Health and Technology (2025) 15:635–650
https://doi.org/10.1007/s12553-025-00964-w

ORIGINAL PAPER

Economic impact of healthcare cyber risks

M. Fátima Brilhante[1,2] · Sandra Mendonça[2,3] · Pedro Pestana[4,5] · M. Luísa Rocha[2,6,7] · Rui Santos[2,8]

Received: 6 December 2024 / Accepted: 28 March 2025 / Published online: 8 April 2025

Abstract

Purpose The healthcare sector is a primary target for cybercriminals, with health data breaches ranking among the most critical threats. Despite stringent penalties imposed by the U.S. Department of Health and Human Services Office for Civil Rights (OCR), vulnerabilities still persist due to slow detection and ineffective data protection measures. On the other hand, as organizations are often reluctant to disclose security breaches for fear of reputational and market share losses, penalties can serve as a useful proxy for quantifying losses and insurance claims.

Methods This study analyzes fines and settlements (2008–2024) using the traditional lognormal, general extreme value (GEV) and other heavy-tailed statistical models, including the geo-max-stable loglogistic law, and also the mixture models hyperexponential and hyperloglogistic.

Results Mixture models, either the hyperexponential or the hyperloglogistic, deliver the best fit for OCR penalties, and for yearly maxima, the best fit is achieved with the GEV distribution. Regarding Attorneys General fines, the hyperexponential model is optimal, with the GEV model excelling again for their yearly maxima. Hence, mixture models effectively capture the dual nature of penalty data, comprising clusters of moderate and extreme values. However, yearly maxima align better with the GEV model.

Conclusions The findings suggest that while Panjer's theory for aggregate claims suffices for moderate claims, it must be supplemented with strategies to address extreme cybercrime scenarios, ensuring insurers and reinsurers can manage severe losses effectively.

Keywords Vulnerabilities · Healthcare breaches · Cyber risk · Insurance · Extreme value theory

1 Introduction

Vulnerabilities are weaknesses that can be exploited by cybercriminals to access a computer system, with the intention of running malicious code, stealing sensitive data, or installing malware (Tunggal [1]), thus creating risks of possible intrusion and exploitation with potentially serious economic losses. By the end of the twentieth century, vulnerabilities were a major threat and concern. On this topic, see, for example, Howard's [2] dissertation on analyzing security incidents in the Internet.

On the other hand, cyber risks, which include identity theft and theft of customer records, data destruction and recovery and litigation costs, intellectual property theft, business interruption and after effects of reputational damages, can have a major economic impact (see Lian et al. [3], Dejung [4], and Eling et al. [5]). However, the costs associated with cyber risks, which, aside from cybercrime, must encompass insurance costs and provision for eventual regulatory fines and penalties, are scarce and vary considerably across studies. Nonetheless, the costs associated with cybercrime activity in 2023 are estimated to be USD 8 trillion and the damage costs are estimated to grow to USD 10.5 trillion annually by 2025. In this regard, Nikolakopoulos et al. [6] carried out a systematic review of studies on the economic impact of cybersecurity incidents on critical information infrastructures, and Lagazio et al. [7] examined the impact of cybercrime on the financial sector.

In 2005, the Common Vulnerabilities Scoring System (CVSS) became available to the public to assess the severity of vulnerabilities and the risk they pose. In November 2023, CVSS v4.0 [8] was released, with one of its objectives being to respond to one of the biggest criticisms made against its previous version 3.1, namely that health, human safety, and

Extended author information available on the last page of the article

industrial control systems were not well represented. The focus of CVSS v4.0 is now on Operational Technology, more precisely, on Safety Metrics and Values. On this topic, Dugal and Rich [9] state that, and we quote,

> "Many vulnerabilities today have impacts outside of the traditional C/I/A [confidentiality, integrity and availability] triad of logical impacts. Increasingly more common is a concern that, while logical impacts may or may not be recognized on a vulnerable or impacted system, it is possible for tangible harm to occur to humans as a result of a vulnerability exploit. IoT [Internet of Things], ICS [Internet Calendaring and Scheduling] and healthcare sectors in particular care greatly about being able to identify this kind of impact as part of the CVSS specification to help drive prioritization of issues aligned with their growing concerns."

For further information on measuring the risk of vulnerabilities, see Brilhante et al. [10]. Moreover, in Brilhante et al. [11], a refinement of the CVSS v3.1 calculator for the Base metrics is presented, allowing probabilities to be assigned to its nominal variables by the user, according to their level of information, to compute the base score of a vulnerability, and therefore its severity.

When it comes to cybersecurity insurance, many insurance companies offer their clients products, but the pricing of cybersecurity risks still remains a challenging problem (cf. Fahrenwaldt et al. [12], and Xu and Hua [13]), despite the fact that the general principle is that premiums should be calculated as a function of the expected value of severity claims. Xu and Hua [13] discuss, in this context, several scenarios using Weibull and lognormal models in their simulations. In addition, as the lognormal mimics the linear signature of power laws, it has often been used in vulnerabilities lifecycle studies as well (see Brilhante et al. [10]).

Unlike traditional insurance policies, cybersecurity insurance has no standard scoring systems or actuarial tables for the pricing of insurance products, since data on security breaches and losses exist only in small quantities, mainly because organizations are generally reluctant to reveal details of security breaches due to their fear of losing market share and reputation. Making matters worse, insurers tend to increase premiums for larger companies. In fact, cyber risks are very different from the traditional risks covered by indemnity insurance because information and communication technology resources are interconnected in a network, and therefore the risk analysis and its related potential losses must consider the network topology (see Egan et al. [14]). Premiums, on the other hand, are determined based on the estimated losses and the evaluation of the aggregate claims during a specific period, which is fundamental for any insurance company that wants to offer cybersecurity insurance. Hence, the need to understand the evolution and spread of an epidemic over a network is essential.

However, coverage may be limited and also very expensive for companies without a good cybersecurity protection. Furthermore, unlike other risks typically covered by insurers, the losses are generally difficult to verify by the insurance company (see Öğüt et al. [15]). Nevertheless, the global cyber insurance market tripled in volume in the last five years, expanding to gross direct premiums of around USD 13 billion in 2022. For example, the Swiss Re Institute [16] expects premiums to grow to USD 23 billion by 2025, although the market remains small relatively to the fast-evolving cyber risks.

In this paper, Section 2 deals with healthcare data breaches. Penalties and settlements, imposed by the U.S. Department of Health and Human Services Office for Civil Rights (OCR) to careless entities partly responsible for breaching protected health information, are naturally correlated to cyber risks and so they provide some useful information for insurance pricing principles.

Section 3 contains a brief overview of the Extreme Value Theory (EVT) models in the Independent and Identically Distributed (IID) framework (Fréchet, Gumbel and Weibull), and in the Rachev and Resnick [17] geometrically thinned framework (loglogistic, logistic and backward loglogistic).

In Section 4, the rationale behind the use of power laws, Pareto-like heavy-tailed and general extreme and geo-extreme models for the yearly maxima penalties and fines shown in Tables 2 and 4 of Section 2 is discussed. Using the data in Tables 1, 2, 3 and 4, the goodness-of-fit with some mixture models, more precisely, with the hyperexponential and hyperloglogistic, is also investigated. This will serve as a guideline for the analysis of outstanding and of yearly maxima of penalties and fines values, which is discussed in Section 5.

In Section 6, it is reinforced that insurance companies must consider strategies that merge Panjer's theory for aggregate claims with the consideration of outstanding extreme claims.

2 Healthcare data breaches

Healthcare data are the most valuable type of data on the black market, since it takes longer for healthcare fraud to be discovered and stolen data can generally be used much longer. The analysis of data breaches recorded on the Privacy Rights database between 2015 and 2022 shows that one third of all recorded data breaches were in the healthcare sector, and that it was much higher in this sector than in any other sector.

