Cyber Risk Management Strategies

Marco PIRRA, Italy

About the speaker

- **Marco Pirra** – *Assistant Professor, Università della Calabria*
  Assistant Professor, 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.

- Università della Calabria
  Department of Economics, Statistics and Finance

UNIVERSITÀ DELLA CALABRIA
DIPARTIMENTO DI **ECONOMIA, STATISTICA E FINANZA**
"Giovanni Anania"

Agenda

- ✓ Introduction
- ✓ Methodology
- ✓ Results
- ✓ Conclusions

Cyber risk

https://www.thecroforum.org/

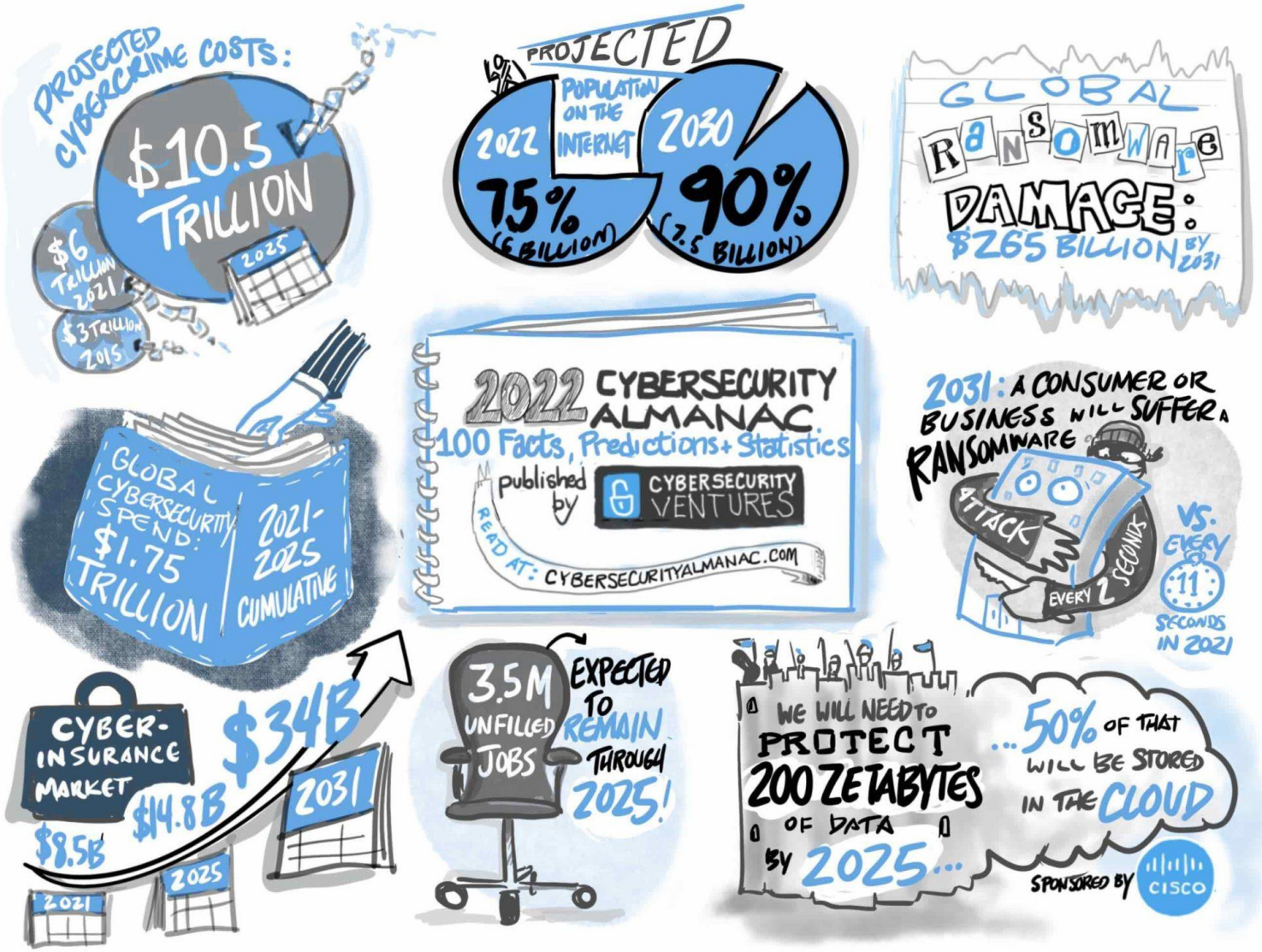
There is **no standardised definition** of the term “cyber risk.”

The CRO Forum has broadly described “cyber risk” to mean: “*Any risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks*.

It also encompasses physical damage that can be caused by cybersecurity incidents, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity and confidentiality of electronic information – be it related to individuals, companies or governments.”

The cost of Cybercrime [*Cybersecurity Ventures*]

If it were measured as a country, then cybercrime — which is predicted to inflict damages totaling **$8 trillion USD** globally in 2023 — would be the world's third-largest economy after the U.S. and China.



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, including exit scams, rug pulls, and theft will cost the world $30 billion USD in 2025 alone, nearly twice the $17.5 billion USD lost in 2021.
The **cyberinsurance market will grow** to $14.8 billion USD in 2025 and will exceed $34 billion USD by 2031, based on a compound annual growth rate (CAGR) of 15 percent calculated over an 11-year period (2020 to 2031).

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

Annual Cost of a Data Breach Study 2022 [Ponemon]

2022 Cost of a Data Breach Study: Global Overview

Benchmark research sponsored by IBM Security

Independently conducted by Ponemon Institute LLC

The global average total cost of a data breach increased by USD 0.11 million to USD 4.35 million in 2022, the **highest** it's been in the history of the report.

The increase from USD 4.24 million in the 2021 report to USD 4.35 million in the 2022 report represents a 2.6% increase.

In the last two years, the average total cost has increased **12.7%** from USD 3.86 million in the 2020 report.

