CYBER RISK MANAGEMENT AND SOLVENCY ASSESSMENT

Advanced wider fields: a challange for Actuaries

Salvatore Forte

21 september 2022

AGENDA

- CYBER RISK E RISK BASED SUPERVISION
- AIM OF THE WORK
- THE DATA UNDERLYING THE STUDY
- THE ACTUARIAL MODEL
- CYBER RISK PRICING
- CYBER RISK CAPITAL ADD-ON
- COMMENTS
- MAIN REFERENCES

ISOA

CYBER RISK E RISK-BASED SUPERVISION

Numerous initiatives on the subject of cyber risk by bodies and supervisory authorities from 2016 to today:

G7

IOSCO Cyber Task Force

Financial Stability Institute

Basel Committee on Banking Supervision's Operational Resilience Working Group

International Association of Insurance Supervisors

European Supervisory Authorities (ESAs)

European Banking Authority (EBA)

European Insurance and Occupational Pensions Authority (EIOPA)

European Securities and Markets Authority (ESMA)

ECB Banking Supervision

European Systemic Risk Board (ESRB)

European Systemic Cyber Group (ESCG)

ISOA

AIM OF THE WORK

The main objective of this work:

- on the one hand, we want to determine the capital add-on that we would have in a pillar 1 perspective to also cover the cyber risk
- on the other hand, we want to price a policy to cover the cyber risk for the entire Italian insurance market.

ISOA

THE DATA UNDERLYING THE STUDY

Based on the data collected in the following paper, "Accenture, The cost of cyber crime, 2019", the following is shown:

- In Italy, 22 companies were analyzed in 2018, including insurance companies, the cost in terms of losses due to cyber risk is equal to 8.01 million dollars, an increase of 19% compared to the previous year 2017;
- Considering 19 types of industries, 355 companies, including 20 insurance companies, in 11 different countries, the total cost of cyber risk for the year 2018 was equal to 211.25 million dollars;
- Considering 20 insurance companies based in 11 countries including Italy, the cost of cyber risk in 2018 was equal to 15.76 million dollars, an increase of 22% compared to the previous year 2017. Therefore in 2018, the cost for the insurance sector was 7.46% for the 11 countries analyzed.

ISOA

THE DATA UNDERLYING THE STUDY

In order to estimate the losses due to cyber risk relating only to Italian companies, assuming that also in Italy the proportion of cost per cyber risk for the insurance sector alone is equal to 7.46% of the Italian total cost, we have a expected cost for cyber losses equal to **597,574 dollars** (assuming only 1 company in the sample).

- The revenue for this sector, or the premiums written for the life and non-life market in 2020, amounted to approximately 138.6 billion euros (Source: ANIA, Italian insurance 2020-2021).

- by 2020 an absolutely modest cost considering the revenue of the insurance sector

ISOA

THE DATA UNDERLYING THE STUDY – VOLATILITY ESTIMATION

Analysis of the work of Biener, Eling, Wirfs, **Insurability of cyber risk: an empirical analysis**, 2015, referring to 994 operational losses linked to cyber risks

Table 4 Losses per risk type (in million US$)

Category	N	Mean	Std. dev.	Min.	Quantiles			VaR	TVaR	Max.
					25%	50%	75%	(95%)	(95%)	
Panel A: Cyber versus non-cyber risk										
Cyber Risk	994	40.53	443.88	0.10	0.56	1.87	7.72	89.56	676.88	13,313
Non-Cyber Risk	21,081	99.65	1,160.17	0.10	1.88	6.20	25.37	248.97	1,595.27	89,143
Panel B: Cyber risk subcategories										
Actions of people	903	40.69	463.25	0.10	0.55	1.83	6.87	84.36	679.04	13,313
Systems and technical failure	37	29.07	77.33	0.10	1.10	5.03	11.65	168.95	329.04	370
Failed internal processes	41	47.72	205.92	0.14	0.42	2.04	9.05	158.65	743.40	1,311
External events	13	39.40	115.73	0.28	0.56	1.03	13.77	192.88	422.71	422