Due to the increasing digitalization of healthcare data and the increasing sophistication of cyberattacks (see recent

Table 1 OCR penalties imposed to resolve the HIPAA right of access violations (2008-2024)

100	2250	35	1000	866	1000	4300	50	100	1500
1500	1700	150	275	400	1216	1700	150	215	250
800	1725	4800	125	218	750	750	850	3500	25
400	650	650	750	1550	2141	2200	2700	2750	3900
5550	240	31	387	400	475	2200	2300	2400	2500
5500	3200	100	100	384	515	3500	16000	4348	10
65	85	85	100	2175	3000	3000	1600	2154	100
25	1040	10	4	70	15	38	1500	2300	6850
160	100	1000	202	25	15	65	36	200	5100
75	70	65	30	25	5	80	10	160	100
30	32	63	50	28	30	875	4	5	20
23	30	50	55	55	65	240	100	301	25
30	80	23	20	17	1250	15	350	30	240
75	80	1300	100	80	480	160	4750	40	

Table 2 Yearly maximum of OCR penalties for HIPAA violations (2008–2024)

100	2250	1000	4300	1700	1700	4800	3500	5550	5500
16000	3000	6850	5100	875	1300	4750			

Table 3 Attorneys General HIPAA fines (2010-2024)

250	100	55	750	2500	140	100	40	150	90
15	130	264	1100	100	2000	1150	575	418	200
230	175	365	100	200	100	75	935	900	10000
8700	39500	5000	21000	495	425	425	600	425	200
400	200	2500	550	450	49000	250	60	49500	350
1400	450	120	400	300	1650				

Table 4 Yearly maximum of Attorneys General HIPAA fines (2010-2024)

250	100	2500	140	150	90	—	2000
1150	10000	39500	21000	600	49500	1650	

Fig. 1 HIPAA violation penalty tiers (source: The HIPAA Journal [22])

statistics in Griffiths [18, 19]), the number of healthcare data breaches is growing. However, increased awareness of compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) should have an impact on reducing the number of HIPAA breaches attributable to lost or stolen drives and devices, as a consequence of fewer covered organizations carrying unencrypted protected health information on drives and devices, and relying more on cloud computing, although the latter has also been a target for hackers (see Griffiths [20]). The OCR Breach Portal [21], listing all breaches of unsecured protected health information affecting 500 or more individuals reported within the previous 24 months, and that are still currently under screening, indicates that, on September 26, 2024, there were 891 breaches being investigated. For detailed information on data breach statistics, consult the HIPPA Journal [22]. Moreover, Neto et al. [23] discuss the challenges encountered for developing a global data breach database.

On the other hand, Government backstops and other market-intervening tools must mitigate catastrophic losses. For example, the two most extreme cases known are in the healthcare sector (including hospitals) and the cross-sector attack, with estimated losses of USD 28 and 35 billion, respectively, thus ranking at the top 10 of the biggest losses in the history of events. Nevertheless, organizations in the healthcare sector have stricter breach notification requirements than other sectors. For instance, ransomware attacks, that can have drastic consequences, have to be reported, even if it cannot be established that data has been compromised. This was the case with the 2017 WannaCry ransomware that crippled healthcare institutions and many other organizations around the world, and which led to economic losses estimated at USD 8 billion. For more information on this topic, consult Trautman and Ormerod [24]. Furthermore, OCR imposes heavy fines when violations have been allowed to persist for several years, or when there is a systemic non-compliance with the HIPAA rules. The penalty structure for violations of HIPAA regulations is described in Figs. 1 and 2.

As organizations are reluctant to disclose any information on security breaches because of their fear of losing market share and reputation, the access to data on security breaches and losses in the healthcare sector is therefore limited. For this reason, data on OCR penalties and on the Attorneys General HIPAA fines are used as a proxy, since these are highly and positively correlated with the severity of the losses.

Table 1 lists the OCR penalties (in thousands USD) imposed to resolve the HIPAA Right of Access violations from 2008 to January 2024 (source: The HIPAA Journal [22]). In Table 2, the yearly maxima penalties (in thousands USD), extracted from Table 1, are listed.

The Attorneys General HIPAA fines (in thousands USD) for 2010-2024 are listed in Table 3 (notice that no fine has

Fig. 2 HIPAA violation penalty tiers (source: The HIPAA Journal [22])

Annual Penalty Limit	Annual Penalty Limit	Minimum Penalty per Violation	Maximum Penalty per Violation	Annual Penalty Cap
Tier 1	Lack of Knowledge	$137	$34,464	$34,464
Tier 2	Reasonable Cause	$1,379	$68,928	$137,886
Tier 3	Willful Neglect	$13,785	$68,928	$344,638
Tier 4	Willful neglect (not corrected within 30 days	$68,928	$68,928	$2,067,813

been imposed in 2016), and the yearly maxima are shown in Table 4 (source: The HIPAA Journal [22]).

3 A brief overview of the theory

Distributions for variables modeling phenomena linked to vulnerabilities exploitation have in general heavy right tails, and therefore there is a tendency to believe that power laws are adequate models. Good references on this subject are Clauset et al. [25] and Stumpf and Porter [26]. For a detailed discussion on the use of heavy-tailed models for vulnerabilities data, more specifically, on vulnerabilities lifecycle variables, see Brilhante et al. [10], and for the use of mixture models, namely about the hyperexponential, consult Feldmann and Whitt [27]. The lognormal law has also been used in this context as a model because it mimics the linear signature of power laws (see Mitzenmacher [28]). Moreover, the Generalized Pareto (GP) model and, in general, slowly varying tailed models have been studied as well. For a comprehensive view on the topic, see Brilhante et al. [10].

In statistical analysis, asymptotic results can be useful to support model choices. For example, the extremal limit theorem and EVT give the necessary tools when heavy-tailed models are reasonable candidates to fit a data set. Therefore, Section 3.1 gives a brief account of EVT in the traditional IID framework, but also in the geometrically thinned scheme, since healthcare data breaches may be underreported due to reputational concerns. On this subject, it is worth mentioning that, contrasting with the fast rate of convergence in the central limit theorem when dealing with central order statistics, the rate of convergence in the extremal limit theorem for extreme order statistics can be very slow, which is a well-known fact from Fisher and Tippett's [29] remark on the penultimate behavior of normalized maxima. This suggests that it is legitimate to find alternative fits to the traditionally used heavy-tailed models. The results outlined in Section 3.1 are simply intended to indicate that the GEV, more specifically the Fréchet, and loglogistic models, can provide useful fits to the data. Readers less familiar with these concepts can skip the more technical details in Section 3.1, taking only into consideration the features of the models, since they are used in Section 5.

3.1 Extreme value theory

The bulk of central order statistics and the central limit theorem play a key role in the majority of the decisions that are based on data analysis. On the other hand, extreme order statistics and the extremal limit theorem are crucial in the analysis of outstanding risks, namely in the analysis of large claims in insurance (see Gomes and Pestana [30], Embrechts et al. [31], and Beirlant et al. [32]).

Fréchet [33] transposed Lévy's [34] stability theory for sums to maxima, obtaining the Fréchet distribution, with the standardized form

$$\Phi_\alpha(x) = \exp\left(-x^{-\alpha}\right)\, \mathbb{I}_{[0,\infty)}(x),\ \alpha > 0.$$

Soon after, Fisher and Tippett [29] established the initial form of the extremal limit theorem obtaining the (later called) Gumbel and max-Weibull types, respectively,

$$\Lambda(x) = \exp\left(-\mathrm{e}^{-x}\right)\, \mathbb{I}_{\mathbb{R}}(x),$$

and

$$\Psi_\alpha(x) = \begin{cases} \exp\left[-(-x)^{\alpha}\right], & x < 0 \\ 1 & , \ x \geq 0 \end{cases}, \ \alpha > 0.$$

Gnedenko [35] demonstrated that the Fréchet, Gumbel and max-Weibull distributions are the only possible limit types for normalized maxima $M_n = \max\{X_1, \ldots, X_n\}$ of a IID sequence of random variables $(X_n)_{n\in\mathbb{N}}$, with a cumulative distribution function F, i.e., they are the only solutions of the stability equation $F^n(A_n x + B_n) = F(x)$, for appropriate attraction coefficients $A_n > 0$ and $B_n \in \mathbb{R}$, thus fully characterizing the domains of attraction of the Fréchet and of the max-Weibull types. As for the characterization of the domain of attraction of the Gumbel type, this was done by de Haan [36]. Therefore, Gnedenko and de Haan's definitive form of the extremal limit theorem provides the adequate framework for the asymptotic choice of extremal models for M_n when $n \to \infty$.

