Received: 29 July 2022 | Revised: 15 February 2023 | Accepted: 18 April 2023

DOI: 10.1002/asmb.2767

RESEARCH ARTICLE

WILEY

Vine copula modeling dependence among cyber risks: A dangerous regulatory paradox

Maria Carannante[1] | **Valeria D'Amato**[1] | **Paola Fersini**[2] | **Salvatore Forte**[3] | **Giuseppe Melisi**[4]

[1]Department of Pharmacy, University of Salerno, Fisciano, Italy

[2]Department of Business and Management, Luiss Guido Carli University, Rome, Italy

[3]Faculty of Law, Giustino Fortunato University, Benevento, Italy

[4]Department of Law, Economics, Management and Quantitative Methods, University of Sannio, Benevento, Italy

Correspondence
Maria Carannante, Department of Pharmacy, University of Salerno, Fisciano, Italy.
Email: mcarannante@unisa.it

Abstract

Dependence among different cyber risk classes is a fundamentally underexplored topic in the literature. However, disregarding the dependence structure in cyber risk management leads to inconsistent estimates of potential unintended losses. To bridge this gap, this article adopts a regulatory perspective to develop vine copulas to capture dependence. In quantifying the solvency capital requirement gradient for cyber risk measurement according to Solvency II, a dangerous paradox emerges: an insurance company does not tend to provide cyber risk hedging products as they are excessively expensive and would require huge premiums that it would not be possible to find policyholders.

KEYWORDS

cyber risk, solvency capital requirements, vine copula

1 | INTRODUCTION

The National Institute of Standards and Technology (NIST) defines cyber risk as "risk of financial loss, operational disruption, or damage, from the failure of the digital technologies employed for informational and/or operational functions introduced to a manufacturing system via electronic means from the unauthorized access, use, disclosure, disruption, modification, or destruction of the manufacturing system."[1]

Cyber risk is often treated as an information technology problem based on vulnerabilities in computer software and network topologies (e.g., computers, routers, switches, storage devices), typically nodes of an ICT network. Generally, the cascading effects of an organization's internal dependencies are investigated through cyber impact propagation modeling. The literature on cyber risk presents an interesting variety of network models for modeling dependence between different nodes representing the states of network components and edges as transitions among different states.[2-7] Some authors adopt the beta-binomial and one-factor latent risk model to model the internal correlation among cyber risks.[8] Reference 9 formalize the specific properties of cyber risks, such as interdependent security, correlated risk, and information asymmetries. The Bayesian network approach analyses the cyber risk propagation dynamics using the multivariate Gaussian copula.[10] Reference 11 also use the copula tool to model dependence among cyber attacks, stressing the inconsistency of evaluations when disregarding dependence among cyber attack events. In Reference 12, the dependence among high-dimensional risks is analysed using the vine copula, also highlighting that ignoring the dependence structure can lead to a severe underestimation of losses. To study cross-breach-type and cross-industry risks, Reference 13 implemented a vine copula to model various dependence structures. In Reference 14, the Gumbel copula captures the positive nonlinear dependence between frequency and severity. Nevertheless, besides Reference 15, to the best of our knowledge,

no study focuses on the dependence inherent in cyber risk classes and the explicit financial consequences of ignoring dependence. Compared to Reference 16 highlighting the severe underestimation of cyber loss and the insurance contract premiums by implementing the L-hop propagation model developed in Reference 15, we develop a cyber risk pricing setting and we study the effects of the dependence structure among cyber risks on insurance company solvency in terms of the regulatory perspective of the solvency capital requirements (henceforth SCR) and the capital add-on, on the basis of vine copulas methodology. In particular, unbiased pricing for cyber risk evaluates the cost of capital and considers the distributions' tails for determining VaR and TVaR. In our research, we unveil a paradox for which insurance companies should offer huge premiums to avoid liquidity problems, making cyber insurance products out of the market unless they apply many limitation clauses.

The remainder of the article is structured as follows. Section 2 illustrates pair vine copulas, particularly stressing their features. Section 3 develops the vine copula setting for quoting cyber policies and the impact of the dependence structure among different cyber risks. Section 4 presents the main outcomes of the empirical applications, and Section 5 concludes.

2 | PAIR VINE COPULAS

The copulas represent a convenient tool for modeling the dependence of the random variables separately from the marginal distributions.[17] Copulas are general dependence models and have been used for representing two types of dependence, either cross-sectional or serial. In particular, in many areas, the high-dimensional dependence structures are analysed by multivariate Gaussian copulas. Nevertheless, they fail to capture various tail dependences, they cannot account for features such as asymmetry, being more restrictive than flexible multivariate distributions such as Regular vine (R-vine) copulas, also called pair-copula constructions (PCC). R-vine copula address exactly this high-dimensional probabilistic modeling problem, instead of using an N-dimensional copula directly, by decomposing the probability density into conditional probabilities, and further decomposing conditional probabilities into bivariate copulas. Reference 18 introduced the construction of a multivariate copula by using conditional bivariate copulas. A more general construction method for multivariate densities has been provided by Bedford et al.[19] by developing R-vine to arrange different pair copula constructions. The vine copulas take advantage properly of the rich variety of bivariate copulas as building blocks. The flexibility of the method relies on the multiplicity of the different pair copulas that may be mixed in a vine copula, matching any possible dependence structure. These graphical models consisting of a nested sequence of trees are built on a d-dimensional dependence structure from two-dimensional building blocks, called pair-copulas. Each edge is associated with a pair-copula, and each pair-copula encodes the conditional dependence between a pair of variables. The canonical vine (C-vine) and the drawable vine (D-vine) copulas consist in special subclasses of the R-vine copulas, the inference of the two special cases, where the former exhibits star shaped structures having a tree sequence and the latter a path structure, being developed by Aas et al.[20] As stressed in Reference 21, the C-vines are indicated to best-fit data sets that have a dominant variable, whereas D-vines are suitable in the case of the variables exercising the most influence over the rest through large correlation values.[21,22] In particular, D-vines can be suggested when we pose no assumption on the existence of a keynote that governs the dependencies. Broadly speaking, the C-vine applies to fitting a multi-variable with a key variable that controls interactions in the data, while the D-vine is appropriate, especially when variables are relatively independent.

3 | VINE COPULA SETUP

3.1 | Vine copula for different cyber risk categories

To estimate different types of cyber risks affecting insurance company activities, we model the corresponding aggregate loss distribution, namely, the sum of individual losses in an annual time horizon. In other words, we model the multivariate dependence of different categories of cyber risk. While Reference 8 describe the correlation between cyber security risks, Reference 23 proposes a copula-based actuarial model for pricing cyber security risks. The copula tool allows the effective modeling of high-dimensional dependence. Indeed, the vine copula first introduced in Reference 24 offers a great deal of flexibility in modeling dependence and accommodating diverse dependence structures between different pairs of variables.

Reference 25 provided one of the first studies on statistical methods for detecting cyber attacks using vine copulas. Reference 12 widely discuss the dependence between cyber security risks in a high-dimensionality setting. Nevertheless, in the actuarial literature, no regulatory perspective is adopted in managing cyber risks via the vine copula.

As in Nelsen,[26] copulas are functions that join or "couple" multivariate distribution functions to their one-dimensional marginal distribution functions, or multivariate distribution functions whose one-dimensional margins are uniform on the interval (0,1). For example, the multivariate distribution function

$$C\left(F_1\left(x_1\right),\ F_2\left(x_2\right),\ \ldots\ ,F_n\left(x_n\right)\right)=C\left(u_1,u_2,\ \ldots\ ,u_n\right). \tag{1}$$

With univariate distributions $F_i, i=1,2,\ \ldots\ n$, correspondent densities $f_i, i=1,2,\ \ldots\ n$ and uniformly distributed marginal distributions $u_i, i=1,2,\ \ldots\ n$. $c\left(u_1,u_2,\ \ldots\ ,u_n\right)$ represents the respective density function. According to Reference 17, any multivariate distribution function can be decomposed into its univariate marginal distributions and a copula function. A continuous three-dimensional density function can be decomposed in multiple ways. For instance

$$f\left(x_1,x_2,x_3\right)=f_1\left(x_1\right)\ f_2\left(x_2\right)f_3\left(x_3\right)c_{12}\left[F_1\left(x_1\right),\ F_2\left(x_2\right)\right]c_{13}\left[F_1\left(x_1\right),\ F_3\left(x_3\right)\right]c_{23|1}\left[F\left(x_2|x_1\right),\ F\left(x_3|x_1\right)\right], \tag{2}$$

where c describes the density of the copulas, and F describes the distribution. We can generalize with the following definition.