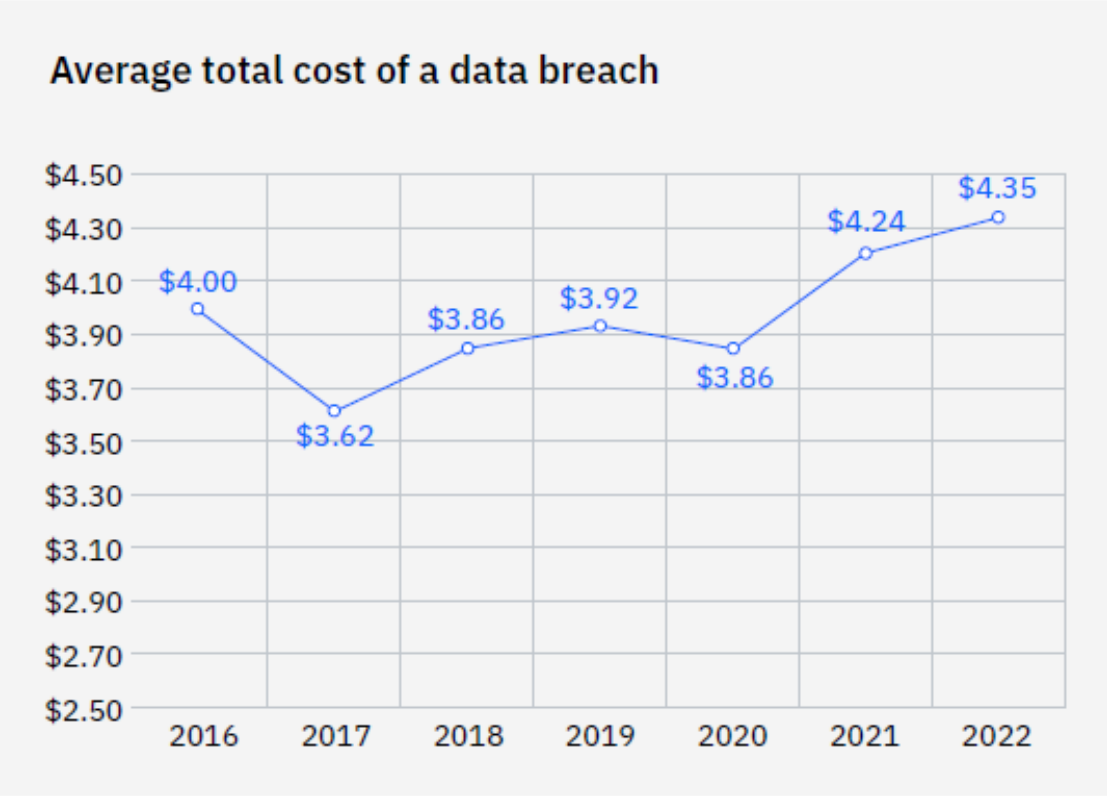


Figure 1: Measured in USD millions

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

Now in its 17th 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.

Annual Cost of a Data Breach Study 2022 [Ponemon]

Figure 2: **The per record cost of a data breach hit a seven-year high**.

The global per record cost of a data breach in 2022 was **USD 164**, a 1.9% increase from USD 161 in 2021.

The increase from USD 146 in 2020 is an increase of 12.3%.

The study examines 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.

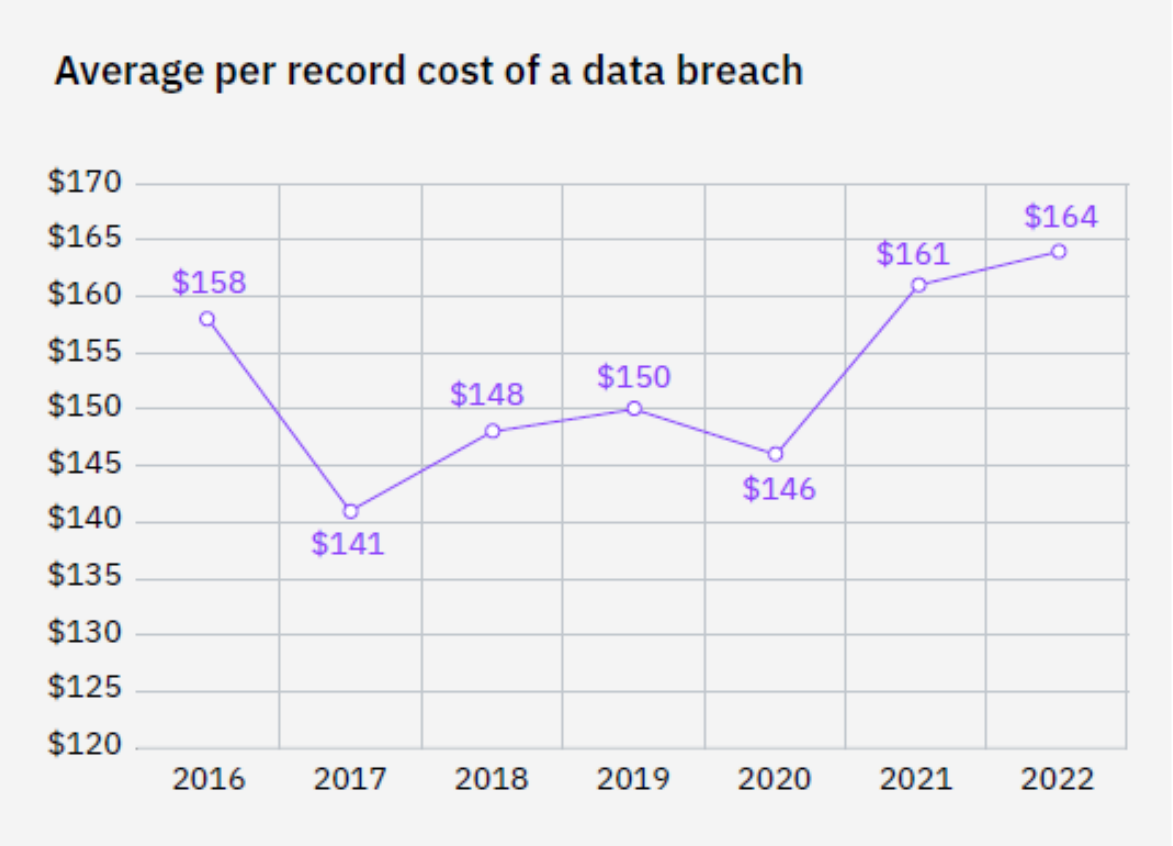


Figure 2: Measured in USD

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

Annual Cost of a Data Breach Study 2022 [Ponemon]

Figure 4: **Healthcare was highest cost industry for the 12th year in a row**. The average total cost of a breach in healthcare increased from USD 9.23 million in the 2021 report to USD 10.10 million in 2022, an increase of USD 0.87 million or 9.4%. *Healthcare is one of the more highly regulated industries and is considered critical infrastructure by the US government.*

