that hits mobile services in Britain and Japan. Reuters, 06.12.2018
8. BBC News (2017) Global ransomware attack causes turmoil. BBC, 28.06.2017
9. The Express Tribune (2007) Shadow brokers threaten to release Windows 10 hacking tools. The Express Tribune, 31.05.2017
10. Ponemon Institute LLC (2013) Managing cyber security as a business risk: cyber insurance in the digital age. https://www.ponemon.org/research/ponemon-library/security/managing-cyber-security-as-a-business-risk-cyber-insurance-in-the-digital-age.html
11. Swiss Re and IBM Institute for business value (2016) Cyber: in search of resilience in an interconnected world, Swiss Re Ltd. https://www.swissre.com/dam/jcr:2acf5235-17e1-4a3e-ac71-fec0be9057bf/ZRH-16-09789-P1_Cyber+Publication_web.pdf
12. Allianz Global Corporate & Specialty (2019) Allianz risk barometer - top business risks for 2019. https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2019.pdf
13. ENISA, Robinson N, RAND Europe (2012) Incentives and barriers of the cyber insurance market in Europe. https://www.enisa.europa.eu/publications/incentives-and-barriers-of-the-cyber-insurance-market-in-europe
14. Advisen and PartnerRe (2018) 2018 Survey of cyber insurance market trends. https://partnerre.com/wp-content/uploads/2018/10/2018-Survey-of-Cyber-Insurance-Market-Trends.pdf
15. Romanosky S, Ablon L, Kuehn A, Jones T (2019) Content analysis of cyber insurance policies: how do carriers price cyber risk? J Cybersecur 5(1):117
16. Böhme R, Schwartz G (2010) Modeling cyber-insurance: towards a unifying framework. WEIS, https://www.econinfosec.org/archive/weis2010/papers/session5/weis2010_boehme.pdf
17. Bolot J, Lelarge M (2008) A new perspective on internet security using insurance. In: IEEE INFOCOM 2008 - the 27th conference on computer communications, pp 1948–1956. IEEE, 13.04.2008–18.04.2008

18. Hofmann A (2007) Internalizing externalities of loss prevention through insurance monopoly: an analysis of interdependent risks. Geneva Risk Insur Rev 32(1):91–111
19. Lelarge M, Bolot J (2009) Economic incentives to increase security in the internet: the case for insurance. In: IEEE INFOCOM 2009, pp 1494–1502. IEEE
20. Ogut H, Menon N, Raghunathan S (2005) Cyber insurance and it security investment: impact of interdependence risk. In: WEIS
21. Radosavac S, Kempf J, Kozat U (2008) Using insurance to increase internet security. In: Proceedings of the 3rd international workshop on economics of networked systems, pp 43–48
22. Shetty N, Schwartz G, Walrand J (2010) Can competitive insurers improve network security? In: Trust and trustworthy computing, volume 6101 of Lecture Notes in Computer Science, pp 308–322. Springer
23. Böhme R, Kataria G (2006) Models and measures for correlation in cyber-insurance. WEIS, https://www.econinfosec.org/archive/weis2006/docs/16.pdf
24. Böhme R (2005) Cyber-insurance revisited. WEIS, http://infosecon.net/workshop/pdf/15.pdf
25. Marotta A, Martinelli F, Nanni S, Orlando A, Yautsiukhin A (2017) Cyber-insurance survey. Comput Sci Rev 24:35–61
26. Zhao X, Xue L, Whinston A (2009) Managing interdependent information security risks: a study of cyberinsurance, managed security service and risk pooling. In: ICIS 2009 proceedings, p 49
27. Schwartz G, Sastry S (2014) Cyber-insurance framework for large scale interdependent networks. In: Proceedings of the 3rd international conference on high confidence networked systems, pp 145–154
28. Schwartz G, Shetty N, Walrand J (2013) Why cyber-insurance contracts fail to reflect cyber-risks. In: Başar T, Milenkovic O (eds) 51st Annual Allerton conference on communication, control, and computing (Allerton). IEEE, pp 781–787
29. Shetty N, Schwartz G, Felegyhazi M, Walrand J (2010) Competitive cyber-insurance and internet security. In: Economics of information security and privacy, vol 5, pp 229–247. Springer Science+Business Media LLC
30. Shim W (2012) An analysis of information security management strategies in the presence of interdependent security risk. Asia Pac J Inf Syst 22(1):79–101
31. Pal R (2012) Cyber-insurance for cyber-security a solution to the information asymmetry problem
32. Yang Z, Lui J (2014) Security adoption and influence of cyber-insurance markets in heterogeneous networks. Perform Eval 74:1–17
33. Pal R, Golubchik L, Psounis K, Hui P (2013) On a way to improve cyber-insurer profits when a security vendor becomes the cyber-insurer. In: Proceedings of the 12th IFIP, 2013, pp 1–9. IEEE
34. Pal R, Golubchik L, Psounis K, Hui P (2014) Will cyber-insurance improve network security? A market analysis. In: Proceedings/IEEE INFOCOM, 2014, pp 235–243. IEEE