Definition 1. Let $(X_1,\ \ldots\ ,X_d)$ denote a vector of random variables and F is the correspondent joint distribution, letting $f_1,\ \ldots\ ,f_d$ the correspondent marginal density functions. According to Reference 21, a possible decomposition of $f\left(x_1,\ \ldots\ ,x_d\right)$ is represented by

$$f\left(x_1,\ \ldots\ ,x_d\right)=\prod_{j=1}^{d-1}\prod_{i=1}^{d-j}c\left[\left(i,i+j|i+1,\ \ldots\ ,i+j-1\right)\right]\prod_{k=1}^{d}f_k\left(x_k\right), \tag{3}$$

where $c\left(i,j|i_1,\ \ldots\ ,i_k\right)=c\left(i,j|i_1,\ \ldots\ ,i_k\right)\left[F\left(x_{i,}|x_{i1},\ \ldots\ ,x_{ik}\right),F\left(x_{j,}|x_{i1},\ \ldots\ ,x_{ik}\right)\right]$ with $i<j$ and $i_1<\cdots<i_k$

Based on such decompositions, References 19,24,27-30 introduced the concept of vine copulas recently adopted in the literature,[31,32] and applied in the context of financial data.[33-36]

The dependence relationship between different pairs of variables can be flexibly captured via vine copulas instead of the traditional approaches to modeling high-dimensional dependence restrictive in high-dimensionality settings.[12,37,38] Furthermore, in vine copulas, the computation in high-dimensionality settings can be efficiently handled, as shown, for example, in Reference 39.

Definition 2 (24). $V=(T_1,\ \ldots\ ,T_d)$ on d elements is called an R-vine if:

- T_1 is the first tree (level 1) with node set $N_1=\{1,\ \ldots\ ,d\}$ and edge set E_1;
- for $i=2,\ \ldots\ ,\ d-1$ the edge set E_{i-1} is the node set of tree T_i;
- (Proximity condition) for tree $T_i\ i=2,\ \ldots\ ,\ d-1$, if two nodes in E_{i-1} are connected by an edge in E_i, then these two nodes as edges in T_{i-1} share the same node in E_i.

Definition 3 (24). The properties of R-vines can be studied based on the following three sets

- The complete union set of $e_i\in E_i$ is defined as

$$U_{e_i}=\left\{d\in N_1\exists e_j\in\ E_j,j=1,\ \ldots\ ,i-1\text{ with }d\text{ in }e_1\in\ \ldots\ \in e_i\right\}\subset N_1.$$

  That is, the complete union of an edge is a set of all indices that this edge contains.

- For an edge $e_i=\{a,b\}\in E_i$ the conditioning set of edge e_iei is defined as $D_{e_i}=U_a\cap U_b$.
- For an edge e_i, the conditioned sets of e_i are defined as $C_{e_i,a}=U_a\setminus D_{e_i}$ and $C_{e_i,b}=U_b\setminus D_{e_i}$.

Let (F, V, B) denote a vine copula specification where $F = (F_1, \ldots, F_d)$ is a vector of continuous invertible marginal distribution functions, and $B = \{B_e | i = 1, \ldots, d-1; e \in E_i\}$ is a set of copulas with B_e being a pair-copula. There is a unique distribution that achieves this vine copula specification with density

$$f_{1\ldots d}(x) = \prod_{k=1}^{d} f_k(x_k) \prod_{i=1}^{d-1} \prod_{e \in E_i} c_{C_{e,a}, C_{e,b}|D_e} \left(F_{C_{e,a}|D_e} \left(\mathbf{x}_{C_{e,a}} | \mathbf{x}_{D_e} \right), F_{C_{e,b}|D_e} \left(\mathbf{x}_{C_{e,b}} | \mathbf{x}_{D_e} \right) \right), \tag{4}$$

where $\mathbf{x} = (x_1, \ldots, x_d)$, $e = \{a, b\}$, $x_{D_e} = \{x_i | i \in D_e\}$ and $c_{C_{e,a}, C_{e,b}|D_e}$ is the bivariate copula density for edge $e = \{a, b\}$.

According to Reference 20, we classify vine copulas into *C*-vine (star form) and *D*-vine (line form) copulas based on the structure of the graph.

Vine copulas are suitable for describing the dependence between variables using a series of bi-variate copulas, so-called pair copulas. Expressing the multivariate density function as the product between pair-copula and marginal densities, we can combine the advantages of multivariate copula due to the separation of the marginal distributions of the dependence structure and the flexibility of bivariate copulas. The inference of vine copulas consists of the best decomposition fitting the dependence data and the parameter estimation

$$\sum_{j=1}^{d-1} \sum_{i=1}^{d-j} \sum_{t=1}^{T} \log \left\{ c_{(j,j+1)} | 1, \ldots, j-1 \left[F\left(x_{j,t} | x_{1,t}, \ldots, x_{j-1,t}\right), F\left(x_{j+i,t} | x_{1,t}, \ldots, x_{j-1,t}\right) \right] \right\}. \tag{5}$$

3.2 | Insurance contract pricing

From an actuarial perspective, we can define the equivalence premium as the expected value of losses considering six cyber risks

$$E[Z]. \tag{6}$$

The pure premium is the sum of the equivalence premium and the safety loading

$$PP = E[Z] + \delta_k, \tag{7}$$

where δ_k is the safety loading by using the kth principle for the pure premium calculation.

The expenses-loaded premium is the sum of the pure premium and the expenses loading

$$EP = \frac{PP}{(1-\beta)}, \tag{8}$$

where β is the expenses loading percentage of the expenses-loaded premium. In the following numerical application, in line with the Italian market, we assume $\beta = 25\%$.

To evaluate the tariffs to cover the cyber risk, we adopt the cost of capital principle to for safety loading.

If ρ is the cost of the capital rate, assuming that the risk will expire after one year, the target solvency ratio is equal to 200% and $i_{rf}(0,1)$ is the risk-free rate between 0 and 1, then

$$\delta_{COC} = \frac{2\rho \cdot SCR}{\left(1 + i_{rf}(0,1)\right)} = \frac{2\rho \cdot \left[VaR_{99,5\%}(Z) - E[Z]\right]}{\left(1 + i_{rf}(0,1)\right)} \tag{9}$$

according to Solvency II to assess the solvency capital requirement (SCR) (Directive 2009/138/EC of the European Parliament).

In our numerical application, we used two different risk measures to quantify SCR and δ_{COC}: $\text{VaR}_{99,5\%}(Z)$ and $\text{TVaR}_{99,5\%}(Z)$ to consider the strong right asymmetry that typically occurs for cyber risk losses.[40]

4 | NUMERICAL APPLICATION

In this section, we used a simulation study to propose a framework to evaluate the opportunity for insurance companies to offer cyber risks hedging products. To obtain data, we start from the available aggregated data and generate random

TABLE 1 Operational losses for cyber risk.[40]

Category	N	Mean	Std. dev.	Min	Quantiles 25%	Quantiles 50%	Quantiles 75%	VaR (95%)	TVaR (95%)	Max
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	1160.17	0.10	1.88	6.20	25.37	1595.27	1595.27	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	13.31
Systems and technical failures	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	1311
	13	39.40	115.73	0.28	0.56	1.03	13.77	192.88	422.71	422

variables for each single risk. For simplicity, the relationships among risks are modeled using a linear correlation, through a Gaussian copula hypothesis. In this way, it is possible to perform an uncertainty analysis, as defined by Blanchet et al.,[41] defining a baseline model, that is, the definition of a hedging product neglecting the relationships among cyber risks and the positive asymmetry of distributions, and a metric to estimate the alternative model, that is, the vine copula, starting from the information related to the relationship between cyber risks defined by Biener et al.[40]

Simulated studies are used in the field of cyber risk. For instance, Reference 42 use automation software to simulate events to analyse the potential cyber risk in the manufacturing sector; Reference 43 published a report to show the advantages of the use of Monte Carlo simulation techniques to assess the investments in security in the IT sector; Reference 44 proposed a methodology based on simulated data to evaluate pre-event cyber security risk; Reference 45 provide an overview of the literature to assess the efforts of simulation studies on cyber security effectiveness; Reference 46 use an agent-based model to simulate the security of a computer network from cyber-attacks. The use of simulated analysis is also common in the evaluation of solvency capital requirements. For instance, Reference 47 proposes a simulation study to evaluate the compliance with the solvency capital requirement for non-life insurance risk; Reference 48 propose a nested simulated methodology, based on Markov-chain models, to estimate the compliance with the solvency capital requirements for the insurance companies in the European Union according to the Solvency II framework; Reference 49 proposes a Monte Carlo simulation procedure to evaluate the internal risk in the Solvency II framework.

4.1 | The underlying data

Between 2017 and 2018, the cyber risk losses in the Italian market increased by around 19% to $8.1 million, according to Accenture[1]. The report classifies 355 organizations, 20 of which are insurance companies, in 19 industries in 11 countries. Among the 20 insurance companies in the sample, the cyber risk cost in 2018 was $15.76 million, recording an increase of 22% concerning 2017. In other words, the insurance market cyber cost amounted to 7.46% of the total cyber risk cost, with an average cost of $597,574 referring to the single Italian insurance company.

Table 1 shows the operational losses due to cyber risk according to Reference 40 evaluated in terms of volatilities.

Starting from the values of Table 1, with reference to the 994 operational losses, it is possible to compute the following ratios relating to cyber risk.

- VaR(95%)/MEAN = 89.56/40.53 = 2.21.
- TVaR(95%)/MEAN = 676.88/40.53 = 16.70.

Based on these values, we can state that the empirical distribution of operational losses shows compelling positive asymmetry with a very heavy right tail. Table 2 shows the results.

