*7th European Conference on Industrial Engineering and Operations Management*
*Augsburg, Germany, July 16-18, 2024*
Publisher: IEOM Society International, USA DOI: 10.46254/EU07.20240258
Published: July 16, 2024

# Analyzing the Critical Challenges of Cyber Insurance Market: A Fuzzy DEMATEL Approach

**Subinoy Banerjee**
Research Scholar
Vinod Gupta School of Management
Indian Institute of Technology
Kharagpur, West Bengal, India

**Dr Saini Das**
Vinod Gupta School of Management
Indian Institute of Technology
Kharagpur, West Bengal, India
subinoy@iitkgp.ac.in, saini@vgsom.iitkgp.ac.in

## Abstract

Cyber Insurance (CI) is an important cyber risk management tool in industry and academia. Despite several commitments, its adoption rate is meagre. This research provides significant insights and analysis into the complex issues of i) identifying the key challenges in the cyber insurance (CI) market and ii) understanding how these influential challenges and their cause-effect relationships can inform policymakers to improve the CI ecosystem. An extensive literature review identified twenty-three challenges in the cyber insurance market. Industry experts in this field further validated these challenges, filtering them down to eleven major challenges for further analysis. The cause-effect analysis of the challenges is determined using the fuzzy DEMATEL (FDEMATEL) approach. Finally, this study concludes that for a cyber insurance (CI) ecosystem to be successful, it is crucial to a) tackle the significant challenges posed by the cascading effects of correlated cyber risks and b) ensure the active participation of Chief Information Security Officers (CISOs) to grasp the CI value chain.

## Keywords
Cyber security, Cyber Insurance, FDEMATEL, Correlated Cyber Risk.

## 1. Introduction and Literature Review
The development of information technology reduces business costs and operation time but enhances information security risks at an unexpected level. In order to protect themselves from cyber risks, organizations are implementing various information security controls. However, complete mitigation of those cyber risks is not feasible. There was always an element of risk that cannot be mitigated. (Marotta et al. 2017.;Pal et al. 2014.;OECD. 2017) CI is designed to transfer those residual risks to a third party i.e., the insurer (Bohme 2005) . Despite several commitments, the CI adoption rate is abysmal (Meland et al. 2015;Eling, M., and Schnell,W. 2016.). Several studies have investigated the various barriers in the cyber insurance market, focusing on specific contexts such as small and medium businesses, geography-specific rules and regulations, and specific business scenarios (Meland et al. 2015;Woods, D., and Simpson 2017). However, an exhaustive literature review revealed a lack of comprehensive studies on the major challenges in the cyber insurance market. To address this research gap, this study formulated the following research questions. RQ1: What are the primary challenges confronting the present cyber insurance market? RQ2: How can the correlation

between these challenges be measured? RQ3: What insights can be derived from these challenges in policymaking to improve cyber insurance adoption?

## 2. Objectives

The objective of this study is to understand the primary challenges confronting the present cyber insurance market. And how can the correlation between these challenges be measured.

## 3. Methods and Data Collection

This paper employs the FDEMATEL method to identify the primary challenges in the cyber insurance process. The steps involved are as follows. Initially, the extensive literature review identifies a list of 23 challenges in the CI process (Aziz et al. 2020). Subsequently, an interview with a panel of 11 experts (Table 1) in this field is conducted to categorize and pinpoint the key challenges in the CI process. Most respondents possess over 17 years of experience in various domains, including information security, insurance business, risk management, actuarial science, and cyber law. Following the interviews, 11 major challenges for the CI process were identified, with details provided in Table 2. Experts were requested to rate the identified challenges in comparison to others using a five-point linguistic scale (Table 3). However, this subjective assessment does not confirm the causal relationship among the key challenges in the cyber insurance (CI) process. Hence, fuzzy set theory is implemented to transform linguistic variables into triangular fuzzy numbers (TFN) (Table 4) (Lin et al. 2006). To overcome the ambiguous concept of subjective judgements. TFN represents the range of triple-values (u, m, l) where $l \leq m \leq u$ in membership functions. 'u' denotes the upper limit of the perceived value, 'm' represents the median of the most likely values, and 'l' indicates the lower limit of the original value. A matrix relation is formed as $Z_{ij}^{k} = \left(l_{ij}, m_{ij}, u_{ij}\right)$ , where $k^{th}$ expert describes the degree to which factor i impacted on factor j. For matrix operation, the fuzzy number is incompatible; hence, a defuzzification is required to convert the fuzzy numbers into crisp numbers named as the best non fuzzy performance value (BNP). This study follows the CFCS method ("Converting Fuzzy data into Crisp Scores") for defuzzication (Opricovic and Tzeng 2004).