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

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

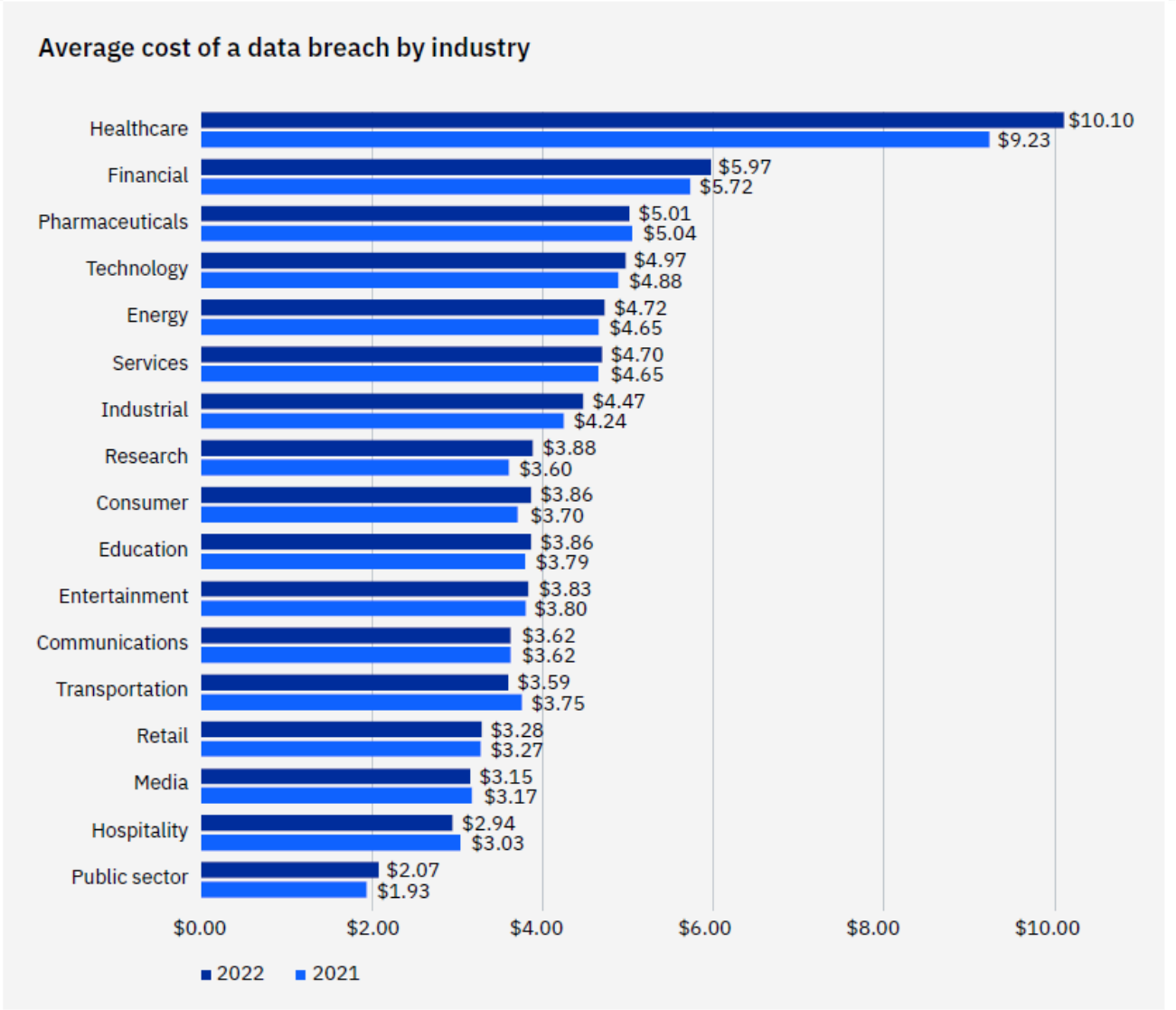


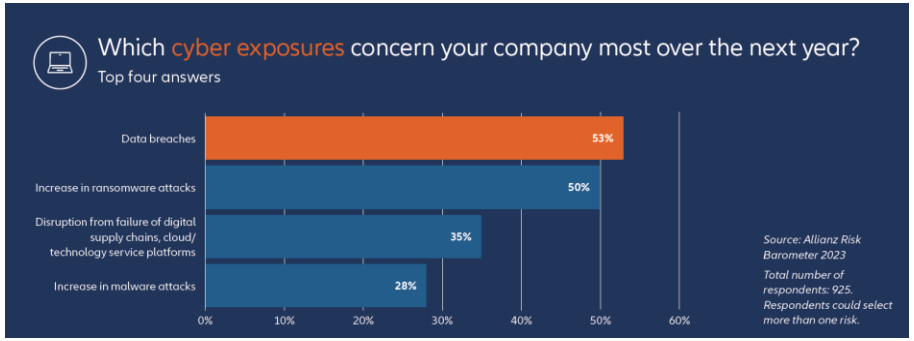
Figure 4: Measured in USD millions

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.

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.



"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

IAIS - International Association of Insurance Supervisors

ISSUES PAPER ON CYBER RISK
TO THE INSURANCE SECTOR (2016)

INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS

Concern over **cybersecurity is growing across all sectors of the global economy**, as cyber risks have grown and cyber criminals have become increasingly sophisticated. For **insurers, cybersecurity incidents can harm the ability to conduct business, compromise the protection of commercial and personal data, and undermine confidence in the sector**. The IAIS has noted that the level of awareness of cyber threats and cybersecurity within the insurance sector, as well as supervisory approaches to combat the risks, appear to vary across jurisdictions.

These factors prompted the IAIS to consider the area of cybersecurity in the insurance sector, **including the involvement of insurance supervisors in assessing and promoting the mitigation of cyber risk**. While many of the most widely publicised cybersecurity incidents involving consumer data have affected retailers, companies in the financial services sector, including insurers, have been victimised as well.

https://www.iaisweb.org/activities-topics/cyber-risk/

IAIS - International Association of Insurance Supervisors

All insurers, regardless of size, complexity, or lines of business, **collect, store, and share with various third-parties** (e.g., service providers, reinsurers) **substantial amounts of private and confidential policyholder information**, including in some instances sensitive health-related information.

Information obtained from insurers through cyber crime may be used for financial gain through extortion, identity theft, misappropriation of intellectual property, or other criminal activities. Exposure of private data can potentially result in severe and lingering harm for the affected policyholders, as well as reputational damage to insurer sector participants.

https://www.iaisweb.org/activities-topics/cyber-risk/

IAIS - International Association of Insurance Supervisors

The objectives of the Issues Paper are to **raise awareness** for **insurers and supervisors of the challenges presented by cyber risk**, including current and contemplated supervisory approaches for addressing these risks. As an Issues Paper, it provides background, describes current practices, identifies examples, and explores related regulatory and supervisory issues and challenges.