On the other hand, von Mises [37] and Jenkinson [38] unified into a single expression the standardized stable limit distribution of normalized maxima, called the general extreme value (GEV) distribution, with cumulative distribution function

$$G_\xi(x) = \exp\left[-(1+\xi x)^{-1/\xi}\right]\, \mathbb{I}_{\{x:1+\xi x>0\}}(x),\ \xi \in \mathbb{R}. \quad (1)$$

If, in Eq. 1, the shape parameter $\xi > 0$, the Fréchet-α type, with $\alpha = 1/\xi$, is obtained, and if $\xi < 0$, the max-Weibull-α type, with $\alpha = -1/\xi$, is obtained. When $\xi \to 0$, G_ξ defined in Eq. 1 converges to the standard Gumbel distribution, i.e., $G_0(x) = \exp\left(-\mathrm{e}^{-x}\right)$ for any real x. More details on EVT can be found in Gomes and Guillou [39], among other review papers.

A relevant issue in what regards healthcare vulnerability and extreme losses due to malicious breaches is the possibility that some data will not be reported. Rachev and Resnick

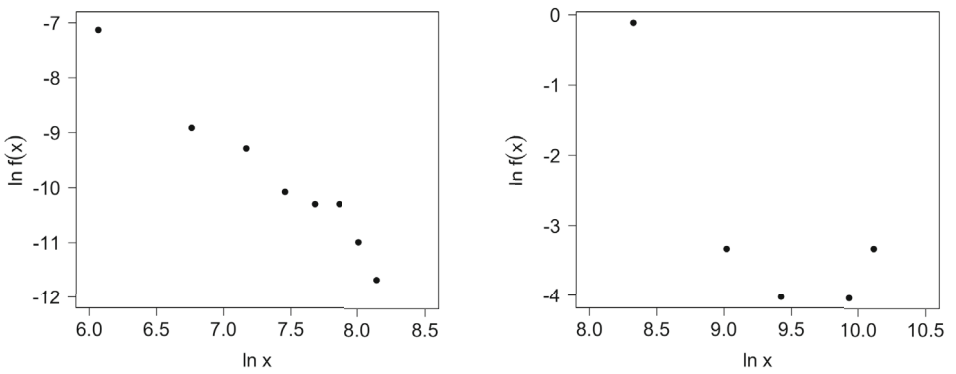


Fig. 3 Power law linear signature in a log-log plot

(a) OCR penalties data (b) Attorneys General HIPAA fines data

[17] developed a straightforward theory under the plausible assumption of geometric thinning of the full sequence of IID random variables $(X_n)_{n\in\mathbb{N}}$, i.e., that each original term of the sequence is reported with probability θ or discarded with probability $1-\theta$, independently of any other.

In case the IID sequence $(X_n)_{n\in\mathbb{N}}$ is Geometrically(θ), $0<\theta<1$, thinned, the geo-max-stable possible distributions ${}^{g}G_{\xi}$ satisfy the relationship ${}^{g}G_{\xi}(x) = \frac{1}{1-\ln G_{\xi}(x)}$ (Rachev and Resnick [17]), and therefore the general (standardized)

Table 5 ML parameter estimates and goodness-of-fit results for the OCR penalties data in Table 1

	AD	CvM	AIC[a]	BIC[a]
Lognormal				
$\widehat{\mu} = 5.426\ (0.165)$[b]	0.525	0.162	2091.07	2096.94
$\widehat{\sigma} = 1.941\ (0.116)$[b]	$(A_n^2 = 2.355)$	$(\omega_n^2 = 0.656)$		
GEV				
$\widehat{\xi} = 1.690\ (0.152)$	0.142	0.112	2102.25	2111.06
$\widehat{\lambda} = 90.958\ (15.030)$	$(A_n^2 = 3.703)$	$(\omega_n^2 = 0.723)$		
$\widehat{\delta} = 157.374\ (29.137)$				
GP				
$\widehat{\xi} = 1.475\ (0.232)$	0.001	0.107	2098.62	2107.42
$\widehat{\lambda} = 4$	$(A_n^2 = \infty)$	$(\omega_n^2 = 0.729)$		
$\widehat{\delta} = 162.125\ (34.451)$				
Loglogistic				
$\widehat{\alpha} = 0.806\ (0.056)$	0.001	0.919	2095.18	2103.98
$\widehat{\lambda} = 4$	$(A_n^2 = \infty)$	$(\omega_n^2 = 0.250)$		
$\widehat{\delta} = 211.606\ (39.526)$				
Hyperexponential				
$\widehat{\mathfrak{p}} = 0.507\ (0.053)$	0.235	0.453	2073.45	<u>2082.25</u>
$\widehat{\theta}_1 = 0.0130\ (0.0024)$	$(A_n^2 = 3.211)$	$(\omega_n^2 = 0.458)$		
$\widehat{\theta}_2 = 0.0005\ (0.0001)$				
Hyperloglogistic				
$\widehat{\mathfrak{p}} = 0.632\ (0.073)$	0.147	0.574	<u>2072.78</u>	2087.45
$\widehat{\alpha}_1 = 1.399\ (0.212)$	$(A_n^2 = 3.668)$	$(\omega_n^2 = 0.405)$		
$\widehat{\delta}_1 = 66.753\ \ (16.270)$				
$\widehat{\alpha}_2 = 2.149\ (0.613)$				
$\widehat{\delta}_2 = 1843.603\ (385.924)$				

[a]Smallest AIC and BIC are underlined.
[b]Parameter estimates of the logarithm of the random variable

geo-max-stable distribution is

$$ {}^{g}G_{\xi}(x) = \frac{1}{1-\ln G_{\xi}(x)} = \frac{1}{1+(1+\xi x)^{-1/\xi}}\,, \quad 1+\xi x > 0\,. \tag{2} $$

Using $\alpha = \frac{1}{|\xi|}$ in Eq. 2, ${}^{g}G_{\xi}$ can be split into the following three families:

– Loglogistic distributions, whose natural logarithm follows the logistic distribution, from the classical max-stable Fréchet-α distribution,

$$ {}^{g}\Phi_{\alpha}(x) = \frac{1}{1+x^{-\alpha}}\,\mathbb{I}_{[0,\infty)}(x),\ \alpha > 0\,; $$

– Logistic distribution, from the classical max-stable Gumbel distribution,

$$ {}^{g}\Lambda(x) = \frac{1}{1+\mathrm{e}^{-x}}\,\mathbb{I}_{\mathbb{R}}(x)\,; $$

– Backward loglogistic distributions, from the max-stable Weibull-α distribution,

$$ {}^{g}\Psi_{\alpha}(x) = \begin{cases} \frac{1}{1+(-x)^{\alpha}}\,, & x < 0 \\ 1\,, & x \geq 0 \end{cases}, \quad \alpha > 0\,. $$

Notice that in the limit distributions (1) and (2) (and in their particular cases) a location parameter $\lambda \in \mathbb{R}$ and a scale parameter $\delta > 0$ can be considered. Moreover, the characterizations of the domains of attraction of geo-max-stable thinned laws are similar to the characterizations of the corresponding max-stable laws.

4 Methods for modeling the data

To assess whether heavy-tailed models should be considered viable candidates to fit the data in Tables 1 and 3, including the mixture models hyperexponential and hyperloglogistic,

Table 6 ML parameter estimates and goodness-of-fit results for the yearly maxima of the OCR penalties data in Table 2