Standardization of fuzzy numbers represented as :

$$xl_{ij}^{k} = \left(l_{ij}^{k} - \min_{1\leq k\leq K} l_{ij}^{k}\right) / \Delta_{\min}^{\max} \quad (1)$$

$$xm_{ij}^{k} = \left(m_{ij}^{k} - \min_{1\leq k\leq K} l_{ij}^{k}\right) / \Delta_{\min}^{\max} \quad (2)$$

$$xu_{ij}^{k} = \left(u_{ij}^{k} - \min_{1\leq k\leq K} l_{ij}^{k}\right) / \Delta_{\min}^{\max} \quad (3)$$

Where $\Delta_{\min}^{\max} = \max u_{ij}^{k} - \min l_{ij}^{k}$

xl, xm, xu are normalized fuzzy numbers.

Left side normalized value

$$xls_{ij}^{k} = xm_{ij}^{k} / \left(1 + xm_{ij}^{k} - xl_{ij}^{k}\right) \quad (4)$$

Right side normalized value

$$xrs_{ij}^{k} = xu_{ij}^{k} / \left(1 + xu_{ij}^{k} - xm_{ij}^{k}\right) \quad (5)$$

The total normalized value is described as $x_{ij}^{k} = \left[xls_{j}^{k}\left(1 - xls_{j}^{k}\right) + xrs_{ij}^{k} xrs_{ij}^{k}\right] / \left(1 + xrs_{j}^{k} - xls_{j}^{k}\right)$

(6)

Crisp score of $k^{th}$ experts assessment

$$BNP_{ij}^{k} = \min l_{ij}^{k} + x_{ij}^{k} \Delta_{\min}^{\max} \quad (7)$$

Integrated score (Crisp score average of all K judgement)

$$a_{ij} = \frac{1}{K} \sum_{k}^{1 \le k \le K} BNP_{ij}^{k} \quad (8)$$

Non negative matrix ( n x n ) is represented by A = $[a_{ij}]$. Where $a_{ij}$ represents the impact of factor i on factor j. The diagonal element of the matrix is 0 for i = j.

The normalized matrix is represented by

$$D = \frac{1}{\max\limits_{1 \le i \le n} \sum_{j=1}^{n} a_{ij}} A \quad (9)$$

Where $0 \le dij \le 1$. X

The total relationship matrix is formed from n x n identity matrix is represented by

$$T=D(I-D)^{-1} \quad (10)$$

The degree of influential impact ($r_i$) is calculated by adding all direct and indirect impacts from i to all other factors.

$$r_i = \sum_{1 \le j \le n} t_{ij} \quad (11)$$

Degree of influenced impact ($c_j$) is calculated by summing all direct and indirect impacts received by factor j from all other factors.

$$C_j = \sum_{1 \le i \le n} t_{ij} \quad (12)$$

When i = j, the sum of $r_i$ and $c_i$ reflects both the influence exerted by factor i on the whole system and the influence received from other system factors. Therefore, the sum, $r_i + c_i$, is a measure of the factor's overall importance within the system. Conversely, the difference between the two, $r_i - c_i$, highlights the direct impact factor i has on the system. Specifically, a positive value for $r_i - c_i$ indicates that factor i predominantly acts as a contributing cause, exerting a net positive influence on the system. If $r_i - c_i$ is negative, then factor i is primarily affected by the system, placing it in the category of a resultant effect.

Create a cause-and-effect relationship diagram by utilizing the dataset of ($r_i + c_i$) and ($r_i - c_i$). This diagram helps to visually represent the intricate connections between different challenges of CI process. By creating this diagram, we can identify which challenges significantly impact the CI process and which could substantially build the CI ecosystem efficiently if they are addressed. Such challenges are critical for this study.