The Issues Paper focuses on **cyber risk to the insurance sector and the mitigation of such risks**, but does not cover IT security risks more broadly. It also does not specifically address insurers' underwriting of cyber risk (i.e., cyber insurance) or risks arising from cybersecurity incidents involving supervisors.

https://www.iaisweb.org/activities-topics/cyber-risk/

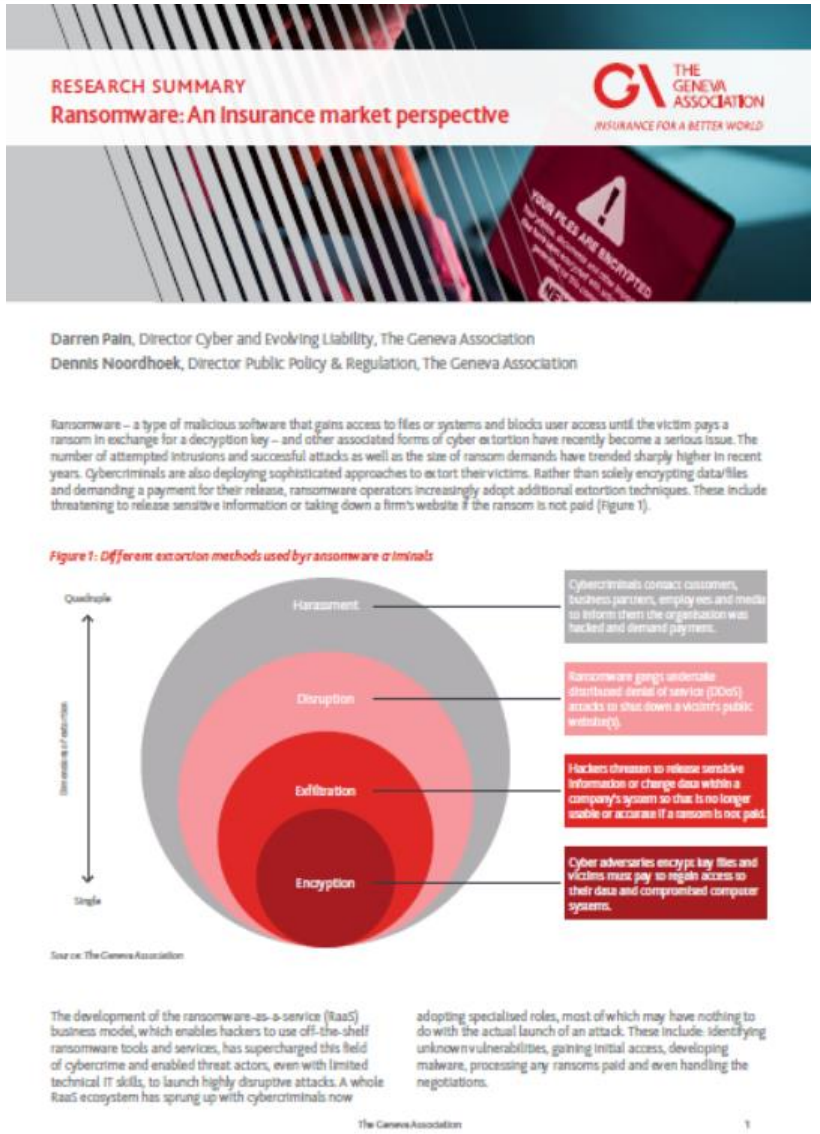
Ransomware: An insurance market perspective

As a form of cyber extortion, **ransomware** is malicious software that gains access to files or systems and blocks user access until the victim pays a ransom in exchange for a decryption key.

It has become a serious issue as the number of attempted intrusions and successful attacks as well as the size of ransom demands have **trended sharply higher** in recent years, contributing to the **deterioration** in cyber insurers' underwriting performance

Cybercriminals are deploying sophisticated approaches to extort their victims, including threats to release sensitive information or take down a firm's website if the ransom is not paid. The development of the ransomware-as-a-service (RaaS) business model has supercharged this field of cybercrime and enabled threat actors, even with limited technical IT skills, to launch highly disruptive attacks.

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



RESEARCH SUMMARY

Ransomware: An Insurance market perspective

THE GENEVA ASSOCIATION

INSURANCE FOR A BETTER WORLD

Darren Pain, Director Cyber and Evolving Liability, The Geneva Association

Dennis Noordhoek, Director Public Policy & Regulation, The Geneva Association

Ransomware – a type of malicious software that gains access to files or systems and blocks user access until the victim pays a ransom in exchange for a decryption key – and other associated forms of cyber extortion have recently become a serious issue. The number of attempted intrusions and successful attacks as well as the size of ransom demands have trended sharply higher in recent years. Cybercriminals are also deploying sophisticated approaches to extort their victims. Rather than solely encrypting data/files and demanding a payment for their release, ransomware operators increasingly adopt additional extortion techniques. These include threatening to release sensitive information or taking down a firm's website if the ransom is not paid (Figure 1).

Figure 1: Different extortion methods used by ransomware criminals

Source: The Geneva Association

The development of the ransomware-as-a-service (RaaS) business model, which enables hackers to use off-the-shelf ransomware tools and services, has supercharged this field of cybercrime and enabled threat actors, even with limited technical IT skills, to launch highly disruptive attacks. A whole RaaS ecosystem has sprung up with cybercriminals now adopting specialised roles, most of which may have nothing to do with the actual launch of an attack. These include: identifying unknown vulnerabilities, gaining initial access, developing malware, processing any ransoms paid and even handling the negotiations.

Ransomware: An insurance market perspective

Alongside governments, private **re/insurers have an important part** to play in the battle against ransomware, both offensively and defensively.

Re/insurers have an incentive to root out cybercrime that generates claims and **hits** their **underwriting profits**. Increased reporting of incidents and the swift exchange of actionable information will improve the authorities' abilities to accurately assess threats and effectively respond to them.

There are already close connections between the industry and global law enforcement, with threat intelligence shared and data gathered, so ways to **improve the efficiency** of that exchange should be explored.

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

Ransomware: 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.