[1]https://www.accenture.com/acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf, accessed on February 4, 2022.

TABLE 2 Parameters estimation of the six cyber risks distributions.

Cyber risk categories	Exponential parameters	Generalized 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 botnet	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

TABLE 3 Main source of cyber risk and relative average costs (Accenture 2019).

Cyber risk categories	Average annual costs (%)	Average annual costs ($)
Phishing and ransomware	15.7%	94,047
Web attacks	30.6%	183,057
Malicious insider	12.4%	74,256
Malware and botnet	23.0%	137,635
Stolen devices	7.5%	44,605
Malicious code	10.7%	63,974
Total	100.0%	597,574

Furthermore, relating to the type of cyber risk to the model, according to the Accenture report, we consider the six main sources of risk and relative average annual costs (in dollars) shown in Table 3:

4.2 | The probability model

To quantify the joint distribution of the six individual cyber risk categories, we propose the following probabilistic model

- To model the probability distribution associated with each cyber risk category with $i = 1, \dots, 6$ we consider the following EVT model.
  - A one-parameter exponential distribution to model up to the 90th percentile of the distribution.
  - A three-parameters generalized the Pareto distribution to model the right tail of the distribution, that is, from the 90th percentile onwards.
- To model the distribution of the aggregate cyber risk categories, we used a normal vine copula.

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

- The average costs for the individual risk, as shown in Table 3.
- VaR(95%)/MEAN = 2.21 assumed constant for all six risk categories considered.
- TVaR(95%)/MEAN = 16.70 assumed constant for all six risk categories considered.

Parameters of the selected distributions, exponential, and generalized Pareto, are estimated considering the following objective function

$$\begin{cases} VaR(95\%)/\mathbb{E}[Y] = 2.21 \\ TVaR(95\%)/\mathbb{E}[Y] = 16.70. \end{cases} \tag{10}$$

Since the lack of data about the individual loss distribution for each risk category, we assume that the empirical values are the same for all six risk categories, a hypothesis that is reflected in Reference 40.

Since the available aggregated database does not allow estimating the copula parameters, namely the linear correlation coefficients between risk pairs, we conduct a sensitivity analysis of the VaR and TVaR risk measures as the level of copula parameters and type of copula.

In particular, we simulate pseudo-data sets, considering a normal copula with a linear correlation matrix composed of linear correlation coefficients equal to 0.25 or 0.5 or 0.75. For this purpose, we simulate a fictional country-level market of 100 insurance companies, assuming that they have all experienced the six cyber risks in the same year, obtaining 100 sextuplets of losses for each correlation hypothesis. The number of companies chosen is consistent with that of a medium-sized country, given that in Italy there are 163 insurance companies. In this sense, even if real data were available, they would not be sufficient to guarantee consistent results. To ensure reliability without unrealistic assumptions about the insurance market size, we perform a sensitivity analysis relating to the type of copula and its parameters.

To correctly estimate copulas, we need that pseudo-random data respect the conditions of IID. In our case, we perform tests to verify if data fit a continuous standard uniform distribution, to verify if data respect randomness conditions and to verify the presence of patterns.[50,51] Table 4 shows the results.

Table 4 shows that pseudo-random data fit well a continuous standard uniform distribution and data sequence respects the randomness condition, with no patterns. For these reasons, we can consider our data equivalent to IID.

Considering the 100×6 matrices, we estimate the normal copula and vine copula. Tables 5–7 show the correlation matrices for the normal copula.

As can we observe in Tables 5–7, the results obtained from the simulations and related estimations of parameters show that the differences between the estimated parameters and the theoretical ones are material because the dimension of the sample (100) is reasonable by considering the market, being not robust from a statistical perspective where the differences should be very close to zero.

Figures 1–3 show the vine copula trees for the different levels of correlation. Figures show the estimation of different trees of vine copula model; each of them builds the couples considered to estimate correlations differently, as defined by Brechmann and Schepsmeier.[52] Assuming d variables, Tree 1 considers the single-variables couples $(1,2),(2,3),(3,4),\ \ldots\ ,(d-1,d)$, Tree 2 considers the correlations among couples composed of two variables on the left side and a single variable on the right side $(1,3|2),(2,4|3),\ \ldots\ ,(d-2,d|d-1)$, Tree 3 considers the correlations

TABLE 4 Randomness test for pseudo-random data.

Test	Statistics	DF	*p*-value
Non parametric chi-squared test for U[0,1] distribution	7.6	9	0.575
Asymptotic Kolmogorov-Smirnov test for U[0,1] distribution	0.074		0.644
Gap test for U[0,1] distribution	11	7	0.150
Rank von Neumann test for autocorrelation	1.793		0.230
Runs test for randomness	−0.905	50; 50	0.367
Poker TEST for randomness	8.8	9	0.460

TABLE 5 Correlation matrix for normal copula and linear correlation 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

TABLE 6 Correlation matrix for normal copula and linear correlation 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	0.4	0.5
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	0.4	0.41	0.48	1	0.6
Malicious code	0.65	0.5	0.56	0.56	0.6	1

TABLE 7 Correlation matrix for normal copula and linear correlation 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	0.7	0.73
Web attacks	0.73	1	0.79	0.65	0.7	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	0.7	0.7	0.73	0.77	1	0.65
Malicious code	0.73	0.69	0.66	0.73	0.65	1

among couples composed of two variables on both sides $(1, 4|2, 3)$, $(2, 5|3, 4)$, … $(d-3, d|d-2, d-1)$, last tree, Tree $d-1$, considers the correlations among a couple with the first and the last variable on the left side and the other variables on the right side $(1, d|2, \ldots, d-1)$. In our application, since we have six variables, we estimated five trees.

Figure 1 summarizes the parameters of the vine copula estimated starting from a sample simulated from a normal copula with a linear correlation coefficient of 0.25.

As shown in Figure 1, Tree 1 defines the following relationships: a Frank copula for the couple phishing and ransomware (1) and malicious insider (3) with parameter 1.98, suggesting a strong positive relationship of the central observations and week for tail observations; a 180° type 1 Rotated Twan copula for the couple web attacks (2) and phishing and ransomware (1), with parameters 1.71 and 0.39, suggesting a positive relationship of the lower extreme values of distribution; Gaussian copula for the couple malware and botnets (4) and stolen devices (5), with parameter 0.35, suggesting a positive linear correlation; survival Gumbel copula for the couple Malicious code (6) and web attacks (2), with parameter 1.28, suggesting a positive strong dependence of the lower tail observations; and Clayton copula for the couple malicious code (6) and malware and botnets (4), with parameter 0.57, suggesting a positive relationship of the lower tail observations.

Tree 2 defines the following relationships: a 270° type 1 Rotated Twan copula for the couple composed by the combination of web attacks (2) and malicious insider (3) and phishing and ransomware (1) with parameters −20 and 0.01, suggesting a negative weak relationship of the lower extreme values of distribution; a 180° type 2 Rotated Twan copula for the couple composed by the combination of malicious code (6) and phishing and ransomware (1) and web attacks (2), with parameters 1.99 and 0.17, suggesting a positive relationship of the lower extreme values of distribution; independence for the remaining two couples composed by the combination of malicious code (6) and stolen devices (5) and malware and botnets (4) and the combination of malware and botnets (4) and web attacks (2) and malicious code (6).

Tree 3 defines the following relationships: a 180° type 2 Rotated Twan copula for the couple composed of the combination of malicious code (6) and malicious insider (3) and the combination of web attacks (2) and phishing and ransomware (1), with parameters 20 and 0.04, suggesting a positive weak relationship of the lower extreme values of distribution: a Joe Copula for the couple composed by the combination of malware and botnets (4) and phishing and ransomware (1) and the combination of malicious code (6) and web attacks (2), with parameters 1.16, suggesting a positive relationship in the upper tail of distribution: independence for the couples composed by the combination of web attacks (2) and stolen devices (5) and the combination of malicious code (6) and malware and botnets (4).