ISOA

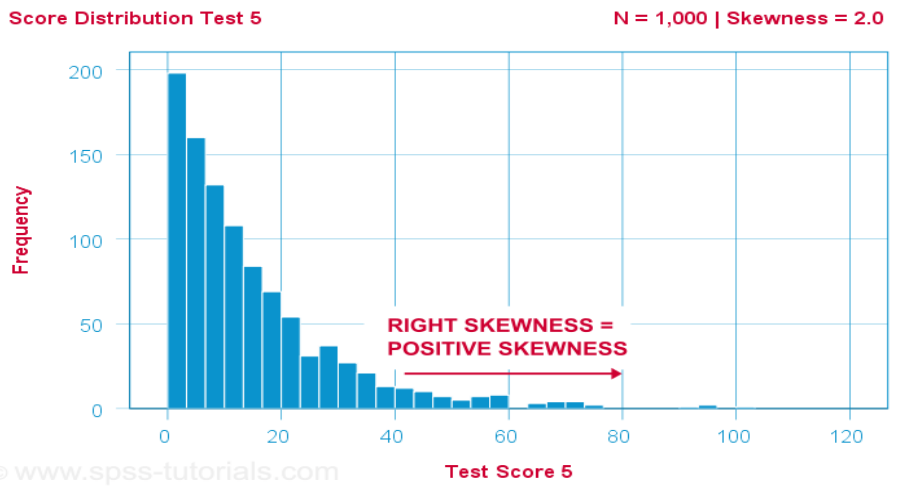
THE DATA UNDERLYING THE STUDY – THE SHAPE OF THE DISTRIBUTION

As we can see from the previous table, with reference to the 994 operating losses we can calculate the following ratios:

VaR (95%) / MEAN = 2.21

TVaR (95%) / MEAN = 16.70

Very material positive asymmetry with an extremely heavy right tail



ISOA

THE DATA UNDERLYING THE STUDY – THE RISKS CATEGORIES

About the cyber risk categories, on the basis of the paper "Accenture, The cost of cyber crime, 2019" we considerthe following six sources of risk and the respective average annual cost (in dollars):

Cyber risks	Average annual cost in %	Average annual cost
Phishing and Ransomware	15,7%	94.047
Web Attacks	30,6%	183.057
Malicious insider	12,4%	74.256
Malware and Botnets	23,0%	137.635
Stolen devices	7,5%	44.605
Malicious code	10,7%	63.974
Total	**100,0%**	**597.574**