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 (2020). 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: 5,498,398,893
from 9,015 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	454	149,183,184
2008	355	113,782,100
2009	272	13,577,270
2010	807	127,964,458
2011	793	144,922,047
2012	893	39,612,107
2013	865	126,507,104
2014	880	36,315,524
2015	548	245,887,500
2016	820	3,704,473,303
2017	688	307,801,937
2018	950	363,376,181
2019	72	1,314,188

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	0.17%
DISC	1861	20.64%	428,153,880	7.79%
HACK	2533	28.10%	4,682,499,697	85.16%
INSD	606	6.72%	66,580,428	1.21%
PHYS	1733	19.22%	39,748,401	0.72%
PORT	1172	13.00%	109,650,895	1.99%
STAT	249	2.76%	16,235,932	0.30%
UNKN	793	8.80%	146,326,624	2.66%

Entity	Events	%	Records	%
BSF	787	8.73%	394,813,919	7.18%
BSO	1045	11.59%	4,207,170,575	76.52%
BSR	623	6.91%	422,161,417	7.68%
EDU	848	9.41%	65,572,197	1.19%
GOV	781	8.66%	151,483,420	2.76%
MED	4343	48.18%	238,095,808	4.33%
NGO	119	1.32%	8,444,531	0.15%
UNKN	469	5.20%	10,657,026	0.19%

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 $X_t = \left(X_{t,1}, \ldots, X_{t,r}\right)^T$

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:

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

Specific form with p=q=1

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

Distributions

Distributional assumption **Negative Binomial**

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

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

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*)

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

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

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

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

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

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

Explicative Variables

A data breach occurs when a cybercriminal successfully infiltrates a data source and extracts sensitive information.

Hackers search for these **data** because they can be used to **make money**

As part of their strategy, the attackers hold the information for ransom and demand a payment in order to have the data removed from the host website.
The motive of a cybercriminal defines what company he/she will attack. Different sources yield different information.

Criminal organizations now are treating this like a **business** “They’re going to plan, they’re going to make sure they understand how they’re going to execute and then they’re going to set out and see where they can execute.”

Bitcoins: Why do we care? What is the relationship with data breaches?

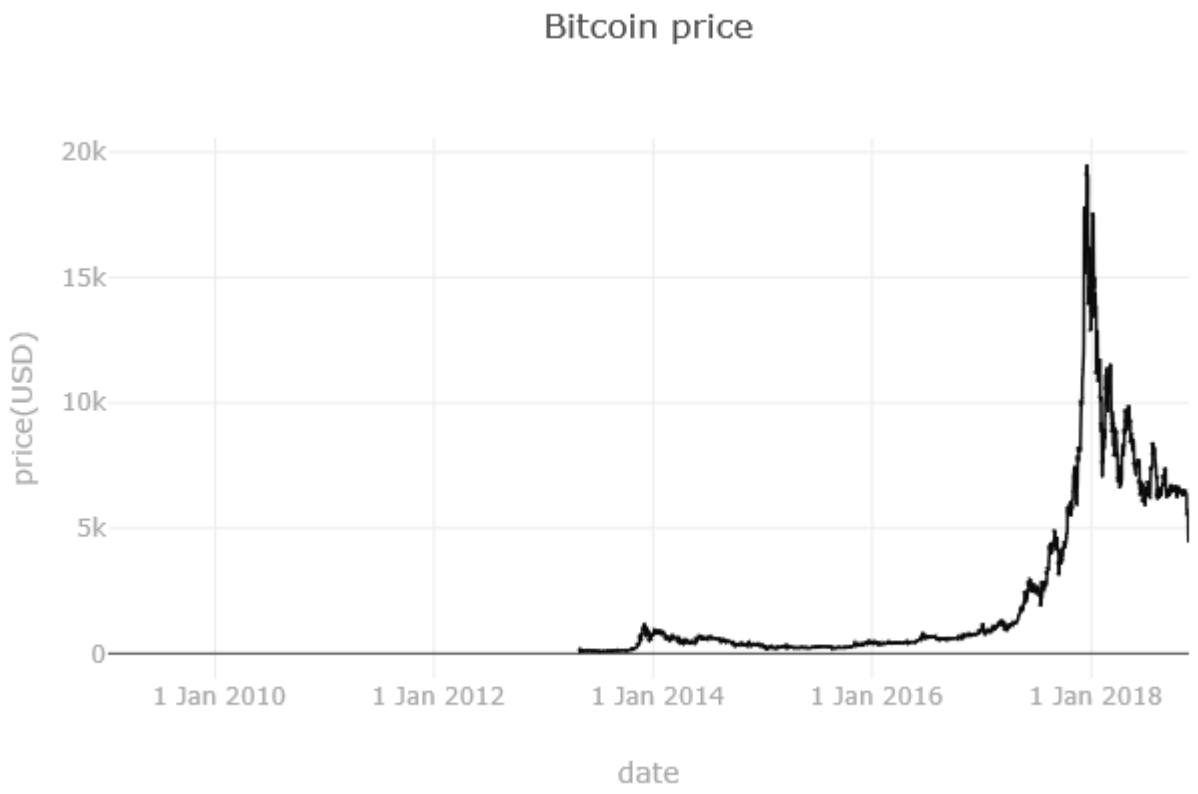
BitCoins

Bitcoin is a **digital payment currency** that utilizes cryptocurrency (a digital medium of exchange) and peer-to-peer (P2P) technology to create and manage monetary transactions as opposed to a central authority. The open source Bitcoin P2P network creates the bitcoins and manages all the bitcoin transactions.
Often referred to as "cash for the Internet," Bitcoin is one of several popular digital payment currencies along with Litecoin, Peercoin and Namecoin.

Bitcoin is considered the **biggest cryptocurrency**. It was first introduced in 2009 and is the most widely-traded cryptocurrency.

Bitcoin as an implementation of the cryptocurrency concept was described by Wei Dai in 1998 on the cypherpunks mailing list. Dai suggested a new form of money that uses cryptography to control its creation and transactions, rather than a central authority. In 2009, the Bitcoin specification and proof of concept was published in a cryptography mailing list by Satoshi Nakamoto. As noted in the Official Bitcoin FAQ, Satoshi Nakamoto left the project in late 2010 without revealing much about himself.

BitCoins [source datahub.io]



Field Name
date
txVolume(USD)
adjustedTxVolume(USD)
txCount
marketcap(USD)
price(USD)
exchangeVolume(USD)
generatedCoins
fees
activeAddresses
averageDifficulty
paymentCount
medianTxValue(USD)
medianFee
blockSize
blockCount

txCount - refers to the number of transactions happening on the public blockchain a day. Be aware that for low-fee blockchains, it's really easy to fabricate a whole bunch of transactions.

generatedCoins - refers to the number of new coins that have been brought into existence on that day. Actual number of newly-minted coins.

