

# Supplementary Information for Manuscript: “How can risk networks support modern risk management: Risk Classification, Identification and Emerging Risks”

Christos Ellinas<sup>1,2,3,\*</sup>, Neil Allan<sup>2</sup>

<sup>1</sup>Engineering Mathematics, University of Bristol, Bristol, UK

<sup>2</sup>IDC in Systems, University of Bristol, Bristol, UK

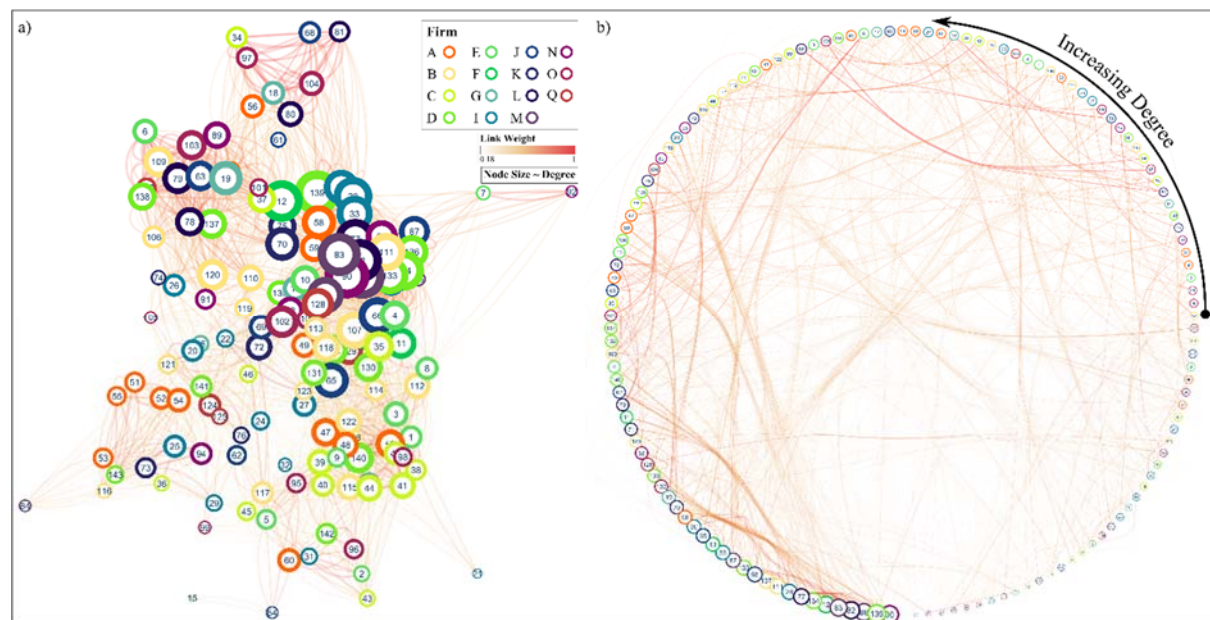
<sup>3</sup>Stevens Institute of Technology, USA

\*Corresponding author

E-mail: [ce12183@bristol.ac.uk](mailto:ce12183@bristol.ac.uk)