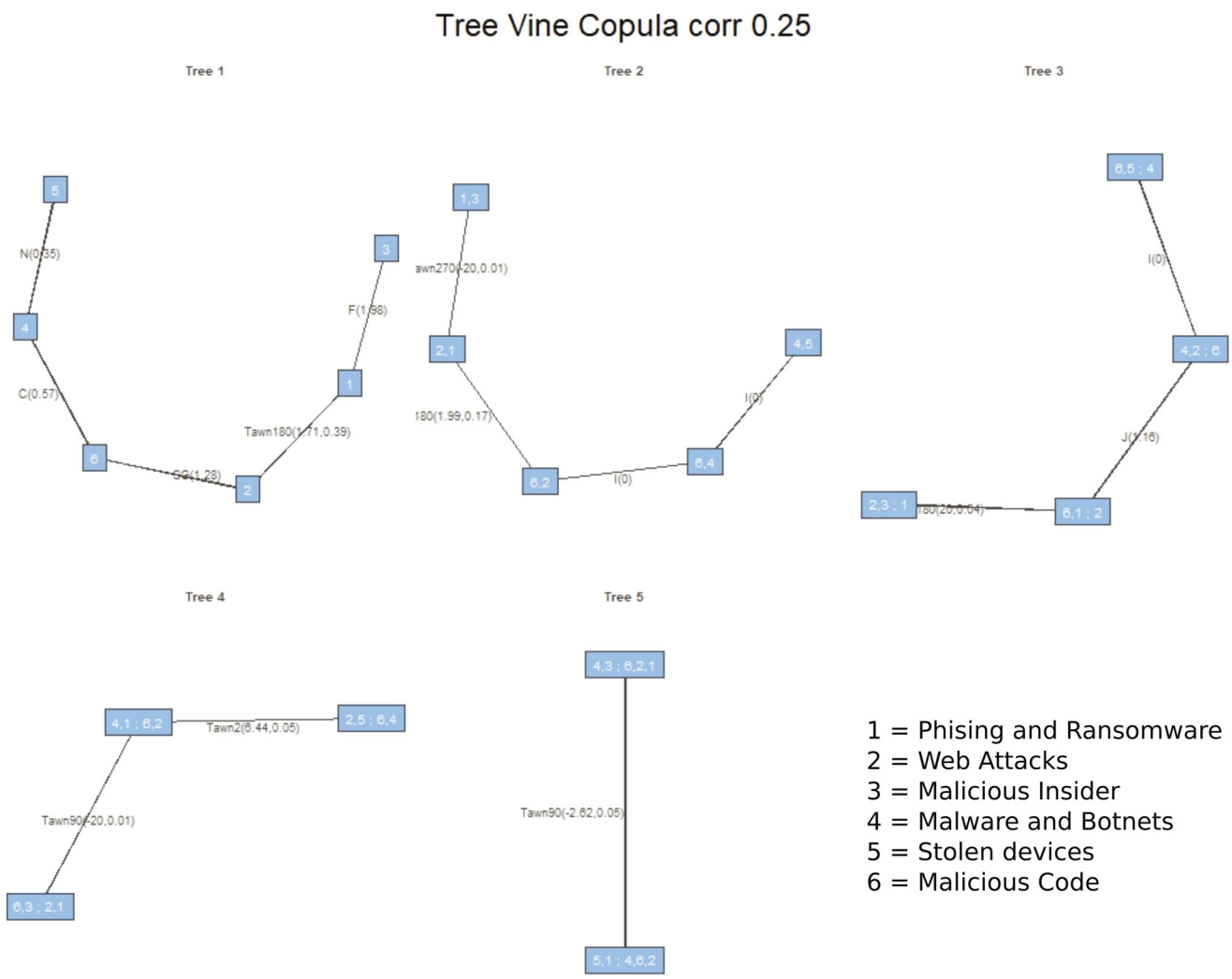

FIGURE 1 Tree of vine copula (normal copula 0.25).

Tree 4 defines the following relationships: a 90° type 1 Rotated Twan copula for the couple composed of the combination of malware and botnets (4) and malicious insider (3) and the combination of malicious code (6), web attacks (2), and phishing and ransomware (1), with parameters −20 and 0.01, suggesting a negative relationship in the upper extreme values of the distribution; and a type 2 Twan copula for the couple composed of the combination of stolen devices (5) and phishing and ransomware (1) and the combination of malware and botnets (4), malicious code (6), and web attacks (2), with parameters 6.44 and 0.05, suggesting a positive relationship in the upper extreme values of the distribution.

Tree 5 defines a 90 degree type 1 Rotated Twan copula with parameters −2.62 and 0.05 for the couple composed of the combination of stolen devices (5) and malicious insider (3) and the combination of malware and botnets (4), malicious code (6), web attacks (2), and phishing and ransomware (1), suggesting a negative relationship in the upper extreme values of the distribution.

Figure 2 summarizes the parameters of the vine copula estimated starting from a sample simulated from a normal copula with a linear correlation coefficient of 0.5.

As shown in Figure 2, Tree 1 defines the following relationships: a Gaussian copula for the couple malicious code (6) and malicious insider (3) with parameter 0.59, suggesting a positive linear correlation; a type 1 Twan copula for the couple malware and botnets (4) and web attacks (2), with parameters 2.03 and 0.56, suggesting a positive relationship of the upper extreme values of the distribution; Frank copula for the couple phishing and ransomware (1) and malware and botnets (4), with parameter 4.51, suggesting a positive relationship of the central observations and week for tail observations; Gumbel copula for the couple malicious code (6) and phishing and ransomware (1), with parameter 1.28,

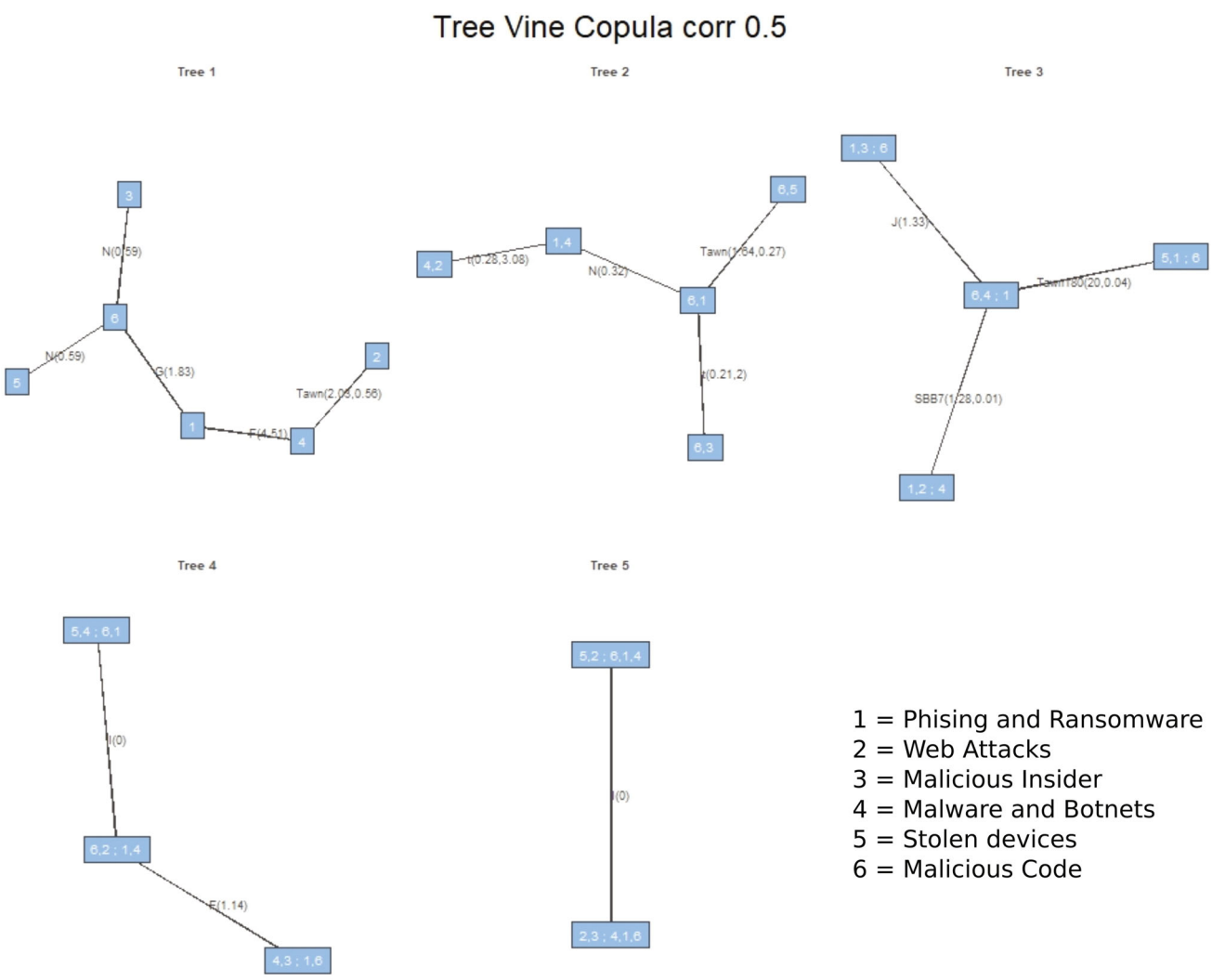

FIGURE 2 Tree of vine copula and linear correlation 0.5.

suggesting a positive dependence of the lower tail observations; and Gaussian copula for the couple malicious code (6) and stolen devices (5), with parameter 0.59, suggesting a positive linear correlation.

Tree 2 defines the following relationships: a t copula for the couple composed by the combination of phishing and ransomware (1) and malicious insider (3) and malicious code (6) with parameters 0.21 and 2, suggesting a positive symmetrical relationship on the tails of distribution; a t copula for the couple composed by the combination of phishing and ransomware (1) and web attacks (2) and malware and botnets (4) with parameters 0.28 and 3.08, suggesting a positive symmetrical relationship on the tails of distribution; a Gaussian copula for the couple composed by the combination of malicious code (6) and malware and botnets (4) and phishing and ransomware (1), with parameter 0.31, suggesting a positive linear correlation; a Type 1 Tawn copula for the couple composed by the combination of stolen devices (5) and phishing and ransomware (1) and malicious code (6), with parameters 1.64 and 0.27, suggesting a positive correlation on the upper extreme values of the distribution.