	AD	CvM	AIC[a]	BIC[a]
Lognormal				
$\widehat{\mu} = 7.871\ (0.267)$[b]	0.307	0.768	323.06	324.72
$\widehat{\sigma} = 1.099\ (0.189)$[b]	$(A_n^2 = 2.062)$	$(\omega_n^2 = 0.185)$		
GEV				
$\widehat{\xi} = 0.241\ (0.232)$	0.484	0.054	<u>321.98</u>	<u>324.48</u>
$\widehat{\lambda} = 2320.269\ (553.441)$	$(A_n^2 = 1.618)$	$(\omega_n^2 = 0.632)$		
$\widehat{\delta} = 1956.944\ (452.419)$				
GP				
$\widehat{\xi} = 0.123\ (0.257)$	0.001	0.800	322.64	325.14
$\widehat{\lambda} = 100$	$(A_n^2 = \infty)$	$(\omega_n^2 = 0.175)$		
$\widehat{\delta} = 2840.896\ (813.015)$				
Loglogistic				
$\widehat{\alpha} = 3.428\ (0.684)$	0.001	0.023	322.44	324.94
$\widehat{\lambda} = 100$	$(A_n^2 = \infty)$	$(\omega_n^2 = 0.752)$		
$\widehat{\delta} = 5143.624\ (636.031)$				
Hyperexponential				
$\widehat{\mathrm{p}} \approx 1\ (0.0000)$	0.806	0.969	322.13	324.63
$\widehat{\theta}_1 = 0.0002\ (0.0001)$	$(A_n^2 = 1.030)$	$(\omega_n^2 = 0.106)$		
$\widehat{\theta}_2 = 0.0099\ (0.0005)$				
Hyperloglogistic				
$\widehat{\mathrm{p}} = 0.712\ (0.056)$	0.871	0.875	320.33	324.50
$\widehat{\alpha}_1 = 1.578\ (0.656)$	$(A_n^2 = 0.910)$	$(\omega_n^2 = 0.149)$		
$\widehat{\delta}_1 = 2148.28\ (765.446)$				
$\widehat{\alpha}_2 = 17.775\ (7.719)$				
$\widehat{\delta}_2 = 5048.84\ (389.066)$				

[a]Smallest AIC and BIC are underlined.
[b]Parameter estimates of the logarithm of the random variable

log-log plots can be useful graphical tools. If a linear signature is detected in the data delimited by some cutoff point, then it is reasonable to consider power laws such as the GP or other regularly varying tail models. Note that, in the broadest sense, power laws are functional relationships of the type $f(x) = \left(\frac{x}{\delta}\right)^{-\alpha}$, $\alpha, \delta > 0$. Since $\ln f(x) = -\alpha \ln x + \alpha \ln \delta$, the straight line seen in a log-log plot is called the signature of the power law. From a statistical point of view, a power law, or more precisely, a distribution with a Paretian right-tail, is a model with a cumulative distribution function F that has a right-tail that satisfies $1 - F(x) = x^{-\alpha} L(x)$, where L is a slowly varying function, i.e., $\lim_{x\to\infty} \frac{L(tx)}{L(x)} = 1$, for all $t > 0$.

Therefore, to determine the existence of a linear signature in the data presented in Tables 1 and 3 (recall that the data in Tables 2 and 4 are subsets of the data in Tables 1 and 3, respectively), a density histogram, i.e., a histogram with an area equal to 1 to roughly estimate the underlying probability density function f, is considered for each case. The bandwidth used for the intervals of the density histogram for the data in Table 1 is $h = 860 \times 10^3$ USD, and for the data in Table 3, $h = 8250 \times 10^3$ USD. The log-log plot is displayed for both cases in Fig. 3, where x represents the midpoint of the interval and $f(x)$ the estimate of the probability density function f at value x, using the corresponding density histogram.

As noticed, a linear signature is clearly visible for the OCR penalties data (left-hand panel of Fig. 3), but this is not the case for the Attorneys General HIPAA fines data (right-hand panel of Fig. 3), which can be the consequence of the density histogram having fewer intervals due to the smaller sample size ($n = 56$). However, fitting the data with heavy-tailed models seems reasonable.

Using the work of Brilhante et al. [10] as a main reference, specifically with regard to the models used to fit

Table 7 ML parameter estimates and goodness-of-fit results for the Attorneys General HIPAA fines data in Table 3

	AD	CvM	AIC[a]	BIC[a]
Lognormal				
$\widehat{\mu} = 6.191\ (0.234)$[b]	0.596	0.993	918.75	922.80
$\widehat{\sigma} = 1.748\ (0.165)$[b]	$(A_n^2 = 1.791)$	$(\omega_n^2 = 0.120)$		
GEV				
$\widehat{\xi} = 1.269\ (0.184)$	0.643	0.924	910.88	916.96
$\widehat{\lambda} = 233.256\ (45.598)$	$(A_n^2 = 1.696)$	$(\omega_n^2 = 0.182)$		
$\widehat{\delta} = 311.120\ (72.677)$				
GP				
$\widehat{\xi} = 1.238\ (0.273)$	0.001	0.329	912.85	918.92
$\widehat{\lambda} = 15$	$(A_n^2 = \infty)$	$(\omega_n^2 = 0.437)$		
$\widehat{\delta} = 364.676\ (93.052)$				
Loglogistic				
$\widehat{\alpha} = 1.039\ (0.118)$	0.001	0181	916.14	922.22
$\widehat{\lambda} = 15$	$(A_n^2 = \infty)$	$(\omega_n^2 = 0.544)$		
$\widehat{\delta} = 391.781\ (86.322)$				
Hyperexponential				
$\widehat{\mathfrak{p}} = 0.843\ (0.056)$	0.397	0.510	<u>910.07</u>	<u>916.15</u>
$\widehat{\theta_1} = 0.0022\ (0.00053)$	$(A_n^2 = 2.240)$	$(\omega_n^2 = 0.349)$		
$\widehat{\theta_2} = 0.0001\ (0.00004)$				
Hyperloglogistic				
$\widehat{\mathfrak{p}} = 0.681\ (0.038)$	0.677	0.078	912.96	923.08
$\widehat{\alpha}_1 = 1.811\ (0.000)$	$(A_n^2 = 1.631)$	$(\omega_n^2 = 0.686)$		
$\widehat{\delta}_1 = 246.746\ (1.133)$				
$\widehat{\alpha}_2 = 0.804\ (0.156)$				
$\widehat{\delta}_2 = 1766.981\ (108.493)$				

[a]Smallest AIC and BIC are underlined.
[b]Parameter estimates of the logarithm of the random variable

vulnerabilities lifecycle variables, the lognormal, GEV, GP, loglogistic, hyperexponential and hyperloglogistic models are fit to each data set, since these models have produced good results. The goodness-of-fit assessment is carried out with the Anderson-Darling (AD) and the Cramér-von Mises (CvM) tests. Note that the Kolmogorov-Smirnov test is not considered here because the need to estimate the model parameters limits its proper use for these particular models, with the exception of the lognormal. On the other hand, the Akaike Information Criterion (AIC) and the Bayesian Information Criterion (BIC) are used to select the best fit between models that are supported by at least one goodness-of-fit test. It must be noted that it is sufficient to consider either AIC or BIC for model selection. Although having similar formulas, the main difference between the two measures is that the AIC strikes a balance between goodness-of-fit and model complexity, while the BIC introduces a stronger penalty for model complexity. In general, AIC is slightly lower than BIC.

As for the GP model with shape parameter $\xi \in \mathbb{R}$, location parameter $\lambda \in \mathbb{R}$ and scale parameter $\delta > 0$, it has a cumulative distribution function

$$F_{\xi,\lambda,\delta}(x) = \begin{cases} 1 - \exp\left(-\frac{x-\lambda}{\delta}\right) & , \ \xi = 0 \\ 1 - \left(1 + \xi \frac{x-\lambda}{\delta}\right)^{-\frac{1}{\xi}} & , \ \xi \neq 0 \end{cases}. \tag{3}$$

If $\xi \geq 0$ in Eq. 3, the distribution has support $[\lambda, \infty)$, and if $\xi < 0$, it has support $\left[\lambda, \lambda - \frac{\delta}{\xi}\right]$.