Results Database PRC

Table 2 Johansen's Cointegration Tests for the PRC dataset.

		$\hat{\lambda}_{\text{trace}}$		$\hat{\lambda}_{\text{max}}$	
Rank	Eigenvalue	Statistics	p-value	Statistics	p-value
0	0.128	507.110	0.000	277.010	0.000
1	0.106	230.100	0.000	227.630	0.000
2	0.001	24.695	0.116	24.695	0.116

Table 3 Vector Error-Correction estimation. PRC dataset[a]

	ΔP_t		ΔC_t		$\Delta\lambda_t^{PRC}$	
	Statistics	p-value	Statistics	p-value	Statistics	p-value
Intercept	0.055	0.749	-1.018	0.009	201.072	0.000
ΔP_{t-1}	-0.092	0.120	-0.440	0.001	0.236	0.564
ΔP_{t-2}	-0.107	0.052	-0.302	0.015	0.263	0.491
ΔP_{t-3}	-0.112	0.027	-0.190	0.095	0.218	0.535
ΔP_{t-4}	-0.084	0.065	-0.127	0.210	0.114	0.716
ΔP_{t-5}	-0.028	0.472	0.002	0.979	-0.069	0.799
ΔP_{t-6}	0.032	0.305	0.062	0.378	0.053	0.807
ΔP_{t-7}	0.011	0.613	0.041	0.406	0.079	0.608
ΔC_{t-1}	0.027	0.007	-0.420	0.000	-0.158	0.021
ΔC_{t-2}	0.017	0.100	-0.444	0.000	0.195	0.008
ΔC_{t-3}	0.005	0.613	-0.429	0.000	0.263	0.000
ΔC_{t-4}	0.024	0.030	-0.359	0.000	0.135	0.076
ΔC_{t-5}	0.014	0.180	-0.438	0.000	0.198	0.007
ΔC_{t-6}	0.016	0.134	-0.188	0.000	0.063	0.395
ΔC_{t-7}	0.014	0.148	0.163	0.000	-0.326	0.000
$\Delta\lambda_{t-1}^{PRC}$	0.005	0.689	-0.078	0.007	**0.626**	**0.000**
$\Delta\lambda_{t-2}^{PRC}$	0.005	0.671	-0.077	0.004	**-0.180**	**0.029**
$\Delta\lambda_{t-3}^{PRC}$	0.005	0.654	-0.073	0.002	-0.135	0.066
$\Delta\lambda_{t-4}^{PRC}$	0.006	0.525	-0.067	0.001	-0.063	0.320
$\Delta\lambda_{t-5}^{PRC}$	0.006	0.438	-0.029	0.074	-0.087	0.085
$\Delta\lambda_{t-6}^{PRC}$	0.004	0.347	-0.025	0.014	-0.013	0.668
$\Delta\lambda_{t-7}^{PRC}$	0.003	0.390	-0.005	0.496	-0.009	0.694
$\Psi^{PRC,1}$	-0.915	0.000	0.617	0.000	-0.194	0.655
$\Psi^{PRC,2}$	0.001	0.000	-0.002	0.000	0.029	0.000

[a] Additional details about the estimation are provided in Appendix A.
[b] Cointegrating vectors: $\beta_1 = (1, 0, -0.08233)$, $\beta_2 = (0, 1, -55.434)$; Adjustment vectors: $\alpha_1 = (-0.91548, 0.61663, -0.19402)$, $\alpha_2 = (0.00146, -0.002388, 0.02903)$.

Almost all the lagged variables ΔC have a strong negative impact on the lagged conditional expectations of data breaches today, as one may observe from the value and the highly significance of the regression coefficients.

This suggests that the **number of transactions** in Bitcoin might be a good predictor for data breaches.

The intuition behind this result is that hackers prepare themselves to monetize the data attack (either by selling the data or by extorting money to the legitimate data proprietor) some days before, by operating on the Bitcoin market.

Results Database PRC

Since both the logarithm of the number of transaction and the logarithm of conditional expectations of data breaches enter the second cointegrating vector, we highlight that the **short-run** impact found is **likely to persist** in the long time.

Our conjecture about the intuition behind this **long-term link** between transactions in Bitcoin and data breaches is as follows: on the one hand, once the hackers have monetized the breach, they posses a bunch of Bitcoins that will later be used in some different context.

On the other hand, a remunerative data breach creates **incentives** to prepare more cyber attacks, which in turn create the needs of more transactions in Bitcoin.

We also find high statistical significance of both cointegrating variables in the equation for the change in Bitcoin prices. This signals that although in the long-run, the effects between Bitcoin metrics and conditional expectations of data breach will impact also on Bitcoin returns.

Results Database BLI

Table 4 Johansen's Cointegration Tests for BLI dataset.

		$\hat{\lambda}_{\text{trace}}$		$\hat{\lambda}_{\text{max}}$	
Rank	Eigenvalue	Statistics	p-value	Statistics	p-value
0	0.110	392.760	0.000	235.540	0.000
1	0.074	157.220	0.000	154.930	0.000
2	0.001	22.898	0.130	22.898	0.130

Table 5 Vector Error-Correction estimation. BLI dataset[a]

	ΔP_t		ΔC_t		$\Delta\lambda_t^{BLI}$	
	Statistics	p-value	Statistics	p-value	Statistics	p-value
Intercept	0.056	0.725	-0.291	0.422	129.025	0.000
ΔP_{t-1}	-0.097	0.101	-0.475	0.000	-0.048	0.898
ΔP_{t-2}	-0.110	0.047	-0.338	0.007	0.100	0.777
ΔP_{t-3}	-0.115	0.024	-0.226	0.049	0.242	0.453
ΔP_{t-4}	-0.084	0.063	-0.164	0.110	0.140	0.627
ΔP_{t-5}	-0.027	0.496	-0.017	0.847	0.106	0.670
ΔP_{t-6}	0.034	0.279	0.056	0.430	-0.041	0.838
ΔP_{t-7}	0.012	0.588	0.042	0.404	-0.010	0.943
ΔC_{t-1}	0.027	0.005	-0.417	0.000	-0.224	0.000
ΔC_{t-2}	0.016	0.120	-0.450	0.000	-0.162	0.016
ΔC_{t-3}	0.002	0.886	-0.431	0.000	-0.063	0.344
ΔC_{t-4}	0.021	0.056	-0.355	0.000	-0.068	0.326
ΔC_{t-5}	0.012	0.246	-0.455	0.000	0.016	0.812
ΔC_{t-6}	0.013	0.203	-0.212	0.000	0.177	0.008
ΔC_{t-7}	0.013	0.181	0.160	0.000	0.075	0.234
$\Delta\lambda_{t-1}^{BLI}$	0.003	0.820	-0.013	0.609	**-0.649**	**0.000**
$\Delta\lambda_{t-2}^{BLI}$	-0.004	0.693	-0.007	0.781	**-0.506**	**0.000**
$\Delta\lambda_{t-3}^{BLI}$	-0.008	0.415	-0.007	0.751	**-0.355**	**0.000**
$\Delta\lambda_{t-4}^{BLI}$	-0.008	0.393	-0.009	0.677	**-0.241**	**0.000**
$\Delta\lambda_{t-5}^{BLI}$	-0.010	0.238	-0.021	0.261	**-0.181**	**0.001**
$\Delta\lambda_{t-6}^{BLI}$	-0.011	0.102	-0.033	0.026	**-0.123**	**0.003**
$\Delta\lambda_{t-7}^{BLI}$	-0.004	0.215	-0.024	0.003	-0.043	0.056
$\Psi^{BLI,1}$	-0.910	0.000	0.646	0.000	0.173	0.665
$\Psi^{BLI,2}$	0.001	0.000	-0.001	0.000	0.002	0.000

