Cyber Risk Mitigation Strategies

Marco PIRRA

UniCal - Department of Economics, Statistics and Finance

5th European
Congress of Actuaries
www.eca2024.org

About the speaker

- **Marco Pirra –** *Researcher*

  Lecturer in Life Insurance and Non-Life Insurance Mathematics, Researcher in the quantitative economics area: his work is presently focused on solvency assessment models for insurance companies and emerging risks. Fully Qualified Actuary.

  Member of the AFIR-ERM Section

AFIR-ERM
Finance, Investment & ERM

- Università della Calabria

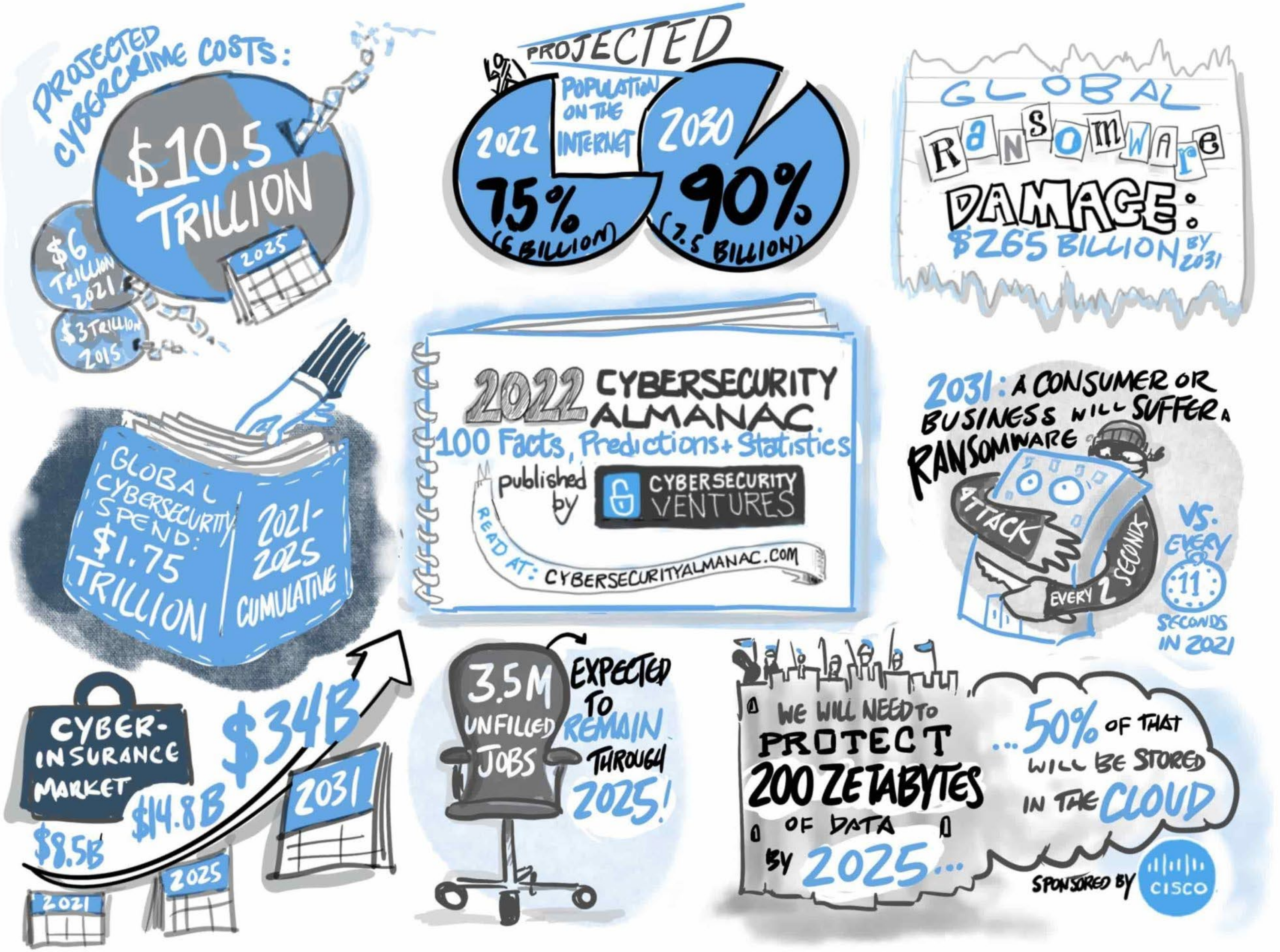
  UniCal - Department of Economics, Statistics and Finance

Agenda

- ✓ *Introduction/Motivation*
- ✓ *Methodology*
- ✓ *Results*
- ✓ *Conclusions*

The cost of Cybercrime [*Cybersecurity Ventures*]

If it were measured as a country, then cybercrime — inflicted damages totaling **$8 trillion USD** globally in 2023 — would be the world's third-largest economy after the U.S. and China, surpassing the wealth of entire nations



PROJECTED CYBERCRIME COSTS:
$10.5 TRILLION
2025
$6 TRILLION 2021
$3 TRILLION 2015
PROJECTED
POPULATION ON THE INTERNET
2022
75%
(6 BILLION)
2030
90%
(7.5 BILLION)
GLOBAL RANSOMWARE DAMAGE:
$265 BILLION BY 2031
2022 CYBERSECURITY ALMANAC
100 Facts, Predictions + Statistics
published by
CYBERSECURITY VENTURES
READ AT: CYBERSECURITYALMANAC.COM
2031: A CONSUMER OR BUSINESS WILL SUFFER A RANSOMWARE ATTACK EVERY 2 SECONDS
VS. EVERY 11 SECONDS IN 2021
GLOBAL CYBERSECURITY SPEND: $1.75 TRILLION
2021-2025 CUMULATIVE
CYBER-INSURANCE MARKET
$8.5B
2021
$14.8B
2025
$34B
2031
3.5M UNFILLED JOBS
EXPECTED TO REMAIN THROUGH 2025!
WE WILL NEED TO PROTECT 200 ZETABYTES OF DATA BY 2025...
...50% OF THAT WILL BE STORED IN THE CLOUD
SPONSORED BY CISCO

https://cybersecurityventures.com/cybersecurity-almanac-2023/

The cost of Cybercrime [*Cybersecurity Ventures*]

Global cybercrime **costs expected to grow by 15 percent per year** over the next five years, *reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015.*
Digital ad fraud is **rising sharply**.