With regard to the mixture models hyperexponential and hyperloglogistic, only two components are considered for each case (Brilhante et al. [10] found no advantages in using three components for these two mixtures in their analysis): the hyperexponential model with cumulative distribution function

$$F(x) = \left[\mathfrak{p}\left(1 - \mathrm{e}^{-\theta_1 x}\right) + (1 - \mathfrak{p})\left(1 - \mathrm{e}^{-\theta_2 x}\right)\right] \mathbb{I}_{(0,\infty)}(x)\,,$$

Table 8 ML parameter estimates and goodness-of-fit results for the yearly maxima of the Attorneys General HIPAA fines data in Table 4

	AD	CvM	AIC[a]	BIC[a]
Lognormal				
$\widehat{\mu} = 7.243\ (0.572)$[b]	0.766	0.565	267.85	269.13
$\widehat{\sigma} = 2.139\ (0.404)$[b]	$(A_n^2 = 1.096)$	$(\omega_n^2 = 0.252)$		
GEV				
$\widehat{\xi} = 3.016\ (0.974)$	0.527	0.798	<u>264.38</u>	<u>266.30</u>
$\widehat{\lambda} = 245.462\ (151.856)$	$(A_n^2 = 1.530)$	$(\omega_n^2 = 0.177)$		
$\widehat{\delta} = 473.980\ (454.309)$				
GP				
$\widehat{\xi} = 0.267$ [c]	0.001	0.007	290.06	291.98
$\widehat{\lambda} = 90$	$(A_n^2 = \infty)$	$(\omega_n^2 = 0.892)$		
$\widehat{\delta} = 12920.61$ [c]				
Loglogistic				
$\widehat{\alpha} = 0.684\ (0.148)$	0.001	0.946	267.69	269.60
$\widehat{\lambda} = 90$	$(A_n^2 = \infty)$	$(\omega_n^2 = 0.119)$		
$\widehat{\delta} = 1057.166\ (737.218)$				
Hyperexponential				
$\widehat{\mathfrak{p}} = 0.666\ (0.159)$	0.814	0.293	267.27	269.17
$\widehat{\theta_1} = 0.00125\ (0.0020)$	$(A_n^2 = 1.015)$	$(\omega_n^2 = 0.367)$		
$\widehat{\theta_2} = 0.00004\ (0.0001)$				
Hyperloglogistic				
$\widehat{\mathfrak{p}} = 0.714\ (0.038)$	0.781	0.712	268.19	271.39
$\widehat{\alpha}_1 = 0.940\ (0.154)$	$(A_n^2 = 1.074)$	$(\omega_n^2 = 0.204)$		
$\widehat{\delta}_1 = 3427.299\ (2192.450)$				
$\widehat{\alpha}_2 = 5.867\ (3.376)$				
$\widehat{\delta}_2 = 122.633\ (32.147)$				

[a] Smallest AIC and BIC are underlined.
[b] Parameter estimates of the logarithm of the random variable.
[c] Standard errors are not available

with $0 \leq \mathfrak{p} \leq 1$ the mixing proportion and $\theta_1, \theta_2 > 0$; and the hyperloglogistic model with cumulative distribution function

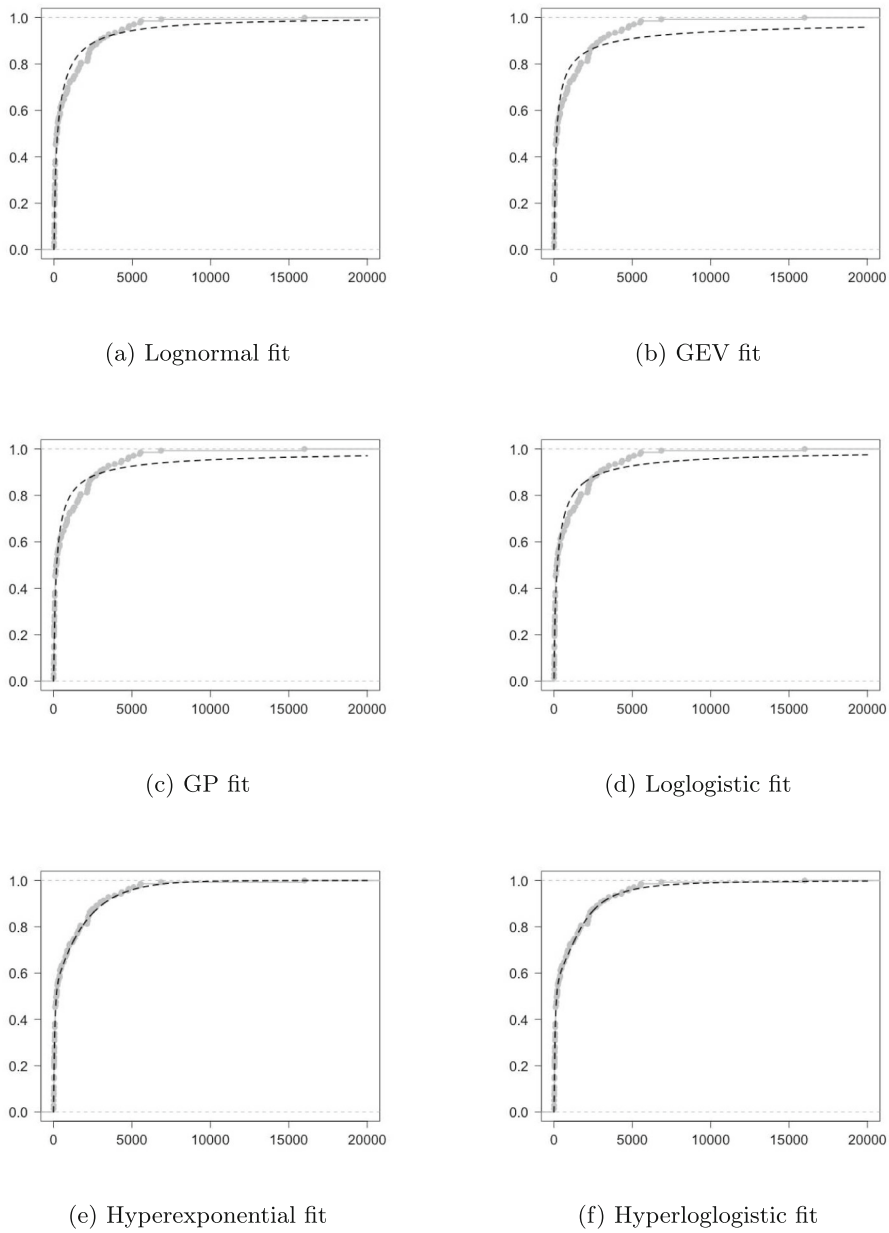
$$F(x) = \left[\mathfrak{p} \frac{1}{1+\left(\frac{x}{\delta_1}\right)^{-\alpha_1}} + (1-\mathfrak{p}) \frac{1}{1+\left(\frac{x}{\delta_2}\right)^{-\alpha_2}} \right] \mathbb{I}_{(0,\infty)}(x),$$

with $0 \leq \mathfrak{p} \leq 1$ and $\alpha_1, \alpha_2, \delta_1, \delta_2 > 0$.

The statistical analysis was carried out with the software R (v4.4.1), a Language and Environment for Statistical Computing.

5 Results and discussion

The results for the lognormal, GEV, GP, loglogistic, hyperexponential and hyperloglogistic fits for each data set are shown in Tables 5, 6, 7 and 8. Note that the standard errors of the Maximum Likelihood (ML) estimates of the model parameters are indicated in brackets, and since the ML estimates of the mixtures' parameters were obtained with the Expectation-Maximization algorithm, the standard errors indicated are bootstrap standard errors, based on 1000 bootstrap samples (for more details, see Efron and Tibshirani [40]). For each goodness-of-fit test, the p-value is indicated,