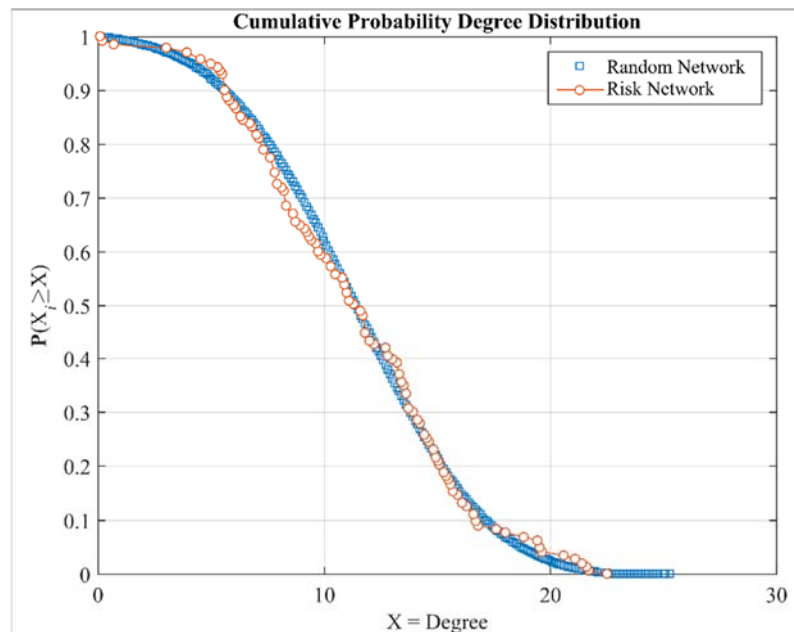
## 1. Visualization and degree distribution of the Risk Network

A typical risk network derived from risk generation process is shown in Figure 1SI, where node colour corresponds to the firm who has identified the respective risk, and node size corresponds to the sum of all weighted links. As such, larger nodes correspond to increasingly connected risks. The degree distribution of the network is also provided in Figure 2SI, in the form of a cumulative probability plot.



**Figure 1SI:** (a) and (b) correspond to different layouts of the risk network, where node size and colour correspond to the weighted sum of connections and the firm that has identified that risk, respectively. Lastly, node label corresponds to the risk id.

The degree distribution of the risk network is also provided in Figure 2SI, in the form of a cumulative probability plot. This degree distribution is well-approximated by normal distribution, suggesting that the underlying topology of the risk networks resembles that of a random network.



**Figure 2SI:** Cumulative probability degree distribution of a risk network (red) and its random counterpart (blue).

## 2. Decomposition of risks contained in Module 3

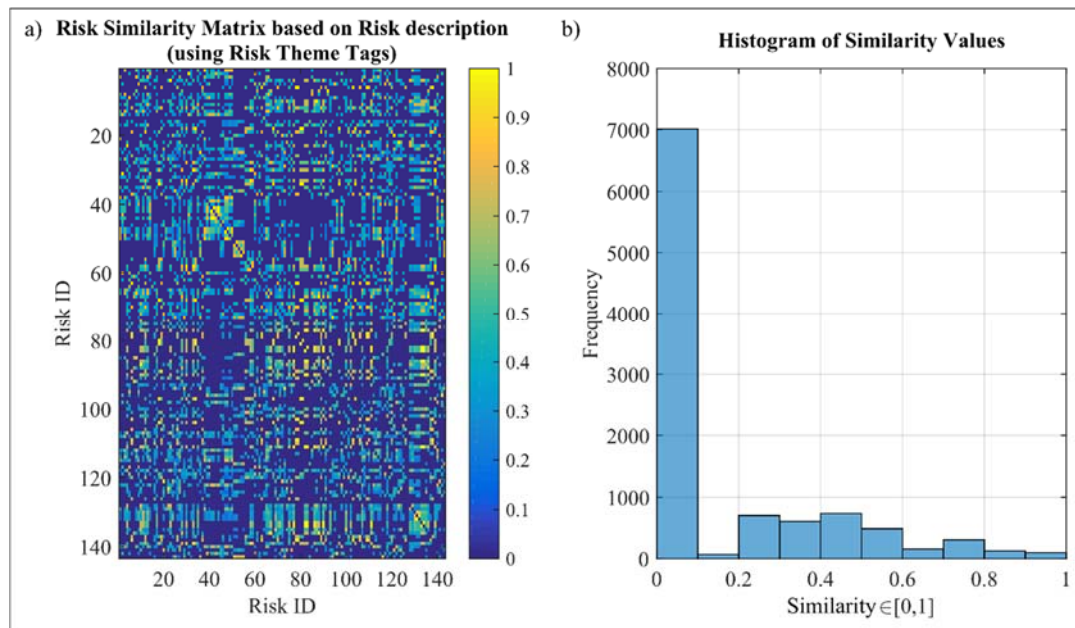
The composition of Module 3 is visualised in the form of a word cloud, where the name of each risk is broken down into single words, and subsequently used to visualise its frequency of occurrence. This is done by linking the frequency of each word with its font size. The dominance of words such as “Cyber”, “Technology”, “Digital” and “New” highlights the cyber-theme nature of Module 3.