Cybercrimes are **vastly undercounted** because they aren't reported — due to embarrassment, fear of reputational harm, and the notion that law enforcement can't help (amongst other reasons). Some estimates suggest as few as 10 percent of the total number of cybercrimes committed each year are actually reported.

Cryptocrime, or crimes having to do with cryptocurrencies, are predicted to cost the world $30 billion in 2025, up from an estimated $17.5 billion in 2021.
The **cyberinsurance market will grow** to $14.8 billion in 2025 (from approximately $8.5 billion in 2021), and exceed $34 billion by 2031, based on a compound annual growth rate (CAGR) of 15 percent over an 11-year period (2020 to 2031) calculated.

https://cybersecurityventures.com/cybersecurity-almanac-2023/

Annual Cost of a Data Breach Study 2023 [*Ponemon*]

2023 Cost of a Data Breach Study: Global Overview

Benchmark research sponsored by IBM Security
Independently conducted by Ponemon Institute LLC

The average cost of a data breach reached an **all-time high** in 2023 of USD 4.45 million. This represents a 2.3% increase from the 2022 cost of USD 4.35 million.

Taking a long-term view, the average cost has increased **15.3%** from USD 3.86 million in the 2020 report.

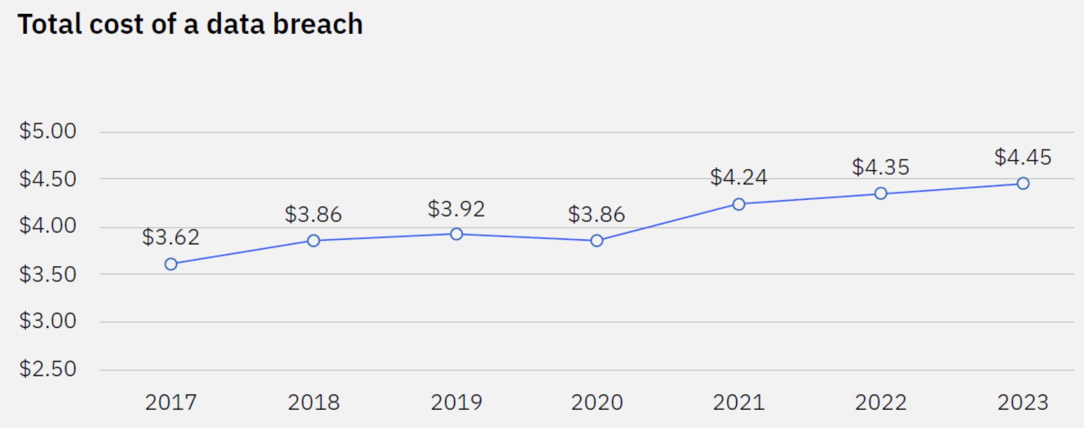


Figure 1. Measured in USD millions

Now in its 18th year, the Cost of a Data Breach Report has become one of the leading benchmark reports in the cybersecurity industry. The report offers IT, risk management and security leaders a lens into dozens of factors that can increase or help mitigate the rising cost of data breaches.

https://www.ibm.com/security/data-breach/

Annual Cost of a Data Breach Study 2023 [*Ponemon*]

The per-record cost of a data breach also reached a new high.

In 2023, the average cost per record involved in a data breach was **USD 165**, a small increase from the 2022 average of USD 164. This matches the relatively small growth from 2021 to 2022, where the cost rose by just USD 3.

In the last seven years, the largest increase in average per-record costs was between 2020 and 2021, when the average rose from USD 146 to USD 161 or 10.3%.

Per-record cost of a data breach

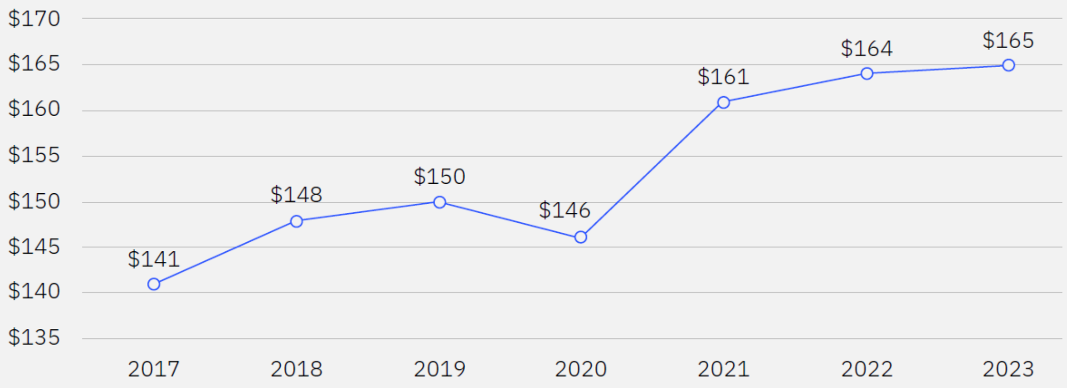


Figure 2. Measured in USD

This study examined breaches sized between 2,200 and 102,000 records. It's not consistent with this research to use the per record cost to calculate the cost of single or multiple breaches above 102,000 records

https://www.ibm.com/security/data-breach/

Annual Cost of a Data Breach Study 2023 [*Ponemon*]

Across industries, **healthcare reported the highest costs for the 13th year in a row**.
Healthcare continues to experience the highest data breach costs of all industries, increasing from USD 10.10 million in 2022 to USD 10.93 million in 2023—an increase of 8.2%. Over the past three years, the average cost of a data breach in healthcare has grown 53.3%, increasing more than USD 3 million compared to the average cost of USD 7.13 million in 2020. Healthcare faces high levels of industry regulation and is considered critical infrastructure by the US government.
Since the start of the COVID-19 pandemic, the industry has seen notably higher average data breach costs.