Tree 3 defines the following relationships: a Joe copula for the couple composed by the combination of malware and botnets (4) and malicious insider (3) and the combination of phishing and ransomware (1) and malicious code (6), with parameter 1.33, suggesting a positive upper tail relationship; a survival BB7 copula for the couple composed by the combination of malicious code (6) and web attacks (2) and the combination of phishing and ransomware (1) and malware and botnets (4), with parameters 1.28 and 0.01, suggesting a positive relationship in the tails of distribution; a 180° Rotated Twan copula for the couple composed by the combination of stolen devices (5) and malware and botnets (4) and the combination of malicious code (6) and phishing and ransomware (1), with parameters 20 and 0.04, suggesting a weak positive correlation of the lower extreme values of distribution.

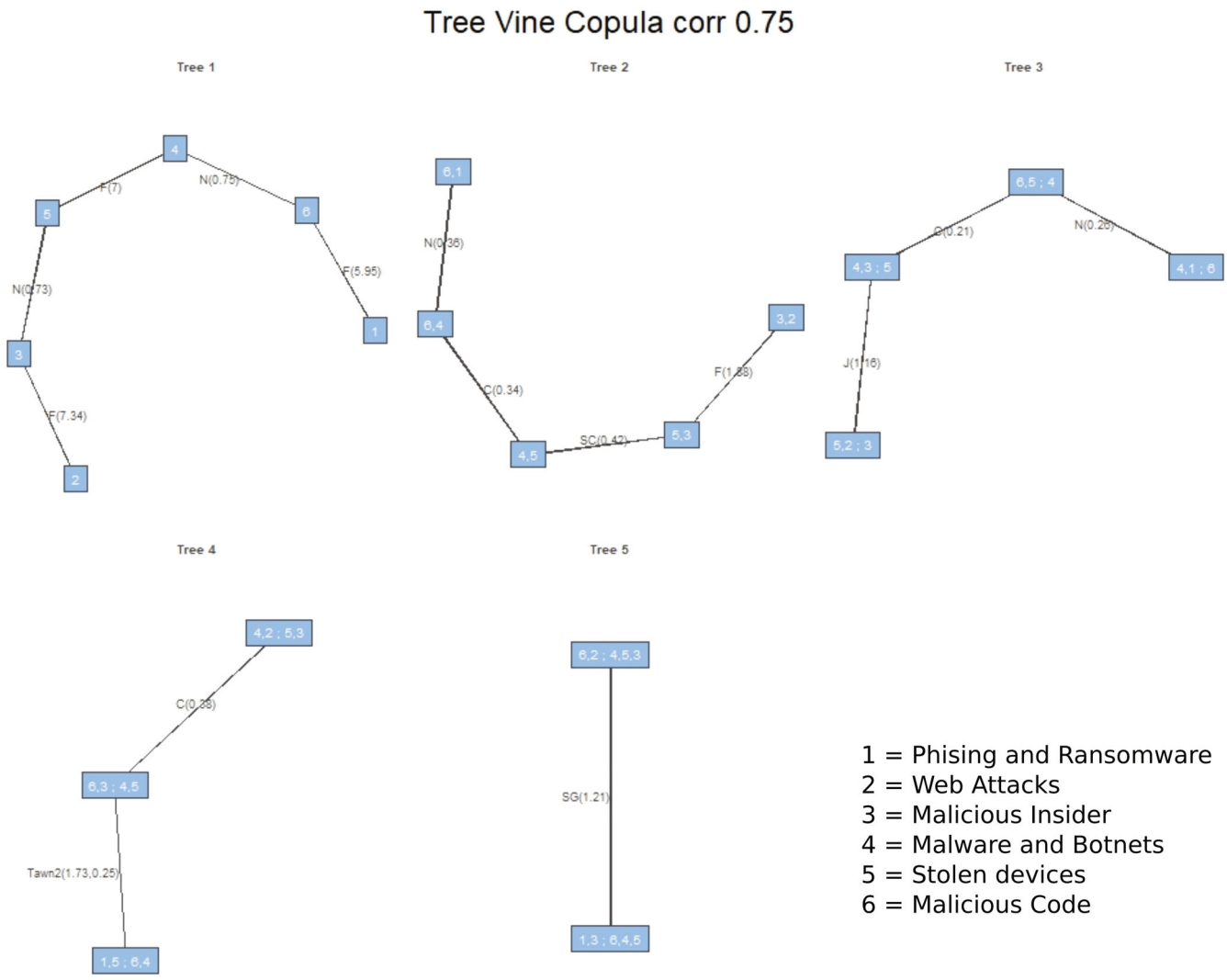

FIGURE 3 Tree of vine copula and linear correlation 0.75.

Tree 4 defines the following relationships: a Frank copula for the couple composed by the combination of web attacks (2) and malicious insider (3) and the combination of malware and botnets (4), phishing and ransomware (1), and malicious code (6), with parameter 1.14, suggesting a positive correlation for the central values of the distribution: independence for the couple composed by the combination of stolen devices (5) and web attacks (2) and the combination of and malicious code (6), phishing and ransomware (1), and malware and botnets (4). Tree 5 defines the following relationship: independence for the couple composed of the combination of stolen devices (5) and malicious insider (3) and the combination of web attacks (2), malware and botnets (4), phishing and ransomware (1), and malicious code (6).

Figure 3 summarizes the parameters of the vine copula estimated starting from a sample simulated from a normal copula with a linear correlation coefficient of 0.75.

As shown in Figure 3, Tree 1 defines the following relationships: a Frank copula for the couple malicious insider (3) and web attacks (2), with parameter 7.34, suggesting a strong positive relationship in the central observations of the distribution; a Gaussian copula for the couple stolen devices (5) and malicious insider (3), with parameters 0.73, suggesting a strong positive linear correlation; a Frank copula for the couple malware and botnets (4) and stolen devices (5), with parameter 7, suggesting a strong positive relationship in the central observations of the distribution; a Frank copula for the couple malicious code (6) and phishing and ransomware (1), with parameter 5.95, suggesting a strong positive relationship in the central observations of the distribution; a Gaussian copula for the couple malicious code (6) and malware and botnets (4), suggesting a strong positive linear correlation.

Tree 2 defines the following relationships: a Frank copula for the couple composed by the combination of stolen devices (5) and web attacks (2) and malicious insider (3), with parameter 88, suggesting a positive relationship in the

central observations of the distribution; a survival Clayton copula for the couple composed by the combination of malware and botnets (4) and malicious insider (3) and stolen devices (5), with parameter 0.34, suggesting a positive relationship in the lower tail of distribution; a Clayton copula for the couple composed by the combination of malicious code (6) and stolen devices (5) and malware and botnets (4), with parameter 0.34, suggesting a positive relationship in the upper tail of distribution; a Gaussian copula for the couple composed by the combination of malware and botnets (4) and phishing and ransomware (1) and malicious code (6), with parameters 0.36, suggesting a positive linear correlation.

Tree 3 defines the following relationships: a Joe copula for the couple composed of the combination of malware and botnets (4) and web attacks (2) and the combination of stolen devices (5) and malicious insider (3), with parameter 1.16, suggesting a weak positive relationship of the upper tail of distribution; a Clayton copula for the couple composed of the combination of malicious code (6) and malicious insider (3) and the combination of malware and botnets (4) and stolen devices (5), with parameter 0.21, suggesting a weak positive relationship in the lower tail of distribution; a Gaussian copula for the couple composed by the combination of phishing and ransomware (1) and stolen devices (5) and the combination of malicious code (6) and malware and botnets (4), with parameter 0.26, suggesting a linear correlation.

Tree 4 defines the following relationships: a Clayton copula for the couple composed by the combination of malicious code (6) and web attacks (2) and the combination of malware and botnets (4), stolen devices (5) and malicious insider (3), with parameter 0.38, suggesting a correlation on the lower tail of distribution; a type 2 Tawn copula for the couple composed by the combination of phishing and ransomware (1) and malicious insider (3) and the combination of malicious code (6), malware and botnets (4) and stolen devices (5), with parameter 1.73, suggesting a relationship in the upper extreme values of distribution.

Tree 5 defines the following relationship: a survival Gumbel for the couple composed of the combination of phishing and ransomware (1) and web attacks (2) and the combination of malicious code (6), malware and botnets (4), stolen devices (5), and malicious insider (3), with parameter 1.21, suggesting a relationship on the lower tail of distribution.

As Figures 1–3 show, the relationships among variables and groups of variables are strongly affected by the a priori hypothesis on the value of the correlation coefficients. In particular, as the correlation coefficient increases, the relationships appear more symmetrical and concentrated on the non-extreme values of the distribution. Assuming a low correlation level (0.25), we observe many non-linear relationships concentrated on the extreme values, in particular, for many pairs the best copula is the Tawn copula class, which considers the strongest relationships in the extreme values of the distribution. Assuming an average correlation (0.5), we observe more Gaussian, t and Frank as best copula, suggesting a symmetrical relationship in the central values of distribution. Finally, assuming a high correlation level (0.75), we observe that asymmetrical copulas are the minority.