## 4. Results and Discussion

Expert interviews are conducted to gather data and assess the interactions between all 11 challenges. The threshold value of the interaction effect comes out to 0.3584. This research considered the interaction effect below threshold values insignificant. The elements in the matrix possessing values above the threshold are depicted in three different shades, representing three value ranges. These ranges are calculated using the difference between the maximum and minimum values and finally dividing by three (R.J. Lin 2013). Table 5 represents the prominence and cause-effect relationships. From the cause group, Lack of historical data (C1) and Uncertainty about the liability(C4) have higher $r_i$-$c_i$, which means C1 and C4 have more influencing power than others. Additionally, C1 and C4 holds $r_i$+$c_i$ values 6.8801 and 7.9816, respectively. It means C1 and C4 have medium to higher prominence to influence other challenges.

The highest prominence value, 8.9819, belongs to C7, which interprets the cascading effect of correlated cyber risk as having mostly influenced other challenges of CI.

## Numerical Results

Table 1. .Respondents Details

| Respondents | Gender | Domain | Experience | Roles |
|---|---|---|---|---|
| R1 | Male | Insurance | 21 | Claim settlement |
| R2 | Male | Insurance | 19 | Risk assessor |
| R3 | Male | Insurance | 23 | I.T. Infrastructure manager |
| R4 | Female | Insurance | 22 | Risk assessor |
| R5 | Male | Director in I.T. consulting | 24 | I.T. risk manager |
| R6 | Male | IT Security | 17 | Info. Security |
| R7 | Male | Insurance | 19 | Risk assessor |
| R8 | Male | IT | 23 | CISO |
| R9 | Female | Bank | 21 | Risk manager |
| R10 | Male | Insurance | 19 | Actuaries |
| R11 | Male | IT | 18 | CTO |

Table 2. Major Challenges Identified

| Code | Challenges | Sources |
|---|---|---|
| C1 | Lack of historical data | (Hatzivasilis et al. 2019) |
| C2 | Dynamic nature of cyber risk | (Kshetri 2019) |
| C3 | Lack of standardisation | (Kshetri 2019) |
| C4 | Uncertainty about the liability | (Skarczinski 2021) |
| C5 | Underrated value chain | (Aziz et al. 2020) |
| C6 | Lack of actuarial data | (Skarczinski 2021) |
| C7 | The cascading effect of correlated cyber risk | (Boyson 2014) |
| C8 | Preference to invest in security control over CI | (Moss 2000) |
| C9 | Existence of the externality effect | (Kshetri 2019,Skarczinski 2021) |
| C10 | Delayed in claim settlement | (Bandyopadhyay 2012) |
| C11 | High premium price | (Bandyopadhyay 2012) |

Table 3. Triangular Fuzzy Scale

| Linguistic terms | Scale | Linguistic values |
|---|---|---|
| Very High Influence(VH) | 4 | (0.75, 1.0, 1.0) |
| High Influence (H) | 3 | (0.5, 0.75, 1.0) |
| Low Influence(L) | 2 | (0,25, 0.5, 0.75) |
| Very Low Influence(VL) | 1 | (0, 0.25, 0.5) |
| No Influence(N) | 0 | (0, 0, 0.25) |