The top three industries by cost were unchanged in the order of ranking from the 2021 report. Following healthcare were the financial and pharmaceuticals industries.

https://www.ibm.com/security/data-breach/

Cost of a data breach by industry

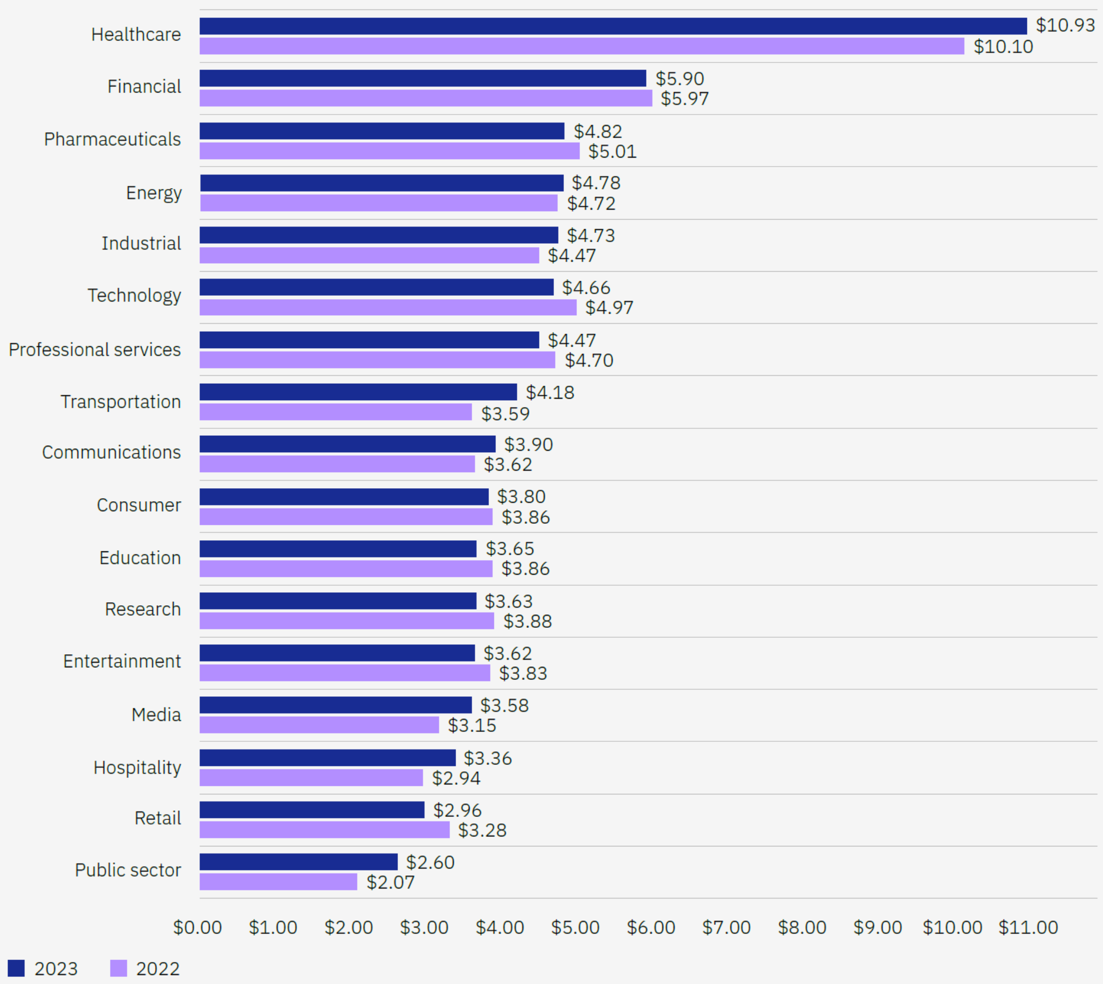
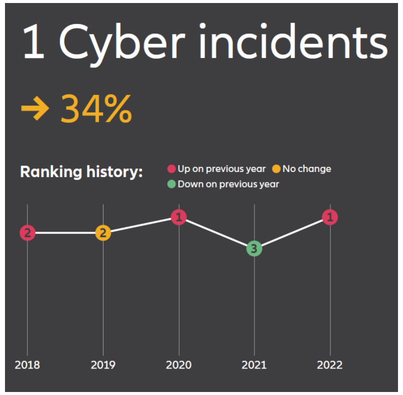


Figure 4. Measured in USD millions

Economical Impact [*Allianz Risk Barometer 2023*]

The 12th Allianz Risk Barometer incorporates the views of 2,712 respondents from 94 countries and territories

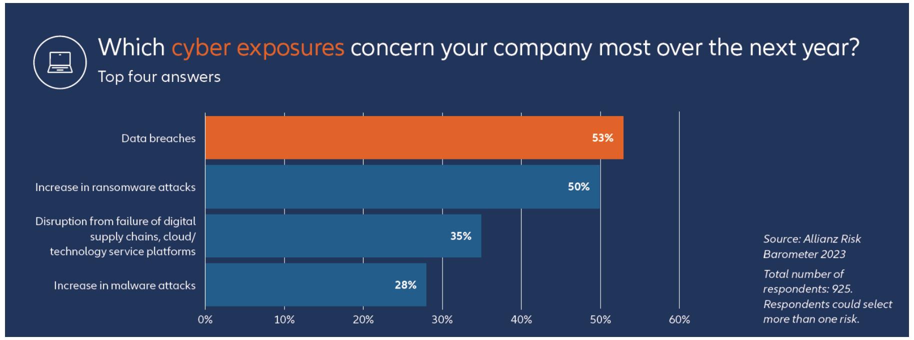
Cyber risks, such as IT outages, ransomware attacks or data breaches, rank as the **most important** risk globally (34% of responses) for the second year in succession – the first time this has occurred.