[a] Additional details about the estimation are provided in Appendix.
[b] Cointegrating vectors: $\beta_1 = (1, 0, -0.524)$, $\beta_2 = (0, 1, -354.95)$; Adjustment vectors: $\alpha_1 = (-0.91, 0.646, 0.173)$, $\alpha_2 = (0.00136, -0.001016, 0.0024)$.

The **cointegration** analysis of the BLI dataset fully confirms the existence of a strong, **statistically significant**, **link** between data breaches and number of transactions in Bitcoin, both in the short-run and in the long-run.

The results confirm the intuition provided in the previous section for which **data breaches have a statistical effect** in the number of transactions in Bitcoin.

The analysis also confirms the lack of a significant short-term relation between data breaches and price of Bitcoin.

Impulse Response Analysis

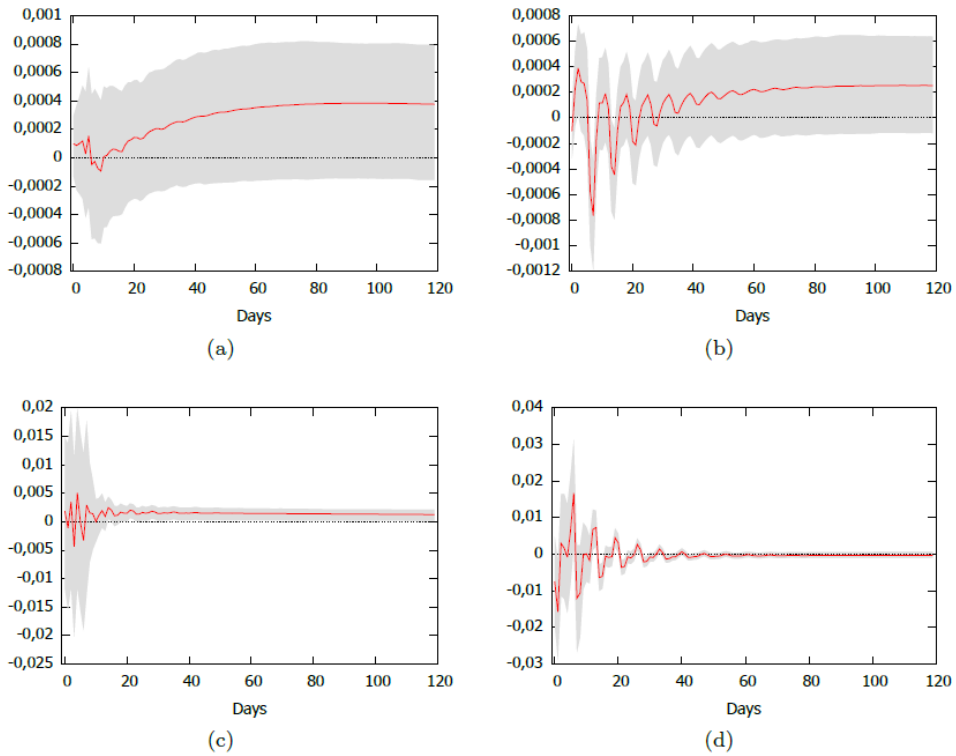


Fig. 3 Impulse response point estimates and 95% confidence bands. Panel (*a*): Shock variable P_t, response variable λ_t^{PRC}. Panel (*b*): Shock variable C_t, response variable λ_t^{PRC}. Panel (*c*): Shock variable P_t, response variable λ_t^{BLI}. Panel (*d*): Shock variable C_t, response variable λ_t^{BLI}.

For both datasets, the **impulse response** estimates associated to the daily number of transactions variable crosses the zero axis more often than the ones associated to the Bitcoin's price do.

More specifically, Panels (a) and (b) refer to changes of PRC data breaches while panels (c) and (d) refer to changes of BLI data breaches due to shocks of Bitcoin-related variables.

We note that the logarithm of the **number of transactions in Bitcoins has a relevant impact** on the future data breaches in both datasets. The size of the response is significantly di fferent from zero and the phenomenon continues to persist in the long run.

Comments

We uncover the strong, **bidirectional**, **relation** between **data breaches** and **Bitcoin-related** variables.

Our analysis suggests that in the short-run the lagged values of the number of transactions in Bitcoin has a strong negative impact on data-breaches today. In the long-run, the existence of a cointegrating vector including all variables under investigation implies that the short-run relation will persist in the long run.

Moreover, we find almost identical results on **two different datasets**, confirming the **robustness** of our result.
The impulse response analyses highlight the **relevant quantitative impact** of both the number of transactions and the Bitcoin price on future data breaches, while the variance decomposition of the forecasting errors suggests that the same variable can explain up to 5% of the variability.

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.