ISOA

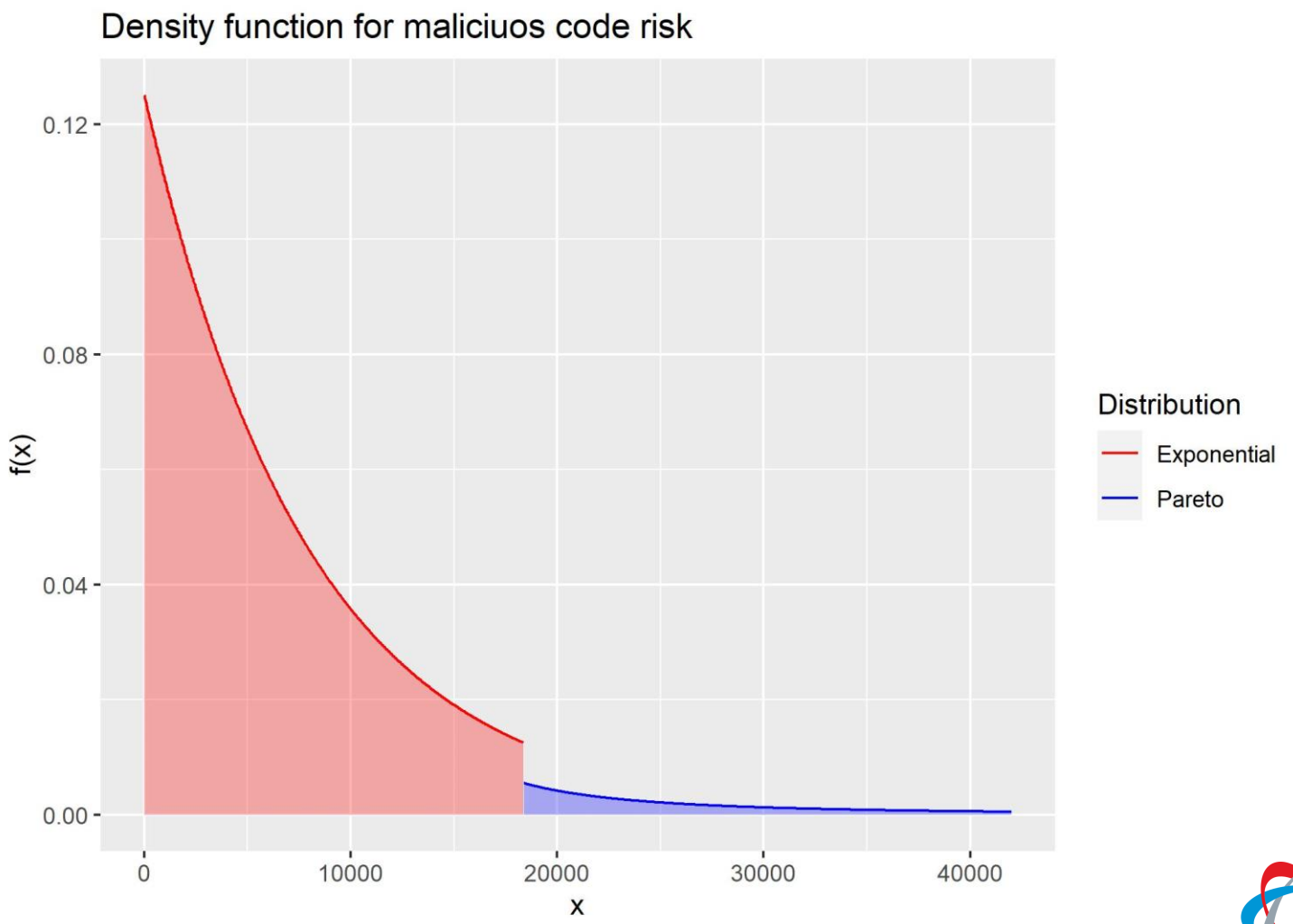
THE ACTUARIAL MODEL FOR THE QUANTIFICATION OF CYBER RISK

In order to model the aggregate distribution for the six risks we use the following probabilistic model:

- In order to model the probability distribution of a single cyber risk i with i=1,..,6 we consider the following EVT model:
  - An exponential distribution with one parameter to model up to 90-th percentile;
  - A Pareto generalized distribution with three parameters to model the right tail from the 90-th percentile onward.
- The parameters of the six marginal distributions were estimated considering the following three empirical statistics:
  - The average cost per single risk as shown in the table on the previous slide
  - VaR (95%) / MEAN = 2.21 constant for all six risks considered
  - TVaR (95%) / MEAN = 16.70 constant for all six risks considered
- In order to model the aggregate distribution we use a Normal Copula and a Vine Copula

ISOA

THE ACTUARIAL MODEL FOR THE QUANTIFICATION OF CYBER RISK – THE MARGINNAL DISTRIBUTIONS



ISOA

THE ACTUARIAL MODEL FOR THE QUANTIFICATION OF CYBER RISK – THE MARGINNAL DISTRIBUTIONS

The parameters of the six marginal distributions were estimated considering the following three empirical statistics:

- The average cost per single risk
- VaR (95%) / MEAN = 2.21
- TVaR (95%) / MEAN = 16.70

CYBER RISKS	Exponential parameter	Generalized Pareto parameters		
	Λ	μ	β	ξ
Phishing and Ransomware	0,0851	50	7,1	0,95
Web Attacks	0,0437	30	19,6	0,95
Malicious insider	0,1077	6	6,1	0,95
Malware and Botnets	0,0581	24	15,1	0,95
Stolen devices	0,1794	24	4,6	0,95
Malicious code	0,1251	14	6,6	0,95

ISOA

THE ACTUARIAL MODEL FOR THE QUANTIFICATION OF CYBER RISK – THE AGGREGATE DISTRIBUTION

With regard to the parameters of the copula, i.e. the linear correlation coefficients between the pairs of risks, considering the aggregate database available it was not possible to estimate these parameters and therefore a sensitivity analysis of the VaR and TVarR risk measures was carried out changing linear correlation level.