1 Cyber incidents

→ 34%

A **data breach** is the exposure which concerns companies **most**, given data privacy and protection is one of the key cyber risks and related legislation has toughened globally in recent years.



Which cyber exposures concern your company most over the next year?

Top four answers

Source: Allianz Risk Barometer 2023

Total number of respondents: 925. Respondents could select more than one risk.

“The role of insurance has always been to ensure good risk management and loss prevention,” “Good cyber maturity and good cyber insurance go hand-in-hand.

Demand for cyber insurance continues to grow, reflecting increased awareness of exposures associated with digitalization and remote working.

https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2023-press.html

An insurance market perspective

Cyber insurance can **boost** society's **overall cyber resilience** to help ensure that the full network benefits of digitalisation can be realised.

The cyber insurance market remains **small** and **nascent**.

Premiums represent **less than 1%** of the global property and casualty market while some reports indicate that only around a third of small businesses purchase this kind of insurance.

Cyber Risk Insurance expected to be the **largest market in p/c insurance** in 2036 in the German speaking countries.

https://www.genevaassociation.org/research-topics/cyber/ransomware-report

Data breaches

A **data breach** is an incident where information is stolen or taken from a system without the knowledge or authorization of the system’s owner.

A small company or large organization may suffer a data breach. Stolen data may involve sensitive, proprietary, or confidential information such as credit card numbers, customer data, trade secrets or matters of national security.

The effects brought on by a data breach can come in the form of damage to the target company’s reputation due to a perceived ‘betrayal of trust.’ Victims and their customers may also suffer ***financial losses*** should related records be part of the information stolen.

Literature Overview

Bessy-Roland Y., Boumezoued A., Hillairet C. *(2020). Multivariate Hawkes process for cyber insurance. https://hal.archives-ouvertes.fr/hal-02546343*

Betterley R. S. *(2016). Cyber/privacy insurance market survey: A tough market for larger insureds, but smaller insureds finding eager insurers. The Betterley Report.*

Böhme R. and G. Kataria G. *(2006). Models and measures for correlation in cyber-insurance. Fifth Workshop on the Economics of Information Security (WEIS), University of Cambridge, UK.*

Böhme R. and Schwartz G*. (2010). Modeling cyber-insurance: Towards a unifying framework. Ninth Fifth Workshop on the Economics of Information Security (WEIS), Harvard.*

Böhme, R., S. Laube and M. Riek. *(2017). A Fundamental Approach to Cyber Risk Analysis. Variance 11, no. 2: 161–85.*

De Giovanni, D., A. Leccadito and M. Pirra *(2021). On the determinants of data breaches: A cointegration analysis. Decisions in Economics and Finance, 1-20.*

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

Eling, M. and W. Schnell *(2016). What do we know about cyber risk and cyber risk insurance? The Journal of Risk Finance, 17(5).*

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

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

Eling, M. *(2020). Cyber risk research in business and actuarial science. European Actuarial Journal volume 10, 303–333.*

Gordon, L. A., Loeb, M. P. and Sohail, T. *(2003). A framework for using insurance for cyber- risk management. Communications of the ACM, 46(3):81–85.*

Literature Overview

Herath, V. S. B. and Herath, T. C. *(2011). Copula-based actuarial model for pricing cyber-insurance policies. Insurance Markets and Companies: Analyses and Actuarial Computations, 2:7–20.*

Hillairet C., Lopez O.*, (2020) Propagation of cyber incidents in an insurance portfolio: counting processes combined with compartmental epidemiological models. https://hal.archives-ouvertes.fr/hal-02564462v2*

Kosub, T. *(2015). Components and challenges of integrated cyber risk management. Zeitschrift fur die gesamte Versicherungswissenschaft, 104(5):615–634.*

Mukhopadhyay A., Chatterjee S., Saha D., Mahanti A. and Sadhukhan S. K. *(2006). e-Risk management with insurance: A framework using copula aided Bayesian belief networks. In Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06), vol. 6, 126.1–126.6. Hoboken, NJ: IEEE.*

Schwartz, G. A. and Sastry, S. S. *(2014). Cyber-insurance framework for large-scale interdependent networks. In Proceedings of the Third International Conference on High Confidence Networked Systems, 145–154. New York: ACM.*

Tatar U., Keskin O., Bahsi H., Ariel Pinto C., *(2020) Quantification of Cyber Risk for Actuaries An Economic-Functional Approach, Society of Actuaries.*

Wheatley, S., A. Hofmann, and D. Sornette *(2019). Data breaches in the catastrophe framework & beyond. arXiv preprint arXiv:1901.00699 .*

Wheatley, S., A. Hofmann, and D. Sornette *(2020). Addressing insurance of data breach cyber risks in the catastrophe framework. The Geneva Papers on Risk and Insurance-Issues and Practice.*

Wheatley, S., T. Maillart, and D. Sornette *(2016). The extreme risk of personal data breaches and the erosion of privacy. The European Physical Journal B 89(1), 7.*

Xu, M., and Hua, L. *(2019) Cybersecurity Insurance: Modeling and Pricing, North American Actuarial Journal, 23, 220-249.*

Yang, Z. and Lui, J. C. S. *(2014). Security adoption and influence of cyber-insurance markets in heterogeneous networks. Performance Evaluation, 74:1–17.*

Contribution of the research

The objective of our research is to contribute to the actuarial literature on cyber risk assessment in order to provide **possible solutions** for the reduction of the gap between supply and demand of cyber insurance.