(a) Lognormal fit (b) GEV fit

(c) GP fit (d) Loglogistic fit

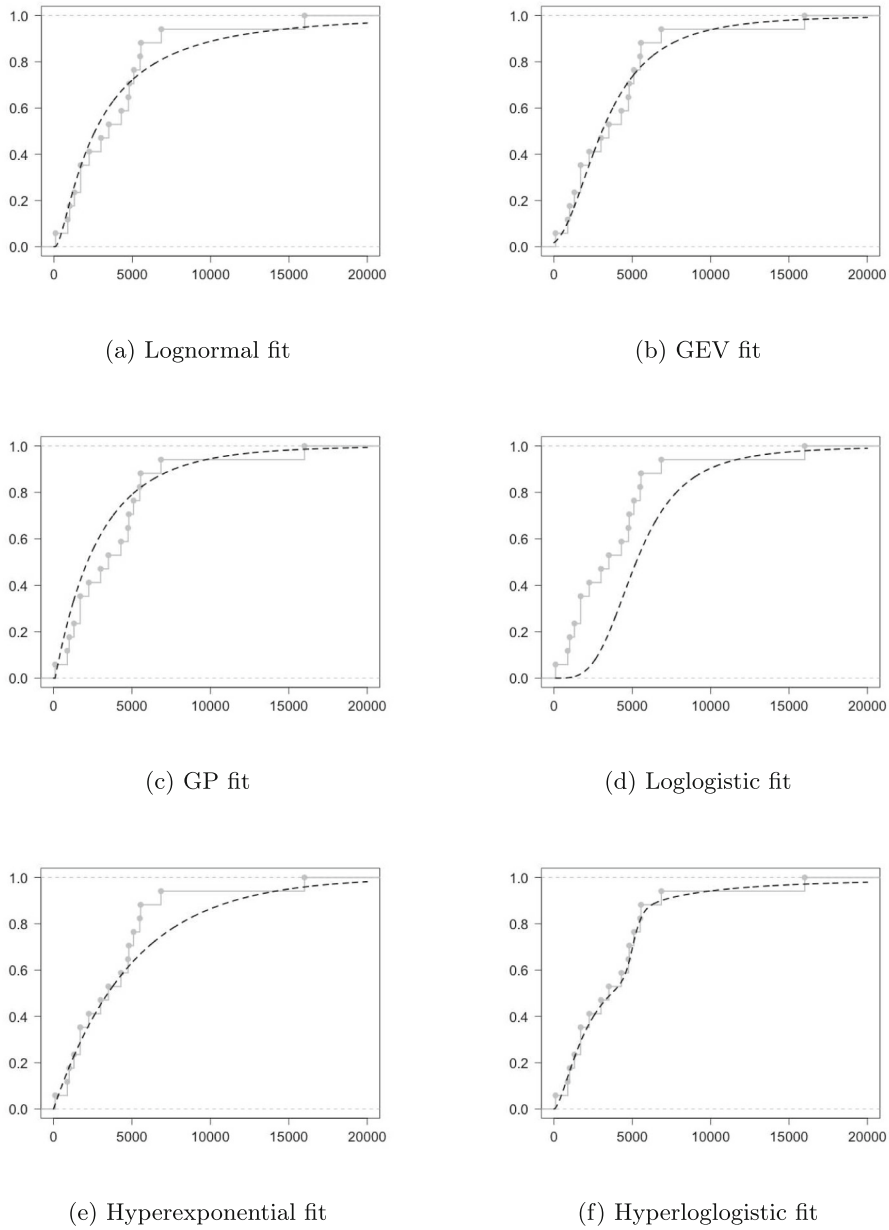
(e) Hyperexponential fit (f) Hyperloglogistic fit

Fig. 4 Empirical distribution function of the data (gray line) and theoretical distribution function of the model fits (black dashed lines) for the OCR penalties data in Table 1

with the value of the test's statistic being displayed underneath in brackets. The smallest observed values of AIC and BIC of the model fits are also underlined for each data set.

In particular, the results in Table 5 and in Table 7 show that, although the traditionally used GEV heavy-tailed model fits the data reasonably well, better fits, however, are achieved with the heavy-tailed hyperexponential and hyperloglogistic models. As for the results for the yearly maxima in Table 6 and in Table 8, which are subsets of the data in Table 1 and in Table 3, respectively, the GEV fit has the smallest AIC and BIC, as somewhat expected because we are dealing with maxima data. The hyperexponential and hyperloglogistic models also seem to be good fits for the maxima data.

Interestingly, the GP and loglogistic models are not supported by the AD test for any data set. Note that the AD test is a modification of the CvM test that gives more weight to the tails of the distribution. Moreover, the loglogistic model should be ruled out as an adequate fit for the yearly maxima of the OCR penalties data and the GP model should not be considered for the yearly maxima of the Attorneys General HIPAA fines data.



(a) Lognormal fit

(b) GEV fit

(c) GP fit

(d) Loglogistic fit

(e) Hyperexponential fit

(f) Hyperloglogistic fit

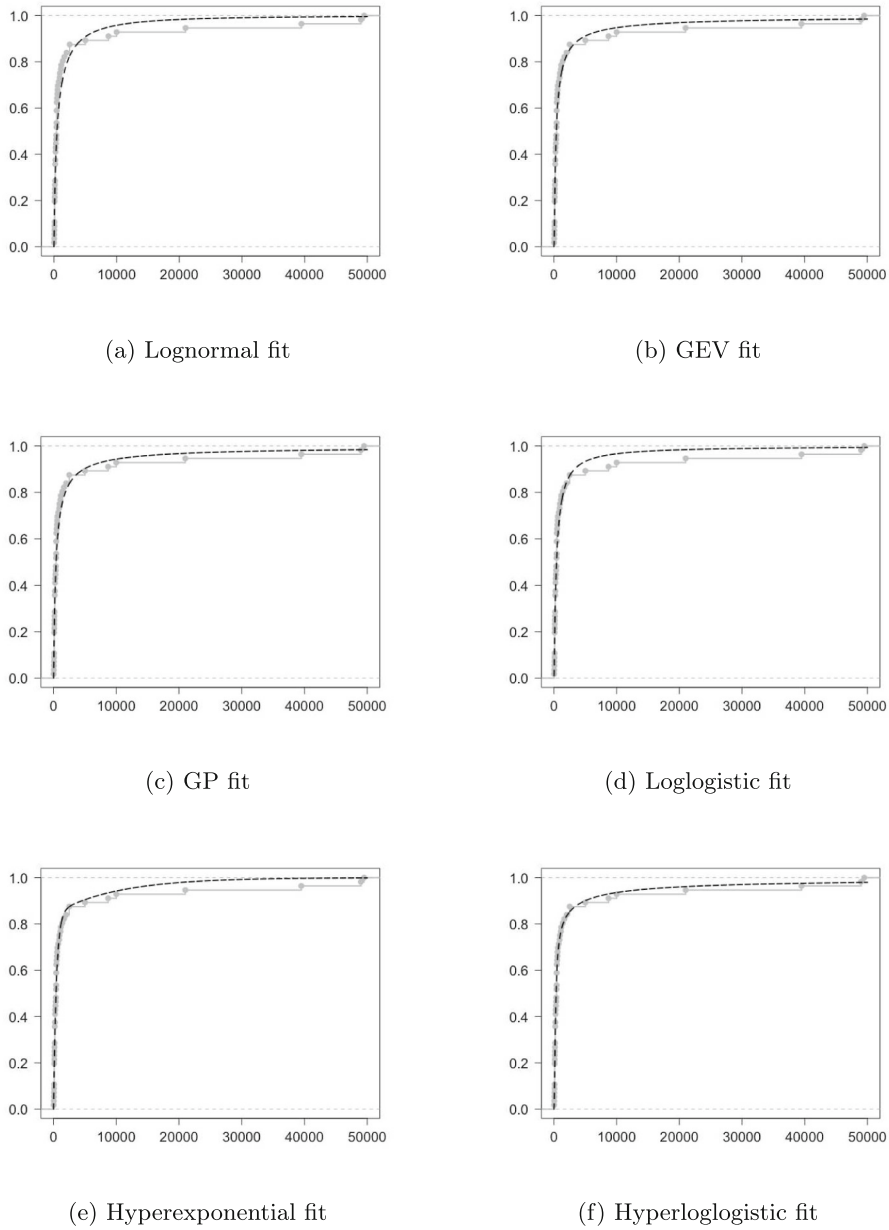
Fig. 5 Empirical distribution function of the data (gray line) and theoretical distribution function of the model fits (black dashed lines) for the yearly maxima of the OCR penalties data in Table 2

Noticing, in general, smaller AIC or BIC for the hyperexponential and hyperloglogistic fits for the data presented in Table 1 and in Table 3, seems to confirm that each data set contains two clusters, one for moderate values and another for extreme values. In fact, fines and penalties may result from moderate to severe breaches.

In Figs. 4, 5, 6 and 7, the empirical distribution function of each data set and each model fit are displayed separately to assess visually the goodness-of-fit of each model to the data. Undoubtedly, the graphs reinforce the idea that we are dealing with a mixture of moderate values and very high values, and therefore the use of mixtures models is useful in this context. Clearly, insurers and reinsurers should take this into account in their analysis.