We proceeded with the simulation of a pseudo-data set considering a normal copula with a linear correlation matrix composed of linear correlation coefficients all equal to 0.25 or 0.5 or 0.75.

In this way, 100 sestines have been simulated for the respective three correlation levels, 0.25, 0.5 and 0.75, which represent in our model our hypothetical 100 insurance companies that have communicated the 6 cyber losses all in the same year suffered.

ISOA

THE AGGREGATE DISTRIBUTION

Considering these three matrices 100x6, the algorithms present in the R-packages **Copula** and **VineCopula** were applied to estimate the parameters of the copulas:

- Normal

- Vine

Obtaining as output data with corr = 0.25:

	Phishing and Ransomware	Web Attacks	Malicious insider	Malware and Botnets	Stolen devices	Malicious code
Phishing and Ransomware	1	0,33	0,33	0,28	0,22	0,27
Web Attacks	0,33	1	0,12	0,23	0,18	0,32
Malicious insider	0,33	0,12	1	0,08	0,08	0,17
Malware and Botnets	0,28	0,23	0,08	1	0,34	0,34
Stolen devices	0,22	0,18	0,08	0,34	1	0,22
Malicious code	0,27	0,32	0,17	0,34	0,22	1

ISOA

THE AGGREGATE DISTRIBUTION

Considering these three matrices 100x6, the algorithms present in the R-packages **Copula** and **VineCopula** were applied to estimate the parameters of the copulas:

- Normal

- Vine

Obtaining as output data with corr = 0.5:

	Phishing and Ransomware	Web Attacks	Malicious insider	Malware and Botnets	Stolen devices	Malicious code
Phishing and Ransomware	1	0,51	0,53	0,62	0,57	0,65
Web Attacks	0,51	1	0,47	0,54	0,40	0,50
Malicious insider	0,53	0,47	1	0,53	0,41	0,56
Malware and Botnets	0,62	0,54	0,53	1	0,48	0,56
Stolen devices	0,57	0,40	0,41	0,48	1	0,60
Malicious code	0,65	0,50	0,56	0,56	0,60	1

ISOA

THE AGGREGATE DISTRIBUTION

Considering these three matrices 100x6, the algorithms present in the R-packages **Copula** and **VineCopula** were applied to estimate the parameters of the copulas:

- Normal

- Vine

Obtaining as output data with corr = 0.75:

	Phishing and Ransomware	Web Attacks	Malicious insider	Malware and Botnets	Stolen devices	Malicious code
Phishing and Ransomware	1	0,73	0,71	0,68	0,70	0,73
Web Attacks	0,73	1	0,79	0,65	0,70	0,69
Malicious insider	0,71	0,79	1	0,69	0,73	0,66
Malware and Botnets	0,68	0,65	0,69	1	0,77	0,73
Stolen devices	0,70	0,70	0,73	0,77	1	0,65
Malicious code	0,73	0,69	0,66	0,73	0,65	1

ISOA

THE AGGREGATE DISTRIBUTION

Once the parameters for both the three normal copulas and the three vine copulas were obtained, we proceeded with the simulation of the aggregate distribution using the R packages (copula and VineCopula) obtaining the simulated joint distribution.

It is specified that in order to estimate the joint probability distributions, we proceeded with the simulation for each copula of 100,000 realizations and this algorithm was repeated 100 times.

At the end of this procedure, both the VaR (99.5%) and the TVaR (99.5%) were calculated respectively for each copula and for each correlation level. This level of probability was chosen in order to quantify the solvency requirements for the cyber risk.

ISOA

PRICING OF CYBER RISK

In order to quantify the price of a potential insurance coverage that can cover the cyber risk for an insurance company, we proceeded as follows:

A. The equivalnce premium is equal to the sum of the six expected losses for the six risks modelled

B. The safety loading was assessed using the cost of capital approach assuming a cost of capital rate of 6% with a solvency ratio target equal to 200%.