In particular, the aim is to achieve a better understanding in quantifying, managing and pricing cyber risk by means of:

I. a **deeper awareness** of cyber risks and of the economic damages they produce;

II. the introduction and validation of new **actuarial techniques** to allow insurers a more effcient management of this new class of risk;

III. The design of **innovative insurance contracts** and alternative ways of risk transfers to reduce the costs of insurance premiums.

Privacy Rights Clearinghouse [*www.privacyrights.org*]

Records Breached: 11,575,804,706
from 8,804 DATA BREACHES
made public since 2005

The first dataset we analyze was obtained from the **Privacy Rights Clearinghouse (PRC)** which is one of the largest and most extensive datasets that is also publicly available.

PRC maintains the Chronology of Data Breaches as a source of information to assist in research involving reported data breaches from 2005 to present.

Many organizations are not aware they've been breached or are not required to report it based on reporting laws. PRC's Chronology is limited to data breaches reported in the U.S. If a data breach affects individuals in other countries, it is included only if individuals in the U.S. are also affected.

Privacy Rights Clearinghouse [*www.privacyrights.org*]

Year	Events	Records
2005	136	55,101,241
2006	482	68,580,749
2007	456	149,957,921
2008	355	130,896,900
2009	270	251,575,814
2010	801	140,937,393
2011	793	447,901,379
2012	886	298,766,833
2013	890	158,789,584
2014	869	1,313,623,927
2015	547	318,837,458
2016	826	4,815,012,420
2017	863	2,051,896,420
2018	828	1,371,001,705
2019	16	321,922

Types of data breach

CARD Payment Card Fraud – fraud involving debit and credit cards that is not accomplished via hacking (e.g., skimming devices at point-of-service terminals)
DISC Unintended disclosure – sensitive information either posted publicly on a website, mishandled, or sent to the wrong party via email, fax, or mail
HACK Hacking or malware – electronic entry by an outside party, malware, and spyware
INSD Insider – someone with legitimate access, such as an employee or contractor, intentionally breaches information
PHYS Physical loss – lost, discarded, or stolen non-electronic records, such as paper documents
PORT Portable device – lost, discarded, or stolen laptop, PDA, smartphone, portable memory device, CD, hard drive, data tape, etc.
STAT Stationary device – lost, discarded, or stolen stationary electronic device, such as a computer or server not designed for mobility
UNKN Unknown or other

Entity types

BSF BSF Businesses – Financial and insurance services
BSO BSO Businesses – Other
BSR BSR Businesses – Retail/Merchant
EDU EDU Educational institution
GOV GOV Government and military
MED MED Healthcare – Medical providers
NGO NGO Nonprofit organizations

Type	Events	%	Records	%
CARD	68	0.75%	9,203,036	0.08%
DISC	1802	19.98%	2,815,845,013	24.33%
HACK	2584	28.65%	8,207,451,875	70.92%
INSD	608	6.74%	83,580,453	0.72%
PHYS	1735	19.24%	40,769,571	0.35%
PORT	1172	13.00%	185,650,895	1.60%
STAT	249	2.76%	16,235,932	0.14%
UNKN	800	8.87%	214,464,891	1.85%

Entity	Events	%	Records	%
BSF	788	8.74%	643,820,265	5.56%
BSO	1047	11.61%	8,990,170,575	77.68%
BSR	623	6.91%	1,383,161,417	11.95%
EDU	862	9.56%	66,376,099	0.57%
GOV	781	8.66%	227,483,420	1.97%
MED	4321	47.92%	242,968,015	2.10%
NGO	119	1.32%	8,444,531	0.07%
UNKN	477	5.29%	10,777,344	0.09%

Breach Level Index [*breachlevelindex.com*]

Data Breach Statistics

Data Records Lost or Stolen Since 2013

14,717,618,286 records

ONLY 4% of breaches were “Secure Breaches” where encryption was used and the stolen data was rendered useless.

The second dataset we analyze was obtained from the **Breach Level Index Data Breach Database** a centralized, global database of data breaches with calculations of their severity based on multiple factors.

The Breach Level Index not only tracks publicly disclosed breaches, but also allows organizations to do their own risk assessment based on a few simple inputs that will calculate their risk score, overall breach severity level, and summarize actions IT can take to reduce the risk score.

Gemalto is the world leader in digital security, helping the largest and most respected brands protect their data, identities, and intellectual property.

Breach Level Index [*breachlevelindex.com*]

YEAR	Events	Records
2013	1217	2,107,666,417
2014	1746	2,888,466,820
2015	1887	743,462,574
2016	1993	1,388,190,640
2017	1958	2,962,190,464
2018	1505	4,876,541,349

#	Source	Events	%	Records	%
1	**Accidental Loss**	2428	24%	4,532,637,539	30.3%
2	**Hacktivist**	164	2%	65,343,200	0.4%
3	**Lost Device**	5	0%	115,007	0.0%
4	**Malicious Insider**	1194	12%	306,945,069	2.1%
5	**Malicious Outsider**	6298	61%	9,430,616,718	63.0%
6	**Ransomware**	5	0%	-	0.0%
7	**State Sponsored**	130	1%	628,967,833	4.2%
8	**Stolen Device**	15	0%	59,069	0.0%
9	**Unknown**	67	1%	1,833,829	0.0%