Table 4.Total Relation Matrix

| | C1 | C2 | C3 | C4 | C5 | C6 | C7 | C8 | C9 | C10 | C11 | $r_i$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| C1 | 0.225 | 0.348 | 0.295 | 0.314 | 0.326 | 0.389 | 0.381 | 0.384 | 0.391 | 0.433 | 0.432 | 3.918 |
| C2 | 0.239 | 0.266 | 0.340 | 0.308 | 0.343 | 0.363 | 0.372 | 0.372 | 0.379 | 0.403 | 0.402 | 3.786 |
| C3 | 0.219 | 0.287 | 0.242 | 0.326 | 0.292 | 0.335 | 0.344 | 0.340 | 0.323 | 0.344 | 0.341 | 3.392 |
| C4 | 0.328 | 0.383 | 0.382 | 0.304 | 0.404 | 0.413 | 0.440 | 0.451 | 0.430 | 0.458 | 0.432 | 4.426 |
| C5 | 0.328 | 0.359 | 0.383 | 0.377 | 0.316 | 0.430 | 0.424 | 0.455 | 0.432 | 0.478 | 0.476 | 4.458 |
| C6 | 0.279 | 0.357 | 0.357 | 0.326 | 0.361 | 0.311 | 0.393 | 0.421 | 0.400 | 0.427 | 0.425 | 4.057 |
| C7 | 0.350 | 0.412 | 0.428 | 0.422 | 0.434 | 0.461 | 0.383 | 0.487 | 0.464 | 0.512 | 0.509 | 4.862 |
| C8 | 0.281 | 0.361 | 0.332 | 0.326 | 0.337 | 0.358 | 0.395 | 0.426 | 0.404 | 0.431 | 0.447 | 4.098 |
| C9 | 0.251 | 0.295 | 0.294 | 0.290 | 0.298 | 0.317 | 0.351 | 0.378 | 0.287 | 0.382 | 0.381 | 3.525 |
| C10 | 0.254 | 0.300 | 0.299 | 0.294 | 0.303 | 0.323 | 0.357 | 0.385 | 0.365 | 0.317 | 0.404 | 3.601 |
| C11 | 0.208 | 0.276 | 0.274 | 0.269 | 0.277 | 0.294 | 0.280 | 0.374 | 0.337 | 0.374 | 0.285 | 3.250 |
| $c_i$ | 2.962 | 3.644 | 3.626 | 3.556 | 3.690 | 3.996 | 4.119 | 4.473 | 4.212 | 4.559 | 4.535 | |

Table 5.Prominence And Relationship

| Challenges | $r_i+c_i$ | $r_i-c_i$ | Rank | Relationship |
|---|---|---|---|---|
| C1 | 6.8801 | 0.9556 | 11 | Cause |
| C2 | 7.4304 | 0.1422 | 9 | Cause |
| C3 | 7.0184 | -0.2337 | 10 | Effect |
| C4 | 7.9816 | 0.8698 | 6 | Cause |
| C5 | 8.1480 | 0.7677 | 4 | Cause |
| C6 | 8.0531 | 0.0609 | 5 | Cause |
| C7 | 8.9819 | 0.7430 | 1 | Cause |
| C8 | 8.5713 | -0.3750 | 2 | Effect |
| C9 | 7.7364 | -0.6868 | 8 | Effect |
| C10 | 8.1608 | -0.9581 | 3 | Effect |
| C11 | 7.7851 | -1.2856 | 7 | Effect |

Table 6. Total Relationship Matrix

| | C1 | C2 | C3 | C4 | C5 | C6 | C7 | C8 | C9 | C10 | C11 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **C1** | 0.225 | 0.348 | 0.295 | 0.314 | 0.326 | 0.389 | 0.381 | 0.384 | 0.391 | 0.433 | 0.432 |
| **C2** | 0.239 | 0.266 | 0.340 | 0.308 | 0.343 | 0.363 | 0.372 | 0.372 | 0.379 | 0.403 | 0.402 |
| **C3** | 0.219 | 0.287 | 0.242 | 0.326 | 0.292 | 0.335 | 0.344 | 0.340 | 0.323 | 0.344 | 0.341 |
| **C4** | 0.328 | 0.383 | 0.382 | 0.304 | 0.404 | 0.413 | 0.440 | 0.451 | 0.430 | 0.458 | 0.432 |
| **C5** | 0.328 | 0.359 | 0.383 | 0.377 | 0.316 | 0.430 | 0.424 | 0.455 | 0.432 | 0.478 | 0.476 |
| **C6** | 0.279 | 0.357 | 0.357 | 0.326 | 0.361 | 0.311 | 0.393 | 0.421 | 0.400 | 0.427 | 0.425 |
| **C7** | 0.350 | 0.412 | 0.428 | 0.422 | 0.434 | 0.461 | 0.383 | 0.487 | 0.464 | 0.512 | 0.509 |
| **C8** | 0.281 | 0.361 | 0.332 | 0.326 | 0.337 | 0.358 | 0.395 | 0.426 | 0.404 | 0.431 | 0.447 |
| **C9** | 0.251 | 0.295 | 0.294 | 0.290 | 0.298 | 0.317 | 0.351 | 0.378 | 0.287 | 0.382 | 0.381 |
| **C10** | 0.254 | 0.300 | 0.299 | 0.294 | 0.303 | 0.323 | 0.357 | 0.385 | 0.365 | 0.317 | 0.404 |
| **C11** | 0.208 | 0.276 | 0.274 | 0.269 | 0.277 | 0.294 | 0.280 | 0.374 | 0.337 | 0.374 | 0.285 |