**Figure 3SI:** Word cloud of the names of risks found within Module 3, where font size corresponds to the frequency by which each word occurs.

### 3. Similarity Matrix

The similarity between any two risks is stored in a symmetric matrix  $\mathbf{S}$ , which we refer to as the Similarity matrix. Each  $\mathbf{S}(i,j)$  entry corresponds to the similarity between risk  $i$  and  $j$  and can range from 0 to 1, corresponding to no similarity and perfect similarity respectively. Figure 4SI(a) visualises matrix  $\mathbf{S}$ , with Figure 4SI(b) plotting the frequency of values, in the form of a histogram. Note the dominance of 0 entries, highlighting the sparse nature of the matrix, where the majority of risks have limited similarity.



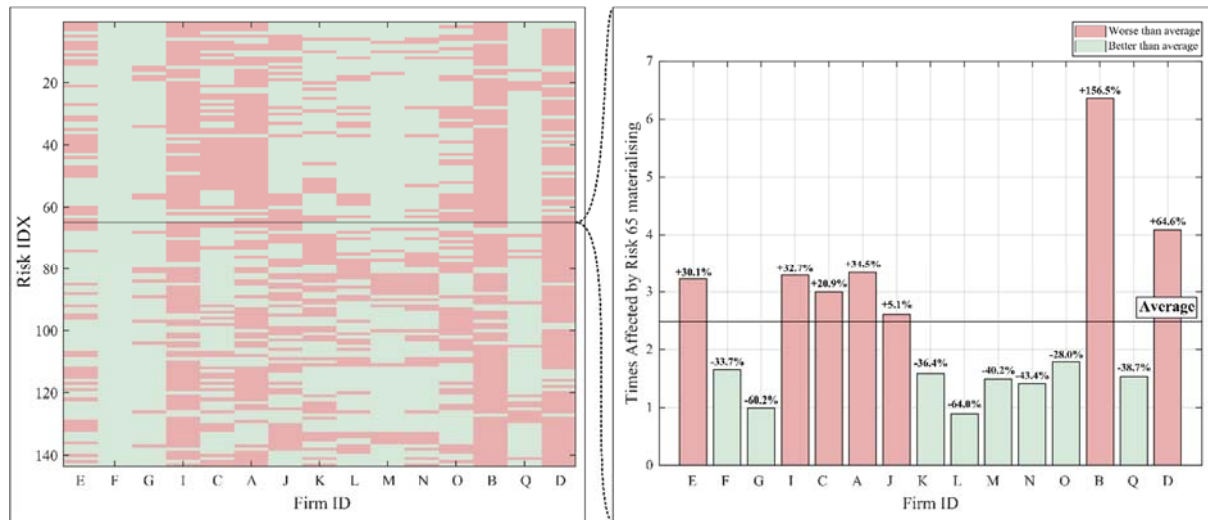
**Figure 4SI:** (a) Similarity Matrix  $\mathbf{S}$ , where each  $\mathbf{S}(i,j)$  entry corresponds to the similarity between risk  $i$  and  $j$  (see colour bar); (b) histogram of similarity values.

### 4. A word of caution

Consider the case where a risk materialises, and subsequently triggers more risks. Figure 5SI, left panel highlights whether a firm has felt the systemic impact of a particular risk materialising (y-axis) more or less than the average, corresponding to green or red bar respectively. These results suggest an intriguing paradox: the firm that reports a given risk is not the one mostly affected by its systemic impact. This is counterintuitive as one would naturally expect that the mere act of reporting a risk is driven by the expectation that its manifestation will impact the firm's operation (1).