With regard to the variables involved in the relationship, Tree 1 shows an invariant correlation between malicious code and stolen devices, and between malware and botnets in the 0.25 and 0.75 scenarios, yet the other relationship changes. For instance, malicious insider changes the neighbor in all trees and is correlated with phishing and ransomware when the correlation is 0.25, with malicious code when the correlation is 0.5, and with web attacks and stolen devices when the correlation is 0.75; for Tree 2, we observe that for a correlation level of 0.5, malicious code is related to the greatest number of risks, while this does not occur in the other scenarios. This aspect is also more evident for the other levels of correlation when in Tree 3, Tree 4 and Tree 5. In this sense, malicious code seems to be the main risk that exposes a company to other cyber risks.

After obtaining the copula parameters, we simulate the joint distribution for the marginal distribution of the aggregated event. To estimate the joint probability distributions, we performed the simulation for each copula on 100,000 realizations, repeating this algorithm 1000 times. In particular, we simulate 100,000 realizations, that is sextuplets, where every element represents the loss of a determined cyber risk, extracting from a given copula and then, by the sum of the six losses, accordingly we calculate the aggregated loss. In this way, for a given copula and a certain set of parameters, we have 100,000 valuations of the aggregate loss. Starting from these values, we calculate the statistics VaR(95%), VaR(99.5%), TVaR(95%) and TVaR(99.5%). Considering that the sensitivity of the tails of the multivariate distribution with 6 dimensions could present, we mitigate the possibility of material errors by repeating 1000 times the simulation procedure of the 100,000 sextuplets, obtaining a distribution of 1000 values of VaR and TVaR. Then, we obtain the final value for VaR and TVaR by the median of the distributions. We selected this level of probability to subsequently calculate the solvency capital requirements for cyber risk. The results are shown in Tables 8 and 9

As Table 8 shows, considering the sample median of 1000 outputs, VaR(99.5%) increases as the correlation increases, and the differences between the normal copula and the vine copula would lead to capital requirement reductions. To note is that this phenomenon of increasing VaR as the correlation increases is not generally true, but occurs in a context of insurable risks, since the greater the diversification, the lower the capital requirement.

TABLE 8 Normal copula and vine copula comparison for VaR(99.5%).

	Sample median VaR(99.5%)					
	Normal copula			Vine copula		
Risks	corr = 0.25%	corr = 0.5%	corr = 0.75%	corr = 0.25%	corr = 0.5%	corr = 0.75%
Phishing and ransomware	1,192,008	1,188,508	1,179,021	1,190,918	1,186,894	1,181,654
Web attacks	3,154,286	3,199,773	3,151,042	3,169,515	3,170,060	3,159,751
Malicious insider	986,261	981,942	987,420	975,731	980,982	974,904
Malware and botnets	2,420,530	2,466,598	2,436,624	2,441,124	2,452,032	2,452,036
Stolen devices	762,511	755,346	760,949	764,342	756,956	759,737
Malicious code	1,075,289	1,067,568	1,076,559	1,073,684	1,069,127	1,073,700
Joint distribution	9,523,611	10,339,891	10,357,404	9,273,039	9,976,752	10,172,877

TABLE 9 Normal copula and vine copula comparison for TVaR(99.5%).

	Sample median TVaR(99.5%)					
	Normal copula			Vine copula		
Risks	corr = 0.25%	corr = 0.5%	corr = 0.75%	corr = 0.25%	corr = 0.5%	corr = 0.75%
Phishing and ransomware	7,337,990	7,654,208	7,611,303	8,107,545	7,532,957	7,411,135
Web attacks	19,815,029	21,806,988	19,050,564	20,441,766	20,135,248	19,266,017
Malicious insider	6,741,089	6,356,957	6,056,343	6,498,443	6,625,805	6,401,735
Malware and botnets	17,504,595	17,155,716	16,029,974	16,548,079	16,126,057	16,449,781
Stolen devices	5,067,898	5,067,610	4,858,431	4,854,961	5,019,510	4,577,981
Malicious code	6,792,429	6,764,862	6,591,121	7,361,943	6,782,254	7,247,575
Joint distribution	61,473,361	64,383,698	65,011,934	56,430,445	59,057,018	59,614,953

TABLE 10 Normal copula and vine copula comparison for VaR(95%)/MEAN.

	VaR(95%)/MEAN					
	Normal copula			Vine copula		
Risks	corr = 0.25%	corr = 0.5%	corr = 0.75%	corr = 0.25%	corr = 0.5%	corr = 0.75%
Phishing and ransomware	2.21	2.22	1.35	1.82	2.48	2.18
Web attacks	2.05	2.35	2.33	1.3	2.11	1.61
Malicious insider	2.24	1.95	1.82	1.98	2.01	2.04
Malware and botnets	2.18	2.52	2.17	2.53	2.12	2.3
Stolen devices	1.56	2.33	1.64	1.11	2.41	1.66
Malicious code	1.29	2.58	2.73	2.02	2.15	2.05
Aggregated risks (from joint distribution)	1.87	2.49	2.1	1.73	2.18	1.86

As Table 9 shows, considering the sample median of 100 outputs, TVaR(99.5%) increases as the correlation increases, and there are differences between the normal copula and the vine copula that would lead to capital requirement reductions. It could be noticed that differences in individual risks do not depend on correlation or copula levels, so they are only the result of simulation error as they should not be affected by correlation levels.

As can we see from Tables 10 and 11 if we analyse the marginal simulated distribution, the ratios VaR(95%)/MEAN and TVaR(95%)/MEAN are very close to the values in Equation (10). This result represents empirical evidence of the goodness of fitting of marginal distributions.

TABLE 11 Normal copula and vine copula comparison for TVaR(95%)/MEAN.

	TVaR(95%)/MEAN					
	Normal copula			Vine copula		
Risks	corr = 0.25%	corr = 0.5%	corr = 0.75%	corr = 0.25%	corr = 0.5%	corr = 0.75%
Phishing and ransomware	16.23	16.20	17.71	16.89	15.78	16.35
Web attacks	16.81	16.38	16.36	17.98	16.72	17.50
Malicious insider	15.88	16.43	16.69	16.35	16.33	16.21
Malware and botnets	16.65	16.18	16.73	16.15	16.75	16.48
Stolen devices	17.68	16.52	17.56	18.36	16.40	17.54
Malicious code	17.96	15.94	15.72	16.81	16.62	16.80
Aggregated risks (from joint distribution)	14.23	14.23	14.23	14.23	14.23	14.23

To proceed with the estimation, the capital requirement is calculated under the Pillar 1 framework, namely, using VaR, and the Pillar 2 framework considering a consistent risk measure, namely, TVaR at the probability level of 99.5% of the multivariate distribution of the aggregate losses. The tail VaR was preferred over the VaR, as well as subadditivity since it better captures the risk related to the tail of the highly asymmetrical distribution and is, therefore, suitable to properly represent the catastrophic events related to cyber risks.

4.3 | Insurance contract estimation

Table 12 reports the main results for the insurance contract.

Considering that there are currently 163 companies in the Italian market, assuming a potential pool of insurers with appropriate reinsurance disposals, the overall premium for the Italian market would be between 365 and 391 million euro, or between approximately 0.26% and 0.28% total premiums stipulated in 2020 of the approximately 138.6 billion Euro (ANIA[2]) considering a VaR risk measure to calculate the solvency capital requirement and the consequent safety loading for pricing: 1504 and 1670 million euros, or between about 1.07% and 1.19% of the total premiums written in 2020 considering a TVaR risk measure to calculate the solvency capital requirement and the consequent safety loading for pricing.

We then calculate the capital add-on in terms of the first pillar for the entire Italian insurance market, including cybernetic risk under operational risks. At the Pillar 1 level, the capital requirement of operational risk is added to the capital requirement of the remaining risks (market, underwriting, counterparty) or implicitly assuming a maximum-positive correlation leading to a zero diversification effect. We make the same assumption to assess the capital add-on for cyber risks, treating the latter as a potential risk in the capital requirement for operational risks.

Considering the solvency data of the Italian market on December 31, 2020, we obtained an SCR of about 58 billion euros, own funds of about 140 billion euros, and a solvency ratio of around 242%. Based on our calculations for the entire Italian market, the capital add-on would be between 1.48 and 1.67 billion euros, namely, between 1.07% and 1.21% of premiums of contracts signed, and considering the capital requirement for cyber risks would therefore reduce the solvency ratio of between 5.99% and 6.76%.

Since both the probability distributions representing the six marginal distributions and the joint multivariate distribution have extremely heavy right tails, if we calculate the capital requirement using a risk measure capable of capturing this aspect (TVaR) at the same 99.5% percentile, we would have a significant capital burden. Based on our calculations for the entire Italian market, this capital add-on would be between 8.31 and 9.31 billion euros, namely, between 6.00% and 6.72% of premiums of contracts signed, and considering the capital requirement for cyber risks would therefore reduce the solvency ratio of between 30.3% and 33.4%.

[2]https://www.ania.it/documents/35135/126701/L%27Assicurazione+Italiana+2020-2021.pdf/e4fa652e-dda7-8c9c-96ef-1e4468d4f903?version=1.0;&t=1626333153413, accessed on February 4, 2022.

TABLE 12 Insurance contracts comparing normal copula and vine copula and VaR and TVaR.