6 Conclusions and open problems

As already mentioned, data on security breaches and losses are scarce. For this reason, official data on penalties and fines were used, for which a mixture of moderate and extremely outstanding values was detected. This clearly has



(a) Lognormal fit

(b) GEV fit

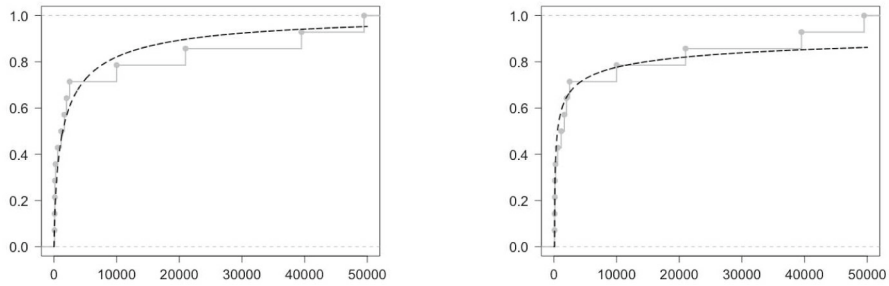
(c) GP fit

(d) Loglogistic fit

(e) Hyperexponential fit

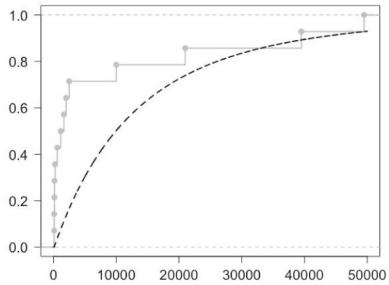
(f) Hyperloglogistic fit

Fig. 6 Empirical distribution function of the data (gray line) and theoretical cumulative distribution function of the model fits (black dashed lines) for the Attorneys General HIPAA fines data in Table 3

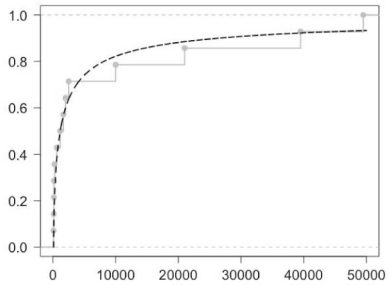


(a) Lognormal fit

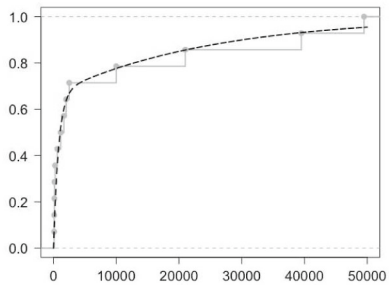
(b) GEV fit



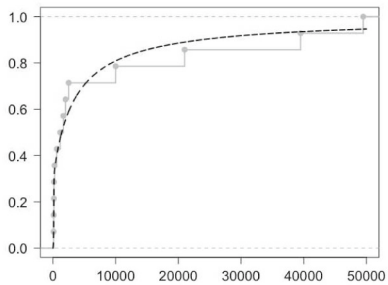
(c) GP fit



(d) Loglogistic fit



(e) Hyperexponential fit



(f) Hyperloglogistic fit

Fig. 7 Empirical distribution function of the data (gray line) and theoretical cumulative distribution function of the model fits (black dashed lines) for the yearly maxima of the Attorneys General HIPAA fines data in Table 4

consequences for insurance companies in terms of both pricing and reinsurance provisions. The rationale for using Panjer's theory for computing aggregate claims is well established (Klugman et al. [41]; Rólski et al. [42]), and in view of the heavy-tailed hyperexponential and hyperloglogistic goodness-of-fit for maxima, it seems reasonable to compound an additive model for moderate claims with some cautionary EV model provision. The overall picture gives some positive signals on the capacity of insurance and reinsurance companies to also provide coverage for extreme cyber losses scenarios — but perhaps at the cost of charging policyholders exorbitant amounts of money as a precautionary measure.

With regard to the OCR penalties data (Table 1), the AIC and BIC in Table 5 support the conclusion that mixture models, either the hyperexponential or the hyperloglogistic, provide the most reliable fit, and therefore there is a cluster of moderate data and a cluster of some extreme outstanding data. Moreover, as the yearly maxima in Table 2 is a sample of those outstanding data, the best fit that is revealed in Table 6 is with the GEV distribution, as expected. It is also interesting to notice that the estimate of the hyperexponential

mixture parameter is $\widehat{\mathrm{p}} \approx 1$, which clearly indicates that no more than a single component should be used, i.e., a simple exponential fit should be considered here.

For the Attorneys General fines (Table 3), the results in Table 7 show that the hyperexponential fit is the best one in terms of AIC and BIC, and for the corresponding yearly maxima (Table 4), the results in Table 8 show that the GEV model is again the best fit.

In view of the above, insurance companies must make provisions or reinsurance to be able to handle sums of large claims, eventually being modeled by additive stable laws with characteristic exponent $\alpha \in (0, 1)$, i.e., very heavy-tailed distributions, in the light of Lévy's [34] concept of additive stability. However, inferences using additive stable laws are a disappointment to work with, because the probability density functions of random variables other than the Gaussian ($\alpha = 2$), Cauchy ($\alpha = 1, \beta = 0$) and the Lévy ($\alpha = \frac{1}{2}, \beta = 1$) random variables, with β a skewness parameter, have no closed-form expressions, and thus methods based on the likelihood function are useless. Nonetheless, we believe that additive stable models with characteristic exponent $\alpha \in (0, 1)$ and $\beta = 1$ can play an important role in this context, but this is still an open problem that needs to be addressed properly.

As a final remark, we would like to say that, in the craft of statistical modeling, one must bear in mind that no chosen model is the true model, but some models are useful to understand, to some degree, the underlying reality of a phenomenon. Therefore, we must expect that with similar data collected from different time frames, the use of AIC or BIC as a measure for model selection can lead to different model choices, providing better fits than the GEV and the mixture models used in the present analysis. Moreover, when dealing with complex phenomena, as is the case here, mixture models should not be ruled out as natural candidates. However, the downside with the use of mixtures is that they usually have more parameters to estimate, and the trade-off between complexity and simplicity must always be an important factor to consider when selecting models.

Acknowledgements The authors would like to thank Steve Alder, Editor-in-Chief of *The HIPAA Journal*, for granting permission to use the data presented in Tables 1 to 4 and to use Figs. 1 and 2. We also extend our gratitude to Dr. Dave Dugal, former co-chair of CVSS-SIG, for authorizing the use of quotes from his presentation at the 35th Annual FIRST Conference in Montréal, 2023.

Author Contributions The authors contributed equally to this work.

Funding Open access funding provided by FCT|FCCN (b-on). Research partially financed by national funds through FCT—Fundação para a Ciência e a Tecnologia, Portugal, under the project UIDB/00006/2020 (https://doi.org/10.54499/UIDB/00006/2020), and research grant UIDB/00685/2020 of CEEAplA—Centro de Estudos de Economia Aplicada do Atlântico da Universidade dos Açores.

Declarations

Conflicts of Interest The authors declare no conflict of interest.

References

1. Tunggal AT. What is a vulnerability? Definition + Examples. https://www.upguard.com/blog/vulnerability Accessed 01-July-2024
2. Howard JD. An analysis of security incidents on the internet. PhD thesis, Carnegie Mellon University; 2012. https://insights.sei.cmu.edu/library/an-analysis-of-security-incidents-on-the-internet/ Accessed 01-July-2024
3. Lian C, Santos JR, Haimes YY. Extreme risk analysis of interdependent economic and infrastructure sectors. Risk Anal. 2007;27:1053–64. https://doi.org/10.1111/j.1539-6924.2007.00943.x.
4. Dejung S. Economic impact of cyber accumulation scenarios. Swiss Insurance Association Cyber Working Group; 2017. https://www.imia.com/wp-content/uploads/2023/07/Economic_impact_Cyber_loss_accumulation_scenarios_SVV.pdf
5. Eling M, Elvedi M, Greg Falco G. The economic impact of extreme cyber risk scenarios. North Am Actuar J. 2023;27(3):429–43. https://doi.org/10.1080/10920277.2022.2034507.
6. Nikolakopoulos T, Darra E, Tofan D. The cost of incidents affecting CIIs: systematic review of studies concerning the economic impact of cyber-security incidents on critical information infrastructures (CII). ENISA, Heraklion, Greece; 2016. https://data.europa.eu/doi/10.2824/475621
7. Lagazio M, Sherif N, Cushman M. A multi-level approach to understanding the impact of cyber crime on the financial sector. Comput Secur. 2014;45:58–74. https://doi.org/10.1016/j.cose.2014.05.006.
8. Common Vulnerabilities Scoring System. https://www.first.org/cvss/v4-0/ Accessed 01-July-2024
9. Dugal D, Rich D. Announcing CVSS v4.0. In: 35th Annual FIRST Conference, Montréal, Canada; 2023. https://www.first.org/resources/papers/conf2023/FIRSTCON23-TLP-CLEAR-SIG-Updates-CVSS-SIG-slides-Dave-Dugal.pdf
10. Brilhante MF, Pestana D, Pestana P, Rocha ML. Measuring the risk of vulnerabilities exploitation. Appl Math. 2023;4(1):20–54. https://doi.org/10.3390/appliedmath4010002.
11. Brilhante MF, Pestana P, Rocha ML, Sequeira F. Risk assessment of vulnerabilities exploitation. In: Henriques-Rodrigues L, Menezes R, Meira Machado L, Faria S, Carvalho M, editors. New Frontiers