#	Industry	Events	%	Records	%
1	**Education**	879	8.5%	126,843,836	0.8%
2	**Entertainment**	104	1.0%	502,594,229	3.4%
3	**Financial**	1301	12.6%	552,524,623	3.7%
4	**Government**	1418	13.8%	1,298,531,178	8.7%
5	**Healthcare**	2714	26.3%	291,675,274	1.9%
6	**Hospitality**	106	1.0%	527,606,802	3.5%
7	**Industrial**	138	1.3%	21,119,009	0.1%
8	**Insurance**	83	0.8%	12,700,290	0.1%
9	**Non-profit**	74	0.7%	410,488	0.0%
10	**Other**	1324	12.8%	3,110,303,702	20.8%
11	**Professional Services**	202	2.0%	147,140,489	1.0%
12	**Retail**	1131	11.0%	1,228,013,093	8.2%
13	**Social Media**	34	0.3%	2,758,853,076	18.4%
14	**Technology**	798	7.7%	4,388,202,175	29.3%

Framework

Count time series $\{Y_t : t \in N\}$. Y_t models the observed breach size at time t.

Time-varying regressors $X_t = \left(X_{t,1}, \dots, X_{t,r}\right)^T$

Conditional mean $E[Y_t | F_{t-1}\ ] = \lambda_t,$
where F_t is the history generated by the joint process $\{Y_t, \lambda_t, X_t : t\ \in N\}$

General form:

$$\log(\lambda_t) = \beta_0 + \sum_{k=1}^{p} \beta_k \log(Y_{t-k} + 1) + \sum_{j=1}^{q} \alpha_j \log\left(\lambda_{t-j}\right) + \ \eta^T X_{t-1}$$

Specific form with p=q=1

$$\boxed{\log(\lambda_t) = \beta_0 + \ \beta_1 \log(Y_{t-1} + 1) + \alpha_1 \log(\lambda_{t-1}) + \ \eta^T X_{t-1}}$$

Distributions

Distributional assumption **Negative Binomial**

$$Y_t|F_{t-1} \sim NB(\lambda_t, \phi)$$

with $P(Y_t|F_{t-1} = n) = p_n^Y = \frac{\Gamma(\phi+n)}{\Gamma(n+1)\Gamma(\phi)} \left(\frac{\phi}{\phi+\lambda_t}\right)^{\phi} \left(\frac{\lambda_t}{\phi+\lambda_t}\right)^{n}, n = 0,1, \ldots$

Distributional Assumption **Poisson**

$$Y_t|F_{t-1} \sim Poiss(\lambda_t\ )$$

Zero-Inflated INGARCH models

Distributional Assumption **0-I Negative binomial** (*our own specification*)

$$Y_t|F_{t-1} \sim 0I - NB(\lambda_t, \phi, r)$$

with $P(Y_t|F_{t-1} = n) = \tilde{p}_n^Y = \begin{cases} (1-r) + r\left(\frac{\phi}{\phi+\lambda_t}\right)^{\phi} & \text{if } n = 0 \\ r\, p_n^Y & \text{if } n > 0 \end{cases}$

$$\widetilde{Y}_t \sim NB(\lambda_t, \phi)$$

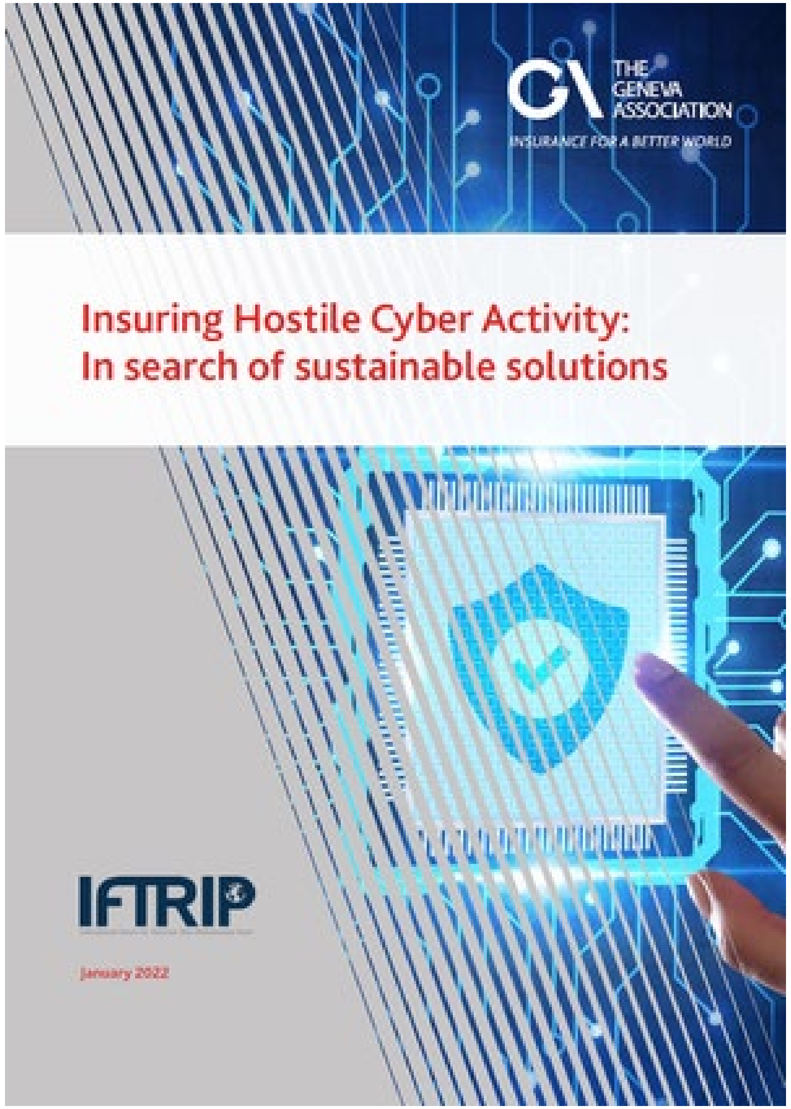
Y_t observed data breaches
$\widetilde{Y}_t$ occurred data breaches

$$Y_t = I_t \widetilde{Y}_t$$

$$I_t \sim Bern\ (r) \begin{cases} I_t = 1 & data\ breaches\ detected\ and\ reported \\ I_t = 0 & data\ breaches\ not\ detected\ or\ not\ reported \end{cases}$$