	Normal copula			Vine copula		
	corr = 0.25%	**corr = 0.5%**	**corr = 0.75%**	**corr = 0.25%**	**corr = 0.5%**	**corr = 0.75%**
Equivalence premium for a single insurance ($)	597,574	597,574	597,574	597,574	597,574	597,574
Dollar/Euro exchange rate at 2020.12.31	1.22	1.22	1.22	1.22	1.22	1.22
Expenses loading %	0.25	0.25	0.25	0.25	0.25	0.25
Safety loading for pure premium with VaR(99,5%) ($)	1,070,766	1,154,634	1,173,852	1,039,562	1,117,090	1,153,236
Expenses loading ($)	199,191	199,191	199,191	199,191	199,191	199,191
Expenses loaded premium for a single insurance ($)	1,867,532	1,951,400	1,970,618	1,836,328	1,913,856	1,950,002
Expenses loaded premium for a single insurance (€)	2,278,389	2,380,708	2,404,154	2,240,320	2,334,904	2,379,002
SCR with VaR(99,5%) (€)	9,336,775	10,087,111	10,259,046	9,057,602	9,751,215	10,074,603
Expected profit net COC with VaR(99.5%) (€)	185,922	198,200	201,014	181,354	192,704	197,995
RORAC with VaR(99,5%) (€)	0.02	0.02	0.02	0.02	0.02	0.02
Total cyber premiums for the Italian market (€)	371,377,443	388,055,375	391,877,025	365,172,190	380,589,306	387,777,357
% on total premiums for the Italian market (€)	0.00	0.00	0.00	0.00	0.00	0.00
Safety loading for pure premium with TVaR(99,5%) ($)	6,957,097	7,472,237	7,790,016	7,051,736	7,364,646	7,452,631
Expenses loading ($)	199,191	199,191	199,191	199,191	199,191	199,191
Expenses loaded premium for a single insurance ($)	7,566,813	8,081,788	8,399,533	7,661,520	7,974,268	8,062,185
Expenses loaded premium for a single insurance (€)	9,231,511	9,859,782	10,247,431	9,347,054	9,728,607	9,835,866
SCR with TVaR(99.5%) (€)	51,006,571	54,784,427	57,114,842	51,700,523	53,995,357	54,640,648
Expected profit net COC with TVaR(99.5%) (€)	2,138,669	2,313,596	2,421,595	2,170,937	2,277,110	2,306,934
RORAC with TVaR(99.5%) (€)	0.04	0.04	0.04	0.04	0.04	0.04
Total cyber premiums for the Italian market (IM) (€)	1,504,736,367	1,607,144,417	1,670,331,197	1,523,569,834	1,585,762,911	1,603,246,117
% on total premiums for the IM (€)	0.01	0.01	0.01	0.01	0.01	0.01
SCR CYBER for the IM with VaR(99.5%) (€)	1,521,894,308	1,644,199,147	1,672,224,577	1,476,389,119	1,589,447,973	1,642,160,346
SCR for the IM with VaR(99.5%) without SCR CYBER (€)	58,000,000,000	58,000,000,000	58,000,000,000	58,000,000,000	58,000,000,000	58,000,000,000

(Continues)

TABLE 12 (Continued)

	Normal copula			Vine copula		
	corr = 0.25%	corr = 0.5%	corr = 0.75%	corr = 0.25%	corr = 0.5%	corr = 0.75%
SCR for the IM with VaR(99.5%) with SCR CYBER (€)	59,521,894,308	59,644,199,147	59,672,224,577	59,476,389,119	59,589,447,973	59,642,160,346
OWN FUNDS (€)	140,000,000,000	140,000,000,000	140,000,000,000	140,000,000,000	140,000,000,000	140,000,000,000
SOLVENCY RATIO for the IM with CYBER risk	2.35	2.35	2.35	2.35	2.35	2.35
SOLVENCY RATIO for the IM without CYBER risk	2.41	2.41	2.41	2.41	2.41	2.41
DELTA%	−0.06	−0.07	−0.07	−0.06	−0.06	−0.07
SCR CYBER for the IM with TVaR(99.5%) (€)	8,314,070,995	8,929,861,544	9,309,719,287	8,427,185,180	8,801,243,248	8,906,425,698
SCR for the IM with TVaR(99.5%) without SCR CYBER (€)	58,000,000,000	58,000,000,000	58,000,000,000	58,000,000,000	58,000,000,000	58,000,000,000
SCR for the IM with TVaR(99.5%) with SCR CYBER (€)	66,314,070,995	66,929,861,544	67,309,719,287	66,427,185,180	66,801,243,248	66,906,425,698
OWN FUNDS (€)	140,000,000,000	140,000,000,000	140,000,000,000	140,000,000,000	140,000,000,000	140,000,000,000
SOLVENCY RATIO for the IM with CYBER risk	2.11	2.09	2.08	2.11	2.10	2.09
SOLVENCY RATIO for the IM without CYBER risk	2.41	2.41	2.41	2.41	2.41	2.41
DELTA %	−0.30	−0.32	−0.33	−0.31	−0.32	−0.32

5 | CONCLUDING REMARKS

Cyber risk is a significant issue in any economic system, particularly in the context of the increasing adoption of digital technologies, for instance, in InsurTech. Several studies document the spillover effects of cyber security breaches (for a complete review see[53]), highlighting the so-called cyber accumulation risk caused by interdependent digital systems. According to our analysis, the dependence structure becomes an essential feature of price-setting and regulatory issues of insurance companies. Disregarding the dependence structure in cyber risk management leads to inconsistent estimates of potential unintended losses. In the context of EU insurance regulation, to determine a pricing method for the cyber risk, it is necessary to consider the large positive asymmetry of distributions, critically different from the other non-life business areas. We propose a method that considers the cost of capital, which likewise considers the distributions' tails since the risk capital is a function of VaR and TVaR. Generally, for non-life insurance contracts, the safety loading never exceeds 50% of the fair premium. In cyber risk cases, the safety loading is 179% of the fair premium considering VaR as a measure of risk and 1165%, considering TVaR as a measure of risk.

As a consequence, hedging to cyber risk is highly expensive as the insurance companies should reserve an amount of risk capital not comparable with the same as the other non-life business areas. Indeed, considering the non-life portfolios of Italian insurance companies, cyber risk hedging products represent on average less than 1% of the total.

This article answers the question of why insurance companies do not ride the wave of cyber risk to offer hedging products. According to our approach, the issue is that insurance companies should offer huge premiums to avoid liquidity problems, making the insurance products out of the market unless they apply many limitation contractual clauses.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are available from the corresponding author upon reasonable request.