For a particular example, consider the case of the most systemic risk – Risk IDX 65. Following its manifestation, its systemic impact is felt by all firms, in terms of subsequent risks triggered (Figure 5SI; Right Panel; y-axis). In particular, the firm that sees the largest number of the risk that is reported, materialising, due to Risk IDX 65 is Firm B; the one with the least is Firm L. Yet, neither of these two firms is the one that actually reported this risk i.e. Firm J. However, additional analysis indicates that this is a mere artefact of noise within the data. In particular, we compute the ratio of the number of

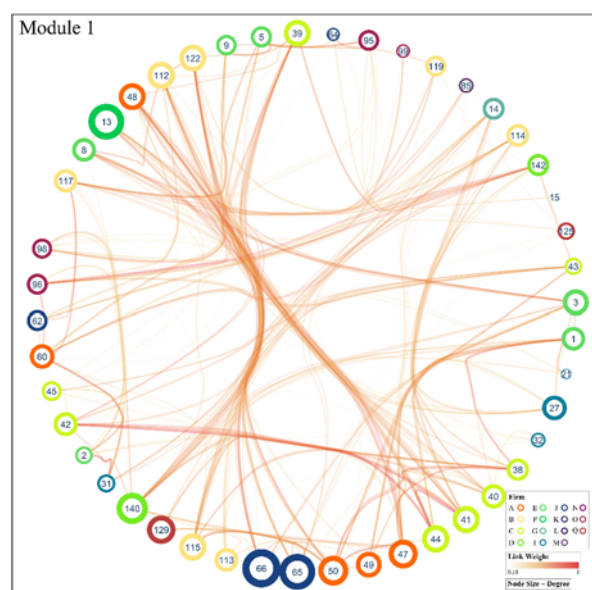
times a firms performs better (green entries) over the number of times it performs worse (red entries). This quantity strongly correlates positively with the number of risks reported by each firm ( $n=15$ ; Pearson Correlation Coefficient=0.827;  $p$ -value=0.000142).



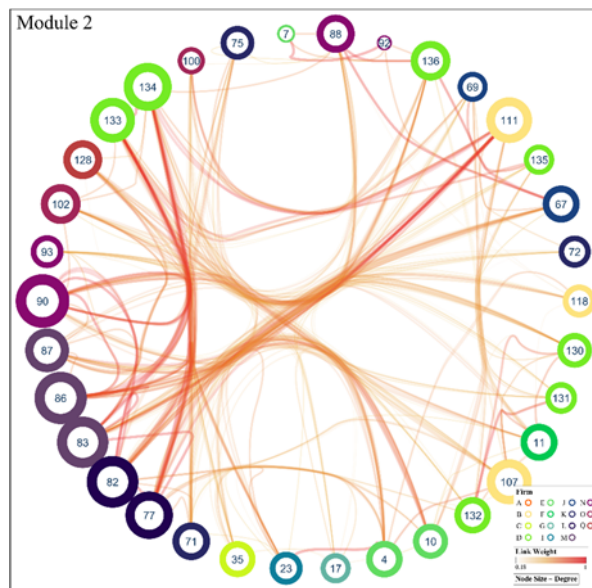
**Figure 5SI:** (Left Panel) Matrix plot where each firm (x-axis) is evaluated in terms of the number of risks that it reported, and have materialised due to a particular risk (y-axis). Entry colour corresponds to whether it performs better (green) or worse (red) compared to the average across all firms; (Right Panel) Number of self-reported risks triggered by the manifestation of the most systemic risk – Risk IDX 65. Results are averaged over 1,000 cases in which a risk network have been generated, and the SI model subsequently applied (see Methods).