C. The expenses loading has been calculated considering only the management costs with an expenses ratio equal to 25%

It should be noted that in order to proceed with the estimate referred to in point B, the capital requirement was calculated from a Pillar 1 perspective with the VaR and from a Pillar 2 perspective, considering a consistent risk measure, with the TVaR at a probability level of 99.5 % of the distribution of multivariate aggregate losses.

TVaR is preferred over VaR:

- for its sub-additivity property
- better captures the risk in the tail of the highly asymmetrical distribution and therefore suitable for appropriately representing catastrophic damage associated with cyber risks.

ISOA

PRICING RESULTS AND COMMENTS

Considering that there are 163 insurance companies in the Italian market, assuming a potential pool of insurers with appropriate reinsurance assignments, the overall premium for the Italian market would be:

- Considering a VaR risk measure in order to calculate the solvency capital requirement and consequently the safety loading: between **379 million and 405 million euros**, or between approximately **0.27% and 0.29% of the total premiums written in 2020** equal to approximately 138.6 billion euros;

- Considering a TVaR risk measure in order to calculate the solvency capital requirement and the consequently the safety loading: between **1,469 million and 1,674 million euros**, or between approximately **1.05% and 1.19% of the total premiums written in 2020**;

ISOA

CAPITAL ADD-ON RESULTS AND COMMENT

Considering the solvency data of the Italian market at 31.12.2020:

- SCR: 58 billion euros
- Own Founds: 140 billion euros
- Solvency ratio: **241%**

Based on our calculations for the Italian market as a whole, this capital add-on would be between 1.5 and 1.6 billion euros and therefore we would have the following market Solvency ratio:

- SCR including cyber risk (prudent) approximately 60 billion euros
- Own Founds of approximately 140 billion euros (constant)
- Solvency ratio of approximately **234%**

In conclusion, also considering the capital requirement for cyber risks would lead to:

- a **reduction of the market solvency ratio of 7.3%**
- an **increase** of the capital requirement equal to **1.3% of the written premiums**

ISOA

CAPITAL ADD-ON RESULTS AND COMMENT

Given that the probability distributions representing the six marginal distributions and the joint multivariate distribution have extremely heavy tails, in order to asses the capital requirement if we used a risk measure capable of capturing this aspect, for instance the TVaR(99.5%,) there would be a significant capital increase.

- From an SCR including cyber risk approximately **60 billion euros** with VaR (99.5%) to an SCR approximately **66 billion euros** with TVaR (99.5%).
- Consequently, a reduction in Italian market solvency ratio from **7.3%** with VaR (99.5%) to **29.3%** with TVaR (99.5%).

ISOA

MAIN REFERENCES

- Accenture, 2019, **The cost of cyber crime** - https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf
- ANIA, 2021, **L'assicurazione Italiana 2020-2021** - https://www.ania.it/documents/35135/126701/L%27Assicurazione+Italiana+2020-2021.pdf/e4fa652e-dda7-8c9c-96ef-1e4468d4f903?version=1.0&t=1626333153413
- Biener C., Eling M., Wirfs J. H., 2015, **Insurability of cyber risk: an empirical analysis**, Geneva Papers on Risk and Insurance, Issues and Practice 40, 131–158 - https://www.alexandria.unisg.ch/238242/1/Insurability%20of%20Cyber%20Risk%20An%20Empirical%20Analysis.pdf
- Carannante M., D'Amato V., Fersini P., Forte S., Melisi G., **Vine Copula modelling dependence among cyber risks: a dangerous regulatory paradox**, 2022 (Under review)
- D'Amato V., Fersini P., Forte S., Melisi G., 2020, **The effect of Disruption in Insurance Industry: Cyber Risk Evaluation**, Actuarial Colloquium Paris - https://www.actuview.com/video/The-Effect-of-Disruption-in-Insurance-Industry-Instant-Policy-Pricing-and-Cyber-Risk-Evaluation/694e0b7cb

THANK YOU VERY MUCH!

Salvatore Forte

21 september 2022