35. Agrafiotis I, Nurse J, Goldsmith M, Creese S, Upton D (2018) A taxonomy of cyber-harms: defining the impacts of cyber-attacks and understanding how they propagate. J Cybersecur 4(1):tyy006
36. Böhme R, Laube S, Riek M (2018) A fundamental approach to cyber risk analysis. Variance 11(2):161–185
37. Bouveret A (2018) Cyber risk for the financial sector: a framework for quantitative assessment, volume WP/18, 143 of IMF working paper. International Monetary Fund, Washington, DC, June
38. Cebula J, Young L (2010) A taxonomy of operational cyber security risks. Software Engineering Institute, Carnegie Mellon University. https://apps.dtic.mil/dtic/tr/fulltext/u2/a537111.pdf
39. Cohen R, Humphries J, Veau S, Francis R (2019) An investigation of cyber loss data and its links to operational risk. J Oper Risk 14(3):1–25
40. Herath H, Herath T (2011) Copula-based actuarial model for pricing cyber-insurance policies. Insur Mark Co 2(1):7–20
41. Mukhopadhyay A, Chatterjee S, Saha D, Mahanti A, Sadhukhan S (2013) Cyber-risk decision models: to insure it or not? Decis Support Syst 56:11–26
42. Peng C, Xu M, Xu S, Hu T (2018) Modeling multivariate cybersecurity risks. J Appl Stat 45(15):2718–2740
43. Peng C, Xu M, Xu S, Hu T (2017) Modeling and predicting extreme cyber attack rates via marked point processes. J Appl Stat 44(14):2534–2563
44. Xu M, Schweitzer K, Bateman R, Xu S (2018) Modeling and predicting cyber hacking breaches. IEEE Trans Inf Forensics Secur 13(11):2856–2871
45. Baldwin A, Gheyas I, Ioannidis C, Pym D, Williams J (2017) Contagion in cyber security attacks. J Oper Res Soc 68(7):780–791

46. Fahrenwaldt M, Weber S, Weske K (2018) Pricing of cyber insurance contracts in a network model. ASTIN Bull 48(3):1175–1218
47. Xu M, Hua L (2019) Cybersecurity insurance: modeling and pricing. N Am Actuar J 23(2):220–249
48. Xu M, Da G, Xu S (2015) Cyber epidemic models with dependences. Internet Math 11(1):62–92
49. Edwards B, Hofmeyr S, Forrest S (2016) Hype and heavy tails: a closer look at data breaches. J Cybersecur 2(1):3–14
50. Eling M, Loperfido N (2017) Data breaches: goodness of fit, pricing, and risk measurement. Insur Math Econ 75:126–136
51. Eling M, Jung K (2018) Copula approaches for modeling cross-sectional dependence of data breach losses. Insur Math Econ 82:167–180
52. Farkas S, Lopez O, Thomas M (2019) Cyber claim analysis through Generalized Pareto Regression Trees with applications to insurance pricing and reserving. https://hal.archives-ouvertes.fr/hal-02118080
53. Maillart T, Sornette D (2010) Heavy-tailed distribution of cyber-risks. Eur Phys J B 75(3):357–364
54. Wheatley S, Maillart T, Sornette D (2016) The extreme risk of personal data breaches and the erosion of privacy. Eur Phys J B 89(1):59
55. Romanosky S (2016) Examining the costs and causes of cyber incidents. J Cybersecur 2(2):121–135
56. Eling M, Wirfs JH (2019) What are the actual costs of cyber risk events? Eur J Oper Res 272(3):1109–1119
57. Chavez-Demoulin V, Embrechts P, Hofert M (2016) An extreme value approach for modeling operational risk losses depending on covariates. J Risk Insur 83(3):735–776
58. Advisen and PartnerRe (2017) 2017 Survey of cyber insurance market trends. https://partnerre.com/wp-content/uploads/2017/10/PartnerRe-2017-Survey-of-Cyber-Insurance-Market-Trends.pdf
59. Munich Re (2020) Cyber insurance: risks and trends 2020
60. Advisen (2015) 2015 Network security & cyber risk management: the fourth annual survey of enterprise-wide cyber risk management practices in Europe. https://www.advisenltd.com/wp-content/uploads/network-security-cyber-risk-management-white-paper-2015-02-06.pdf
61. Allianz Global Corporate & Specialty (2015) Allianz risk barometer top business risks 2015: risk and reputation in the age of disruption. https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2015.pdf
62. Biener C, Eling M, Wirfs JH (2015) Insurability of cyber risk: an empirical analysis. Geneva Pap Risk Insur Issues Pract 40(1):131–158
63. Eling M, Wirfs JH (2016) Cyber risk: too big to insure? Risk transfer options for a mercurial risk class, volume Band 59 of IVW-HSG-Schriftenreihe. Institute of Insurance Economics I.VW-HSG University of St. Gallen, St. Gallen
64. Gesamtverband der Deutschen Versicherungswirtschaft e.V. (2019) Unverbindlicher Muster-Fragebogen zur Risikoerfassung im Rahmen von Cyber-Versicherungen für kleine und mittelständische Unternehmen. (Unverbindliche Bekanntgabe des Gesamtverbandes der Deutschen Versicherungswirtschaft e.V. (GDV) zur fakultativen Verwendung. Abweichende Vereinbarungen sind möglich.)