ORCID

Maria Carannante https://orcid.org/0000-0002-5524-0613

REFERENCES

1. Stouffer K, Zimmerman T, Tang C, Lubell J, Cichonski J, McCarthy J. Cybersecurity framework manufacturing profile. NIST Internal or Interagency Report (NISTIR) 8183. National Institute of Standards and Technology; 2019. Accessed February 4, 2022. https://www.nist.gov/publications/cybersecurity-framework-manufacturing-profile
2. August T, Tunca TI. Who should be responsible for software security? A comparative analysis of liability policies in network environments. *Manag Sci*. 2011;57(5):934-959. doi:10.1287/mnsc.1100.1304
3. Pastor-Satorras R, Castellano C, Van Mieghem P, Vespignani A. Epidemic processes in complex networks. *Rev Mod Phys*. 2015;87(3):925-986. doi:10.1103/RevModPhys.87.925
4. Amini H, Minca A. Inhomogeneous financial networks and contagious links. *Oper Res*. 2016;64(5):1109-1120. doi:10.1287/opre.2016.1540
5. Nagurney A, Shukla S. Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability. *Eur J Oper Res*. 2017;260(2):588-600. doi:10.1016/j.ejor.2016.12.034
6. Khouzani M, Liu Z, Malacaria P. Scalable min-max multi-objective cyber-security optimisation over probabilistic attack graphs. *Eur J Oper Res*. 2019;278(3):894-903. doi:10.1016/j.ejor.2019.04.035
7. Cheung KF, Bell MG. Attacker-defender model against quantal response adversaries for cyber security in logistics management: An introductory study. *Eur J Oper Res*. 2019;291(2):471-481. doi:10.1016/j.ejor.2019.10.019
8. Böhme R, Kataria G. Models and measures for correlation in cyber-insurance. Proceedings of the Workshop on the Economics of Information Security (WEIS). 2006. Accessed February 4, 2022. 2006 https://econinfosec.org/archive/weis2006/docs/16.pdf
9. Böhme R, Schwartz G. Modeling cyber-insurance: towards a unifying framework. Proceedings of the Workshop on the Economics of Information Security. 2010. Accessed February 4, 2022. https://econinfosec.org/archive/weis2010/papers/session5/weis2010_boehme_pres.pdf
10. Mukhopadhyay A, Chatterjee S, Saha D, Mahanti A, Sadhukhan SK. e-risk management with insurance: A framework using copula aided Bayesian belief networks. Proceedings of the 39th Annual Hawaii International Conference on System Sciences; 2006. doi:10.1109/HICSS.2006.138
11. Xu M, Da G, Xu S. Cyber epidemic models with dependences. *Internet Math*. 2015;11(1):62-92. doi:10.1080/15427951.2014.902407
12. Peng C, Xu M, Xu S, Hu T. Modeling multivariate cybersecurity risks. *J Appl Stat*. 2018;45(15):2718-2740. doi:10.1080/02664763.2018.1436701
13. Eling M, Jung K. Copula approaches for modeling cross-sectional dependence of data breach losses. *Insur Math Econ*. 2018;82:167-180. doi:10.1016/j.insmatheco.2018.07.003
14. Sun H, Xu M, Zhao P. Modeling malicious hacking data breach risks. *N Am Actuar J*. 2020;25(4):408-502. doi:10.1080/10920277.2020.1752255
15. Da G, Xu M, Zhang J, Zhao P. Joint cyber risk assessment of network systems with heterogeneous components. 2020. Accessed February 4, 2022. https://arxiv.org/pdf/2006.16092.pdf
16. Da G, Xu M, Zhao P. Multivariate dependence among cyber risks based on L-hop propagation. *Insur Math Econ*. 2021;101:525-546. doi:10.1016/j.insmatheco.2021.09.005
17. Sklar M. *Fonctions de Répartition à n Dimensions et Leurs Marges*. Vol 8. Publications de l'Institut Statistique de l'Université de Paris; 1959:229-231.
18. Joe H. Families of m-variate distributions with given margins and $m(m-1)/2$ bivariate dependence parameters. In: Rüschendorf L, Schweizer B, Taylor MD, eds. *Distributions with Fixed Marginals and Related Topics*. Lecture Notes–Monograph Series. Vol 28. Institute of Mathematical Statistics; 1996:120-141. doi:10.1214/lnms/1215452614
19. Bedford T, Cooke RM. Probability density decomposition for conditionally dependent random variables modeled by vines. *Ann Math Artif Intell*. 2001;32:245-268. doi:10.1023/A:1016725902970
20. Aas K, Czado C, Frigessi A, Bakken H. Pair-copula constructions of multiple dependence. *Insur Math Econ*. 2009;44:182-198. doi:10.1016/j.insmatheco.2007.02.001
21. Czado C. Pair-copula constructions of multivariate copulas. In: Jaworski P, Durante F, Härdle W, Rychlik T, eds. *Copula Theory and Its Applications*. Lecture Notes in Statistics. Vol 198. Springer; 2010:93-109. doi:10.1007/978-3-642-12465-5_4
22. Min A, Czado C. Bayesian inference for multivariate copulas using pair-copula constructions. *J Finan Econ*. 2010;8(4):511-546. doi:10.1093/jfinec/nbp031
23. Herath VSB, Herath TC. Copula-based actuarial model for pricing cyber-insurance policies. *Insur Mark Co Anal Actuar Comput*. 2011;2:7-20.
24. Bedford T, Cooke RM. Vines: A new graphical model for dependent random variables. *Ann Stat*. 2002;30:1031-1068. doi:10.1214/aos/1031689016
25. Xu M, Hua L, Xu S. A vine copula model for predicting the effectiveness of cyber defense early-warning. *Technometrics*. 2017;59:508-520. doi:10.1080/00401706.2016.1256841
26. Nelsen RB. *An Introduction to Copulas*. Springer Series in Statistics. 2nd ed. Springer; 2006.
27. Joe H. Multivariate extreme-value distributions with applications to environmental data. *Can J Stat*. 1994;22:47-64. doi:10.2307/3315822
28. Joe H, Xu JK. The estimation method of inference functions for margins for multivariate models. Working Paper. University of British Columbia. 1996. Accessed February 4, 2022. http://hdl.handle.net/2429/57078
29. Joe H. *Multivariate Models and Dependence Concepts, Monographs on Statistics and Applied Probability*. Vol 73. 1st ed. Chapman ς Hall; 1997.
30. Whelan N. Sampling from Archimedean copulas. *Quant Finance*. 2004;4:339-352.

31. Dißmann JEC, Brechmann CC, Kurowicka D. Selecting and estimating regular vine copulae and application to financial returns. *Comput Stat Data Anal*. 2013;59:52-69. doi:10.1016/j.csda.2012.08.010
32. Joe H, Kurowicka D. *Dependence Modeling: Vine Copula Handbook*. World Scientific; 2011.
33. Dalla Valle L, De Giuli ME, Tarantola C, Manelli C. Default probability estimation via pair copula constructions. *Eur J Oper Res*. 2016;249(1):298-311. doi:10.48550/arXiv.1405.1309
34. Scheffer M, Weiß GNF. Smooth nonparametric Bernstein vine copulas. *Quant Finance*. 2016;17:139-156. doi:10.48550/arXiv.1210.2043
35. Calabrese R, Degl'Innocenti M, Osmetti SA. The effectiveness of TARP-CPP on the US banking industry: A new copula-based approach. *Eur J Oper Res*. 2017;256:1029-1037. doi:10.1016/j.ejor.2016.07.046
36. Pircalabu A, Jung J. A mixed C-vine copula model for hedging price and volumetric risk in wind power trading. *Quant Finance*. 2017;17:1583-1600. doi:10.1080/14697688.2017.1307511
37. Low RKY, Alcock J, Faff R, Brailsford T. Canonical vine copulas in the context of modern portfolio management: Are they worth it? *J Bank Financ*. 2013;37:3085-3099. doi:10.1016/j.jbankfin.2013.02.036
38. Weiß GNF, Supper H. Forecasting liquidity-adjusted intraday value-at-risk with vine copulas. *J Bank Finance*. 2013;37:3334-3350. doi:10.1016/j.jbankfin.2013.05.013
39. Brechmann EC, Czado C, Aas K. Truncated regular vines in high dimensions with application to financial data. *Can J Stat*. 2012;40:68-85. doi:10.1002/cjs.10141
40. Biener C, Eling M, Wirfs J. Insurability of cyber risk: An empirical analysis. *Geneva Pap Risk Insur Issues Pract*. 2014;40:131-158. doi:10.1057/gpp.2014.19
41. Blanchet J, Lam H, Tang Q, Yuan Z. Robust actuarial risk analysis. *N Am Actuar J*. 2019;23(1):33-63. doi:10.1080/10920277.2018.1504686
42. Bracho A, Saygin C, Wan H, Lee Y, Zarreh A. A simulation-based platform for assessing the impact of cyber-threats on smart manufacturing systems. *Procedia Manuf*. 2018;26:1116-1127. doi:10.1016/j.promfg.2018.07.148
43. Conrad JR. Analyzing the risks of information security investments with Monte-Carlo simulations. Workshop on the Economics of Information Security; 2005. IEEE Computer Society. Accessed February 13, 2023. https://infosecon.net/workshop/pdf/13.pdf
44. Couretas JM. Cyber modeling and simulation and system risk analysis. In: Couretas JM, eds. *An Introduction to Cyber Modeling and Simulation*. John Wiley & Sons; 2018:101-124. doi:10.1002/9781119420842.ch9
45. Kavak H, Padilla JJ, Vernon-Bido D, Diallo SY, Gore R, Shetty S. Simulation for cybersecurity: state of the art and future directions. *J Cybersecur*. 2021;7(1):tyab005. doi:10.1093/cybsec/tyab005
46. Wagner N, Lippmann R, Winterrose M, Riordan R, Yu T, Streilein W. Agent-based simulation for assessing network security risk due to unauthorized hardware. Simulation Series. 47. 2015. Accessed February 4, 2022. https://www.ll.mit.edu/sites/default/files/publication/doc/2018-04/2015-04-Wagner-ACM.pdf
47. Alm J. A simulation model for calculating solvency capital requirements for non-life insurance risk. *Scand Actuar J*. 2015;2015(2):107-123. doi:10.1080/03461238.2013.787367
48. Bauer D, Reuss A, Singer D. On the calculation of the solvency capital requirement based on nested simulations. *ASTIN Bull*. 2012;42(2):453-499. doi:10.2143/AST.42.2.2182805
49. Gaigall D. Test for changes in the modeled solvency capital requirement of an internal risk model. *ASTIN Bull*. 2021;51(3):813-837. doi:10.1017/asb.2021.20
50. Rossetti MD. Simulation modeling and arena. 3rd and open text edition; 2021. Accessed February 13, 2023. https://rossetti.github.io/RossettiArenaBook/
51. Planchet F, Jacquemin J. L'utilisation de methodes de simulation en assurance. *Bull Fr d'Actuariat*. 2003;6(11):37-69.
52. Brechmann EC, Schepsmeier U. Modeling dependence with C- and D-vine copulas: The R package CDVine. *J Stat Softw*. 2013;52(3):1-27. doi:10.18637/jss.v052.i03
53. McShane M, Eling M, Nguyen T. Cyber risk management: History and future research directions. *Risk Manag Insur Rev*. 2021;24(1):93-125. doi:10.1111/rmir.12169

How to cite this article: Carannante M, D'Amato V, Fersini P, Forte S, Melisi G. Vine copula modeling dependence among cyber risks: A dangerous regulatory paradox. *Appl Stochastic Models Bus Ind*. 2023;39(4):549-566. doi: 10.1002/asmb.2767