In search of sustainable solutions

Insurance typically involves a **delicate balance** between supply and demand.
Re/insurers need to set coverage conditions and charge **sufficient premiums** to cover the costs of providing risk protection, including compensating the providers of their capital for potential unexpected losses.
At the same time, there needs to be demand for such cover on those terms. Risks are only **insurable in practice** if an insurer and an insurance buyer reach an **agreement** about a specific coverage and its price, including a common understanding of what is insured and what is not. For this reason insurance can only deal with a limited band of the full spectrum of risk.



THE GENEVA ASSOCIATION
INSURANCE FOR A BETTER WORLD

Insuring Hostile Cyber Activity:
In search of sustainable solutions

IFTRIP

January 2022

Parametric Insurance

Parametric Coverage **simple and flexible**: if simple conditions are met [if the information commissioner has to be notified of the data breach - the GDPR legislation requires notification within 72 hours - that notification can be used for the assessment of the claim]

Providing **immediate payout** without the need to wait for loss-adjustment, designed to eliminate coverage gaps often found in other offerings, a parametric coverage offers broad parametric coverage with the following customer benefits: clear triggers, flexible limits, quick payout, affordable premiums

As a **first responder** for small and medium size entities the cover defends against cashflow shortages and reduced revenue immediately following a cyber event.

“Parametric” Insurance

A possible **insurance payout** could be based on a standard indemnity per lost or stolen record, whose value decreases as the size of the number increases in order to mitigate moral hazards

$$I = f(i_N | x, Tr, Ex) = x \times f(x) = \begin{cases} 1 \quad if\ i_N \leq Tr \\ \dfrac{i_N - Tr}{Ex - Tr} \quad if\ Tr < i_N \leq Ex \\ 0 \quad if\ i_N \geq Ex \end{cases}$$

if N	indem
< 10,000	$ 165.00
10,000-25,000	$ 131.47
25,001-50000	$ 79.54
> 50,000	$ 54.56

figure 8 Average total cost of a breach by number of records lost (mln$)

#records	2019	2018	2017	2016	average
< 10,000	2.20	2.10	1.90	2.10	2.08
10,000-25,000	3.30	3.00	2.80	3.00	3.03
25,001-50,000	4.70	4.40	4.60	6.30	5.00
> 50,000	6.40	5.70	6.30	6.70	6.28

“Parametric” Insurance

Case A

if N	indem
< 10,000	$ 165.00
10,000-25,000	$ 165.00
25,001-50000	$ 165.00
> 50,000	$ 165.00

Mean	Devst	MIN	MAX	Var99.5%	ES99.5%
€ 1,517,108	€ 383,963	€ 709,846	€ 6,681,873	€ 3,491,097	€ 4,468,927
	25.31%			*230%*	*295%*

Case B

if N	indem
< 10,000	$ 165.00
10,000-25,000	$ 131.47
25,001-50000	$ 79.54
> 50,000	$ 54.56

Mean	Devst	MIN	MAX	Var99.5%	ES99.5%
€ 655,883	€ 130,487	€ 359,246	€ 2,342,271	€ 1,305,110	€ 1,636,666
	19.89%			*199%*	*250%*

-56.77%

Case C

Index per month

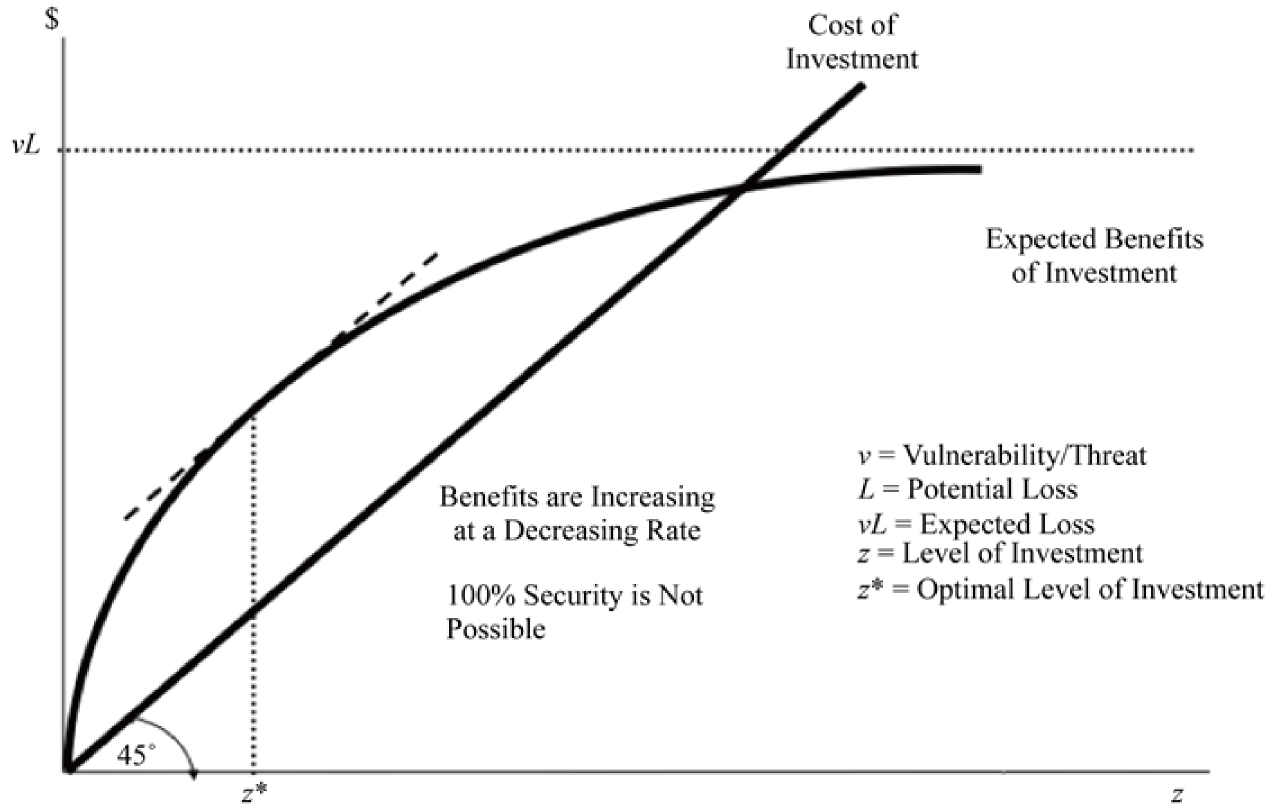
Mean	Devst	MIN	MAX	Var99.5%	ES99.5%
€ 517,455	€ 43,299	€ 354,915	€ 665,156	€ 615,633	€ 625,786
	8.37%			*119.0%*	*121%*