## 5. Discussion

Table 5 indicates that C1, C2, C4, C5, C6 and C7 are identified as cause alternatives, all characterized by a positive value when considering the difference ($r_i$-$c_i$) (Lin 2013). Moreover, these cause alternatives can be divided further into subgroups when looking at their prominence values ($r_i$+$c_i$), categorizing the challenges from a spectrum of low to high. C7 (The cascading effect of correlated cyber risk) is ranked high in prominence and scored as rank one. C4 and C5 also have significant prominence values (7.9816 and 8.148 consecutively) and also have causal influence power towards others' challenges. Out of 11 interaction effects, six positive ($r_i$-$c_i$) values are identified as a causal group, and the remaining five have negative ($r_i$+$c_i$) values.

On the other hand, out of 11 interaction effects, C3, C8, C9, C10 and C11 fall under the effect group. The effect group is represented by the negative values of ($r_i$-$c_i$) (Lin 2013,Patil and Kant 2012). These are less influential in influencing others and are affected by cause group elements. C10 and C11 are getting maximum influenced by the causal group of elements. Hence, it is evident that the challenges of "High premium prices" and "Delays in the claim settlement process" are the worst consequences of the causal effect. These have a moderate prominence value (8.160 and 7.785, respectively) and are scored as rank 3 and rank 7, respectively.

Considering the acceptable range of values (Above threshold values), the elements in the total relation matrix in Table 6 are given three types of coloured shades, signifying different levels of interaction. It results in the following interaction effects: weak (red; values ranging from .3584 to .4096), moderate (yellow; values ranging from .4097 to .4608) and strong (green; values ranging from .4609 to .5119).

## 6. Conclusion

The study employs Fuzzy DEMATEL analysis to reveal major challenges hindering the adoption/ecosystem of CI. Although this study revealed that the Cascading effect of correlated cyber risk (C7) and the Underrated value chain

(C5) are the influential components, the role of higher management remains crucial. The study's findings indicate that the absence of standardization in component C3 is insignificant as it does not exceed the threshold value. Therefore, additional research and insights from experts are necessary to evaluate the efficacy of C3. This fuzzy DEMATEL approach has better cause-effect analyzing power compared to other well-accepted methods like structural equation modelling. This study significantly measured the relationship between the current CI market's challenges. The findings of this work will help cyber insurance providers, regulatory bodies, and policymakers to minimize the challenges and to build a better CI ecosystem. However, this work, like other research, has some limitations. A more significant number of experts may reveal some other challenges. Hence, future work can be done with a larger number of expert's opinions.

## References

Angelica Marotta, Fabio Martinelli , Stefano Nannia, Albina Orlandoc, Artsiom Yautsiukhin, "Cyber-insurance survey", in Computer Science Review, no 24, pp. 35–6, 2017.

Aziz, B., Suhardi, and Kurnia. (2020). A systematic literature review of cyber insurance challenges. *2020 International Conference on Information Technology Systems and Innovation, ICITSI 2020 - Proceedings*, pp 357–363, 2020

Bandyopadhyay, T. (2012). Organizational Adoption of Cyber Insurance Instruments in IT Security Risk Management-A Modeling Approach. *SAIS 2012 Proceedings*, 2012.

Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. *Technovation*, no. *34 vol.* 7, pp 342–353, 2014

Dambra, S., Bilge, L., and Balzarotti, D. (2020). SoK: Cyber insurance - Technical challenges and a system security roadmap. *Proceedings - IEEE Symposium on Security and Privacy*,*2020-May*,1367–1383.