in Statistics and Data Science; 2025. pp. 69–82. Springer, Berlin. https://doi.org/10.1007/978-3-031-68949-9_6
12. Fahrenwaldt MA, Weber S, Weske K. Pricing of cyber insurance contracts in a network model. ASTIN Bull. 2018;48(3):1175–218. https://doi.org/10.1017/asb.2018.23.
13. Xu M, Hua L. Cybersecurity insurance: modeling and pricing. North Am Actuar J. 2019;23(2):220–49. https://doi.org/10.1080/10920277.2019.1566076.
14. Egan R, Cartagena S, Mohamed R, Gosrani V, Grewal J, Acharyya M, Dee A, Bajaj R, Jaeger V, Katz D, Meghen P, Silley M, Nasser-Probert S, Pikinska J, Rubin R, Ang K. Cyber operational risk scenarios for insurance companies. Actuar J. 2019;24(6):1–34. https://doi.org/10.1017/S1357321718000284.
15. Öğüt H, Raghunathan S, Menon N. Cyber security risk management: public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection. Risk Anal. 2011;31(3):497–512. https://doi.org/10.1111/j.1539-6924.2010.01478.x.
16. Swiss Re Institute. https://www.swissre.com/institute/ Accessed 05-Aug-2024
17. Rachev ST, Resnick S. Max-geometric infinite divisibility and stability. Commun Stat Stoch Model. 1991;7:191–218. https://doi.org/10.1080/15326349108807184.
18. Griffiths C. The Latest 2024 Cyber Crime Statistics. https://aag-it.com/the-latest-cyber-crime-statistics/ Accessed 01-July-2024
19. Griffiths C. The Latest 2024 Ransomware Statistics. https://aag-it.com/the-latest-ransomware-statistics/ Accessed 01-July-2024
20. Griffiths C. The Latest Cloud Computing Statistics. https://aag-it.com/the-latest-cloud-computing-statistics/ Accessed 01-July-2024
21. Office for Civil Rights Breach Portal. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf Accessed 01-July-2024
22. The HIPAA Journal: Healthcare Data Breach Statistics. https://www.hipaajournal.com/healthcare-data-breach-statistics/ Accessed 01-July-2024
23. Neto NN, Madnick S, Paula AM, Borges NM. Developing a global data breach database and the challenges encountered. J Data Inf Quality. 2021;13(1):1–33. https://doi.org/10.1145/3439873.
24. Trautman LJ, Ormerod P. Wannacry, ransomware, and the emerging threat to corporations. Tennessee Law Rev. 2018;86:503–56. https://doi.org/10.2139/ssrn.3238293.
25. Clauset A, Shalizi CR, Newman MEJ. Power-law distributions in empirical data. SIAM Rev. 2009;51(4):661–703. Companion implementation of the methods in https://aaronclauset.github.io/powerlaws/
26. Stumpf MPH, Porter MA. Critical truths about power laws. Science. 2012;335:665–6. https://doi.org/10.1126/science.1216142.
27. Feldmann A, Whitt W. Fitting mixtures of exponentials to long-tail distributions to analyze network performance models. Perform Eval. 1998;31(3/4):245–79. https://doi.org/10.1016/S0166-5316(97)00003-5.
28. Mitzenmacher M. A brief history of generative models for power law and lognormal distributions. Int Math. 2004;1(2):226–51. https://doi.org/10.1080/15427951.2004.10129088.
29. Fisher RA, Tippett LHC. Limiting forms of the frequency distribution of the largest and smallest member of a sample. Proc Camb Phil Soc. 1928;24:189–90.
30. Gomes MI, Pestana D. Large claims – extreme value models. In: Goovaerts M, Vylder F, Haezendonck J, editors. Insurance and Risk Theory. Dordrecht: Springer; 1986. p. 301–23.
31. Embrechts P, Claudia Klüppelberg C, Mikosch T. Modelling Extremal Events for Insurance and Finance. Berlin, Heidelberg, Germany: Springer; 1997.
32. Beirlant J, Goegebeur Y, Teugels J, Segers J. Statistics of Extremes: Theory and Applications. Berlin, USA: Wiley; 2004.
33. Fréchet M. Sur la loi de probabilité de l'écart maximum. Annales de la Société Polonaise de Mathématique. 1927;6(1):93–117.
34. Lévy P.: Calcul des Probabilités. Gauthier-Villars, Paris, France,. Reprinted in 2004. Paris, France: Editions Jacques Gabay; 1925.
35. Gnedenko BV. Sur la distribution limite du terme maximum d'une série aléatoire. Ann Math. 1943;44(3):423–53. https://doi.org/10.2307/1968974.
36. de Haan L. On Regular Variation and Its Application to the Weak Convergence of Sample Extremes. Amsterdam, Netherlands: Universiteit van Amsterdam; 1970.
37. von Mises R. La distribution de la plus grande de n valeurs. Rev Math Union Interbalcanique. 1936;1:141–60. Reprinted in Selected Papers of Richard von Mises, Amer Math Soc. 1954;2:271–94
38. Jenkinson AF. The frequency distribution of the annual maximum (or minimum) values of meteorological elements. Q J R Meteorol Soc. 1955;81(348):158–71.
39. Gomes MI, Guillou A. Extreme value theory and statistics of univariate extremes: a review. Int Stat Rev. 2015;83(2):263–92. https://doi.org/10.1111/insr.12058.
40. Efron B, Tibshirani R. Bootstrap methods for standard errors, confidence intervals, and other measures of statistical accuracy. Stat Sci. 1986;1(1):54–75. https://doi.org/10.1214/ss/1177013815.
41. Klugman SA, Panjer HH, Willmot GE. Loss Models: From Data to Decisions, New York, USA: Wiley ; 1998. https://doi.org/10.1002/9780470391341
42. Rólski T, Schmidli H, Schmidt V, Teugels J. Stochastic Processes for Insurance and Finance. New York, USA: Wiley; 1999.

Authors and Affiliations

M. Fátima Brilhante[1,2] · Sandra Mendonça[2,3] · Pedro Pestana[4,5] · M. Luísa Rocha[2,6,7] · Rui Santos[2,8]

✉ Rui Santos
rui.santos@ipleiria.pt

M. Fátima Brilhante
maria.fa.brilhante@uac.pt

Sandra Mendonça
sandram@staff.uma.pt

Pedro Pestana
pedro.pestana@uab.pt

M. Luísa Rocha
maria.ls.rocha@uac.pt

1 Faculdade de Ciências e Tecnologia, Universidade dos Açores, Rua da Mãe de Deus, Ponta Delgada 9500-321, Portugal

2 Centro de Estatística e Aplicações, Universidade de Lisboa (CEAUL), Campo Grande, Lisboa 1749-016, Portugal

3 Departamento de Matemática – FCEE, Universidade da Madeira, Campus Universitário da Penteada, Funchal 9020-105, Portugal

4 Departamento de Ciências e Tecnologia, Universidade Aberta, Rua Almirante Barroso 38, Lisboa 1000-013, Portugal

5 Centro de Investigação em Ciência e Tecnologia das Artes (CITAR), Rua de Diogo Botelho 1327, Porto 4169-005, Portugal

6 Faculdade de Economia e Gestão, Universidade dos Açores, Rua da Mãe de Deus, Ponta Delgada 9500-321, Portugal

7 Centro de Estudos de Economia Aplicada do Atlântico (CEEAplA), Universidade dos Açores, Rua da Mãe de Deus, Ponta Delgada 9500-321, Portugal

8 Escola Superior de Tecnologia e Gestão, Instituto Politécnico de Leiria, Apartado 4133, Leiria 411-901, Portugal