-65.89%

Demand’s view

One approach for deriving an organization's optimal level of cybersecurity investment, which has received a significant amount of attention in the academic and practitioner literature, is referred to as the **Gordon-Loeb Model** [*Gordon, 2002 the original article*].

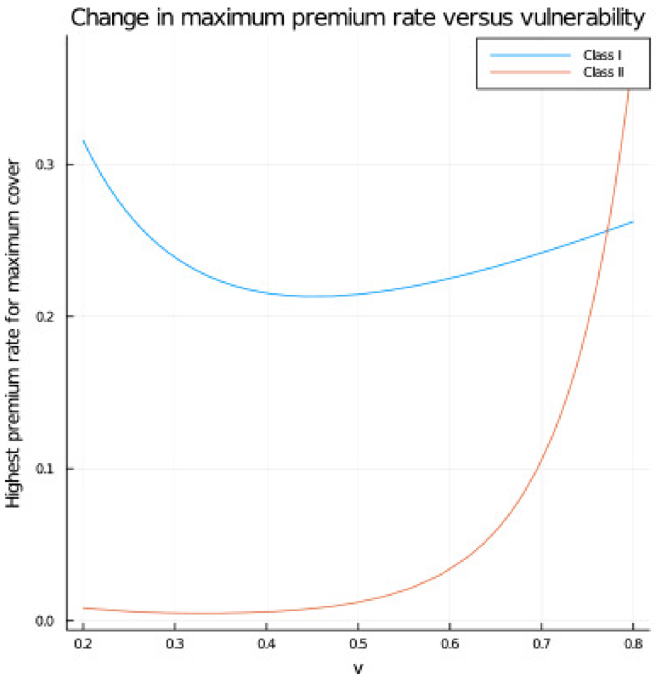
From the model we can gather that the amount of money a company spends in protecting information should, in most cases, be only a small fraction of the predicted loss.



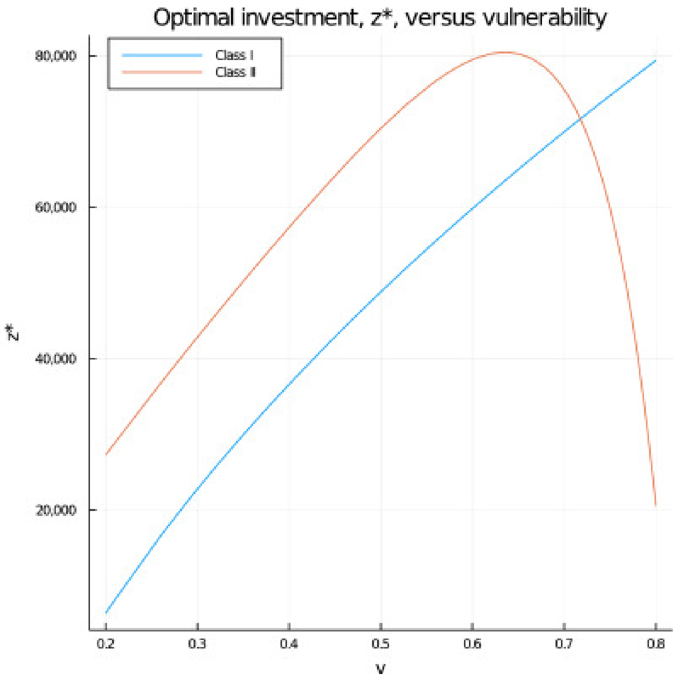
Adapted from [1] (Figure 1, p. 445)

Demand’s view

Skeoch (2022) demonstrates that the Gordon-Loeb model for investment in information security can be used to build a model for cyber-insurance based on maximizing the expected utility of an insurance buyer.



Change in maximum premium rate versus vulnerability



Optimal investment, z*, versus vulnerability

The model suggests that when the Gordon-Loeb recommended optimum is invested in security measures, then **utility is maximised** at full coverage for reasonable insurance premium rates subject to a cash constraint that the total spent on security measures and insurance cannot exceed the maximum amount stipulated by the Gordon-Loeb model.

Thank you

Marco Pirra
marco.pirra@unical.it

Feedbacks appreciated, thank you for the attention!

Acknowledgements AFIR-ERM Research Grant

IAA AAI AFIR-ERM Finance, Investment & ERM