Eling, M., and Schnell, W. (2016). *What do we know About cyber risk and cyber risk insurance?* Emerald Group Publishing Ltd.*Journal of Risk Finance* vol. 17, no 5, pp. 474–491. 2016. https://doi.org/10.1108/JRF-09-2016-0122

Hatzivasilis, G., Chatziadam, P., Petroulakis, N., Ioannidis, S., Mangini, M., Kloukinas, C., Yautsiukhin, A., Antoniou, M., Katehakis, D. G., and Panayiotou, M. (2019). *Cyber insurance of information systems: Security and privacy cyber insurance contracts for ICT and helathcare organizations*. *IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks, CAMAD*, September, 2019.

Kshetri, N. (2020). The evolution of cyber-insurance industry and market: An institutional analysis. *Telecommunications Policy*, Vol. *44 no.* 8, 102007, 2020.

Lin, C. T., Chiu, H., and Chu, P. Y. (2006). Agility index in the supply chain. *International Journal of Production Economics*, vol. *100 no.*2, pp 285–299, 2006.

Meland, P. H., Tondel, I. A., and Solhaug, B. (2015). Mitigating risk with cyber insurance. *IEEE Security and Privacy*, vol. *13 no.* 6, pp 38–43, 2015.

Moss, R. (2000). The Technology Acceptance Model And The Decision To Invest In Information Security. *Proceedings of The Southern Association Of Information Systems Conference*, pp 28–32, 2000

OECD. (2017). *OECD report Enhancing the Role of Insurance in Cyber Risk Management*. OECD,2017

Pal, R., Golubchik, L., Psounis, K., and Hui, P. (2014). *Will Cyber-Insurance Improve Network Security ?* pp 235–243, 2014

R. J. Lin, "Using fuzzy DEMATEL to evaluate the green supply chain management practices," J Clean Prod, vol. 40, pp. 32–39, Feb. 2013.

Rainer Bohme, "*Cyber Insurance Recsited*", Workshop on the Economics of Information Security Kennedy School of Government· Harvard University, 2005.

S. Opricovic and G. H. Tzeng, "Compromise solution by MCDM methods: A comparative analysis of VIKOR and TOPSIS," Eur J Oper Res, vol. 156, no. 2, pp. 445–455, Jul. 2004.

Sachin K.Patil 1, R. Kant, "Identify Critical Success Factor of Knowledge Management in Supply Chain : Fuzzy DEMATEL approach." IEEE Technology Management Council. Singapore Chapter, IEEE Singapore Section, IEEE Systems, M., and Institute of Electrical and Electronics Engineers. (n.d.). *2012 IEEE International Conference on Industrial Engineering and Engineering Management : IEEM2012 : 10 to 13 December 2012.*

Von Skarczinski, B., Boll, L., and Teuteberg, F. (2021). Understanding the adoption of cyber insurance for residual risks - An empirical large-scale survey on organizational factors of the demand side. *European Conference on Information Systems (ECIS)*, pp 1–19. 2021.

Woods, D., and Simpson, *A. Policy measures and cyber insurance: a framework*. Journal of Cyber Policy, vol. 2(2), pp 209–226, 2017.
https://doi.org/10.1080/23738871.2017.1360927.

## Biographies

**Subinoy Banerjee** is a Research Scholar in the field of Information Systems at Vinod Gupta School of Management, Indian Institute of Technology Kharagpur, India. In addition, he gained fifteen years of Industry Experience in various leading IT Industries including IBM. His research interests are in the fields of information security, cyber security, cyber insurance, risk management, etc.

**Saini Das** is an Assistant Professor at Vinod Gupta School of Management, Indian Institute of Technology Kharagpur, India. She has served as a faculty member at IIM Indore for three years before joining IIT Kharagpur. She also worked as a software engineer at Infosys Technologies Ltd. prior to her PhD. Her major teaching interests and competencies are in the areas of business analytics, information security risk management in networks, management information systems (MIS), e-commerce technology and applications, data privacy and digital piracy. Prof. Das has taught in many management development programs across industries. She has authored papers in many national and international journals of repute.