65. Allianz Global Corporate & Specialty (2020) Cyber insurance
66. Eling M, Schnell W, Sommerrock F (2016) Ten key questions on cyber risk and cyber risk insurance. The Geneva Association. https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public//cyber-risk-10_key_questions.pdf
67. Andress J (2014) The basics of information security: understanding the fundamentals of infosec in theory and practice. Syngress, Elsevier Science
68. Carfora M, Martinelli F, Mercaldo F, Orlando A (2019) Cyber risk management: an actuarial point of view. J Oper Risk 14(4):77–103
69. CRO Forum (2016) CRO forum concept paper on a proposed categorisation methodology for cyber risk
70. Deutsche Aktuarvereinigung e.V. Ergebnisbericht des Ausschusses Schadenversicherung: Daten und Methoden zur Bewertung von Cyberrisiken
71. Bandyopadhyay T, Mookerjee V, Rao R (2009) Why IT managers don't go for cyber-insurance products. Commun ACM 52(11):68
72. Jacobs J (2014) Analyzing Ponemon cost of data breach. https://datadrivensecurity.info/blog/posts/2014/Dec/ponemon/
73. Boudreaux D, Rao S, Ferguson W (2013) Measuring losses for small business interruption claims. J Appl Risk Manag Insur 1(1):53–75

74. Deleris L, Elkins D, Pate-Cornell E (2004) Analyzing losses from hazard exposure: a conservative probabilistic estimate using supply chain risk simulation. In: 2004 Winter simulation conference, pp 323–330. IEEE
75. Hashemi SJ, Ahmed S, Khan F (2015) Probabilistic modeling of business interruption and reputational losses for process facilities. Process Saf Prog 34(4):373–382
76. Jain VK, Guin J (2009) Modeling business interruption losses for insurance portfolios. https://www.researchgate.net/publication/290333216
77. Zajdenweber D (1996) Extreme values in business interruption insurance. J Risk Insur 63(1):95
78. Bank for International Settlements BIS (2005) Basel committee on banking supervision. International convergence of capital measurement and capital standards: a revised framework: updated November 2005, volume 118 of Basel Committee Publications. BIS, Basel
79. Daley DJ, Vere-Jones D (2003) An introduction to the theory of point processes: volume I: elementary theory and methods, 2nd edn. Springer, New York
80. Daley DJ, Vere-Jones D (2007) An introduction to the theory of point processes: volume II: general theory and structure. Probability and its applications, 2nd edn. Springer, New York
81. Wood S (2017) Generalized additive models: an introduction with R. Chapman & Hall/CRC texts in statistical science. CRC Press/Taylor & Francis Group, Boca Raton
82. MacKay D (2010) Information theory, inference, and learning algorithms, 1st edn. Cambridge University Press, Cambridge (**9th printing edition, imp. 2010**)
83. Kingman JFC (1993) Poisson processes, vol 3. Oxford studies in probability. Clarendon Press, Oxford
84. Blitzstein J, Hwang J (2015) Introduction to probability. Texts in statistical science, 2nd edn. CRC Press and Taylor & Francis group, Boca Raton
85. Wald A (1944) On cumulative sums of random variables. Ann Math Stat 15(3):283–296
86. Mikosch T (2009) Non-life insurance mathematics: an introduction with the Poisson process. Springer-Verlag, Berlin (**Universitext**)