## 5. Visualisation for Module 1-5

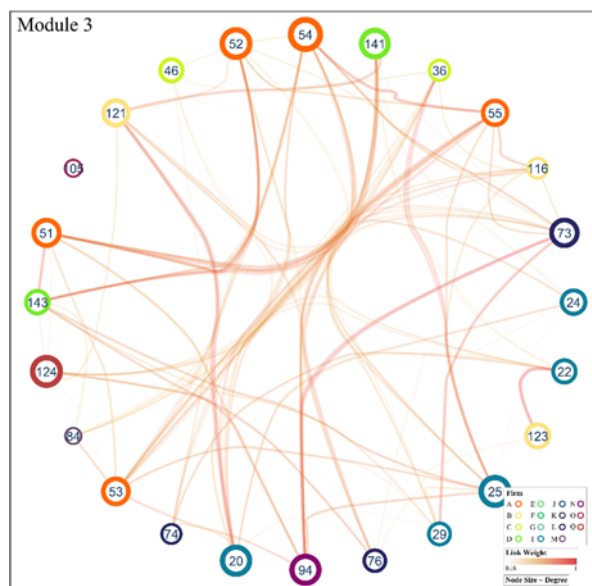
Figure 6SI – 10SI visualise Module 1 – 5 respectively focusing on the connections within each module.



**Figure 6SI:** Module 1 of the risk network

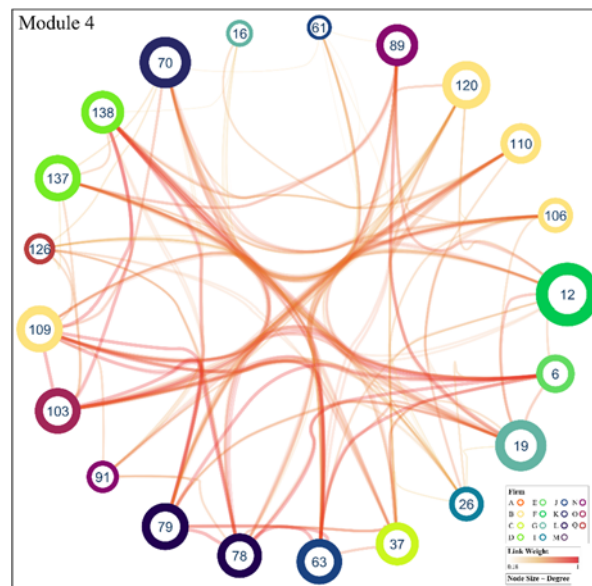


**Figure 7SI:** Module 2 of the risk network

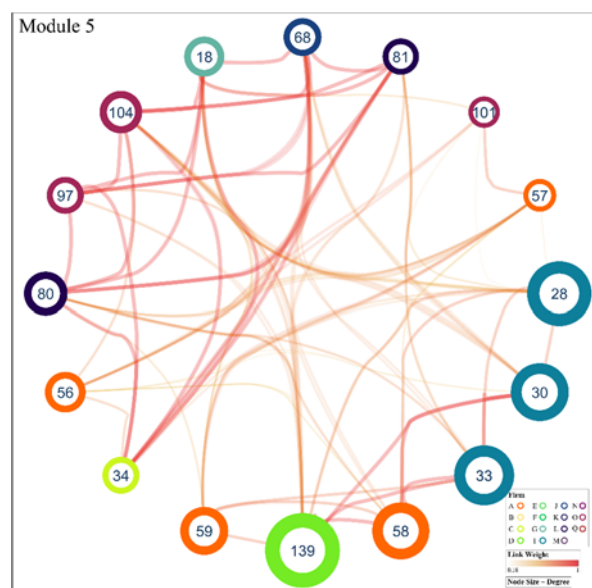


**Figure 8SI:** Module 3 of the risk network





**Figure 9SI:** Module 4 of the risk network



**Figure 10SI:** Module 5 of the risk network

## References

1. ISO. 31000: 2009 Risk management—Principles and guidelines. International Organization for Standardization, Geneva, Switzerland. 2009.