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

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

if N	paym
< 10,000	$ 164.00
10,000-25,000	$ 130.68
25,001-50,000	$ 79.06
> 50,000	$ 54.23

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	valore
< 10,000	$ 164.00
10,000-25,000	$ 164.00
25,001-50000	$ 164.00
> 50,000	$ 164.00

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	valore
< 10,000	$ 164.00
10,000-25,000	$ 130.68
25,001-50000	$ 79.06
> 50,000	$ 54.23

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

<u>Index per month</u>

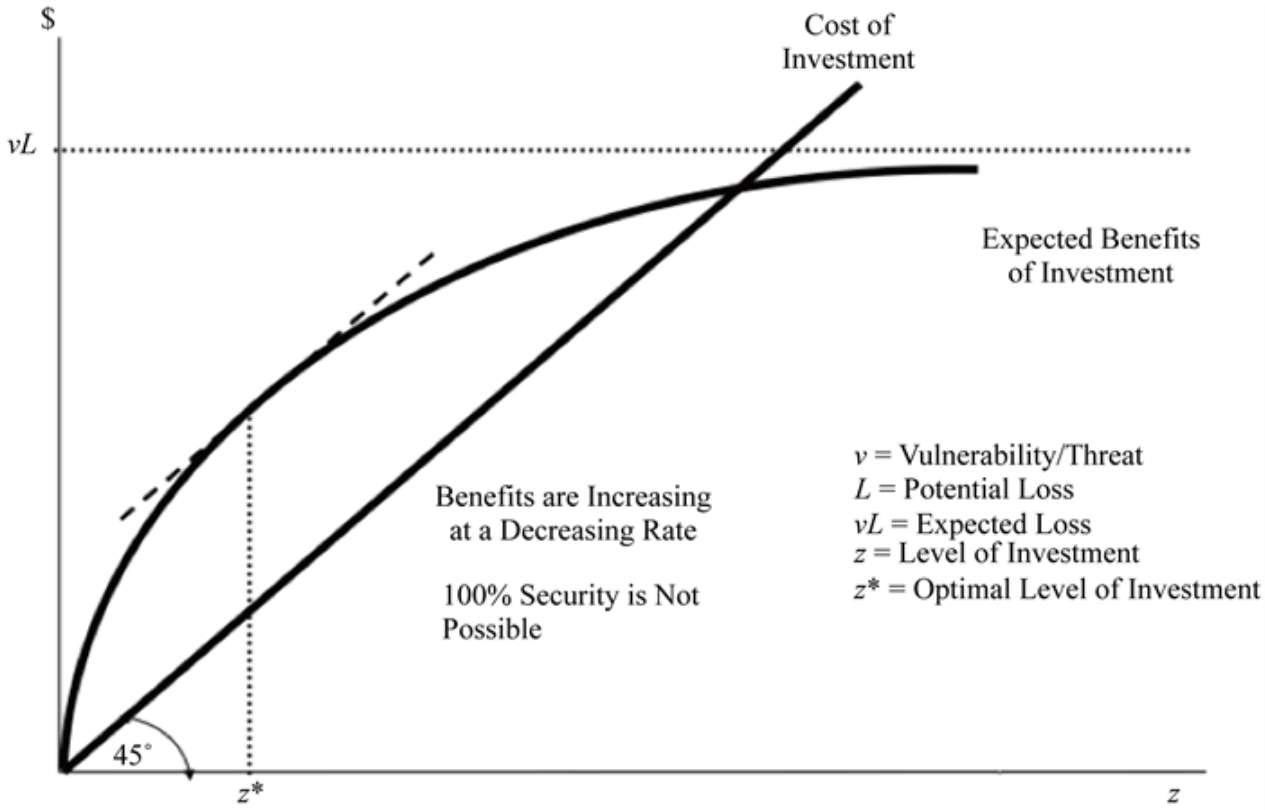
Mean	Devst	MIN	MAX	Var99.5%	ES99.5%
€ 517,455	€ 43,299	€ 354,915	€ 665,156	€ 615,633	€ 625,786
	8.37%			*119.0%*	*121%*

-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*].

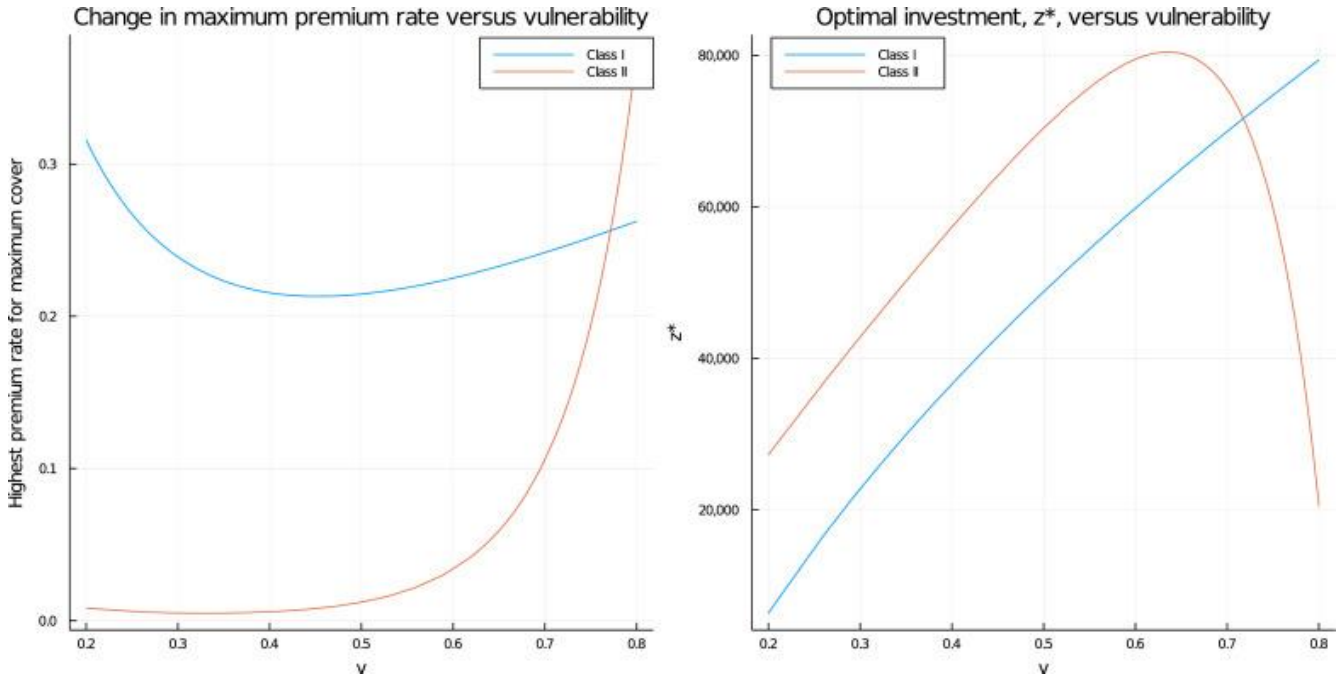
From the model we can gather that the amount of money a company spends in protecting information should, in most cases, be only a small fraction of the predicted loss



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.



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@unical.it

Acknowledgements AFIR-ERM Research Grant