Cybersecurity risk measurement

Silvia Facchinetti
Department of Statistical Science, Università Cattolica del Sacro Cuore, Milano
Paolo Giudici
Department of Economics and Management, University of Pavia, Pavia
Silvia Angela Osmetti
Department of Statistical Science, Università Cattolica del Sacro Cuore, Milano

April 26, 2018

Abstract

This paper proposes a methodology to measure cyber risks, using ordinal data, to prioritise appropriate interventions. The method relies on the construction of a *Criticality index*, whose properties are derived and compared with alternative measures employed in operational risk measurement. The proposed construction is illustrated in the context of a telecommunication service company, a case-study that provides a rather general benchmark. The proposed measure is found to be quite effective to rank cyber risk types and, therefore, allow selective preventive actions.

Keywords: criticality index; operational risks; ordinal variables; cyber attacks.

1 Introduction

Operational risk has been defined, by the Basel Committee on Banking Supervision, as "the risk of a monetary loss caused by human resources, information technology (IT) systems, by organisation processes or by external events". Among operational risks caused by IT systems, cyber risks are gaining increasing importance, due to technological advancements and to the globalisation of financial activities.

Cyber risks can be defined as "any risk emerging from the use of information and communication technology (ICT) that compromises the confidentiality, availability, or the integrity of data or services" (see e.g. [3], [7], [14]).

Financial institutions are encouraged by regulators to use statistical approaches to estimate the capital charge covering operational risk, which include cyber risks. This requires the presence of historical loss data, in a quantitative format. Within this framework, operational risks are usually classified in event types, according to the type of risk involved; and in business lines, according to area of the company that is mostly affected. To measure operational risks, past losses in each business line and event type are collected and, then, the corresponding severity and frequency distributions are calculated. Their convolution, by means of a Monte Carlo simulation, leads to the Value at Risk, which corresponds to the total economic capital required to protect an institution against possible operational losses (see e.g. [6], [2], [10]).

However, besides the regulatory purpose, financial institutions are motivated to measure cyber risk by the need of having under control the quality of their processes, a motivation that applies to non financial institutions as well. In this framework, cyber risk measurement is usually seen as a preventive diagnostics, based on data, expressed in ordinal categories, such as "high", "medium" or "low" risk, rather than in terms of quantitative data.

Ordinal data cannot be used to derive the total economic capital required to cover operational risk, as that requires quantitative data but, however, can be used to rank risks by their "criticality", so to prioritising interventions and, therefore, trigger mitigating actions.

We remark that cyber events are typically rare and not repeatable, being very specific. It is quite natural, therefore, to measure them with a less demanding ordinal approach rather than using quantitative data which are often not available.

While the literature on the quantitative measurement of operational risks (see e.g. [5], [15]), based on loss data, constitute a reasonably large body, that on cyber risk measurement and, particularly, on ordinal cyber risk measurement, is very limited. To our knowledge, the works on the matter are [11] and [12], that, however, mainly promote measurement methods and discuss about problems occurring with simple scoring methods. A recent paper [1] focus on the problem of the scarsity of available data in this context.

Our contribution tries to fill this gap in the literature, providing a cyber risk measure, based on ordinal data, that can be used to rank cyber risks and, therefore, prioritise interventions.

More precisely, we propose a methodology to measure cyber risks, starting from ordinal random variables, that represent the levels of severity for different risk events, in different business lines. In particular we propose, for each business line and event type, a cyber-security risk index that is based on the relative frequencies of the severity levels. As a result, we obtain an ordinal measure of risk which will be used to compare different events and business lines, producing an ordering among risks useful to prioritise intervention in process controls.

For completeness, we emphasize that our measure bears some resemblance to ordinal measures proposed in other fields. For example, in customer satisfaction, [4] propose ordinal models to assess the perceived quality of academic teaching. In quality control framework [8] propose a priority intervention indicator for measuring the risk of failure of a product or process, when the quality is expressed on ordinal scale. Last, [9], propose a stochastic dominance nonparametric measure of operational risk, that is also suited for ordinal variables. For this reason, in the paper we also apply the measure proposed by [9] to cyber risk measurement and compare it to our proposal.

Besides the theoretical proposal, we will present empirical evidences on the performance of our index, using a real data set, that concerns cyber risk measurement in a telecommunication company. This is a very general and interesting benchmark, which can easily be generalised to other industries.

The paper is organized as follows. The next section contains our methodological proposal: the definition of the criticality index and its properties. Section 3 contains the application of the index to the telecommunication data. Finally, the last section contains some concluding remarks.

2 Proposal

In this section we present our methodological proposal for the measurement of cyber risks. Data for cyber risk measurement is typically summarised in a matrix, composed of I event types (the columns of the matrix) and J business lines (the rows of the matrix).

Let E_{ji} be a risk event, in the j-th business line ($j = 1, \ldots, J$) and in the i-th event type ($i = 1, \ldots, I$). For each combination of event type and business line, two different measures of risk are usually considered: the frequency (how many risk events have appeared in that combination) and the severity (the mean loss of the events in that combination).

In the loss data framework, the severity is a continuous random variable, while in the context of ordinal risk data, the severity is generally expressed in an ordinal scale, characterised by K distinct levels, ordered according to the corresponding magnitude: for example $K = 3$, with H=high severity ($k = 1$); M=medium severity ($k = 2$) and L=low severity ($k = 3$). To summarise the frequency and the severity in a summary measure, we may structure a loss contingency table, which counts, for each combination, how many people expect that (the frequency).

More formally, let r_{1ji}, r_{2ji} and r_{Kji} be the number of times for which high, medium or low severity occur for the event type $i = 1, \ldots, I$ in the $j = 1, \ldots, J$ business line.
These frequencies can be reported in a contingency table composed of J rows, representing the business lines $(BL_1, \ldots, BL_J)$ and $I \times S$ columns, equivalent to the number of event types multiplied by the levels of severity K under analysis (in our example three: high=H, medium=M and low=L). Each cell in the table contains the frequency of a combination of business line (row) and event type*severity level (column). Table 1 exemplifies what just described.

Table 1 about here

	ET_1			$\dots$	ET_i			$\dots$	ET_I		
	H	M	L		H	M	L		H	M	L
BL_1	r_{111}	r_{211}	r_{311}	$\dots$	r_{11i}	r_{21i}	r_{31i}	$\dots$	r_{11I}	r_{21I}	r_{31I}
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
BL_j	r_{1j1}	r_{2j1}	r_{3j1}	$\dots$	r_{1ji}	r_{2ji}	r_{3ji}	$\dots$	r_{1jI}	r_{2jI}	r_{3jI}
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
BL_J	r_{1J1}	r_{2J1}	r_{3J1}	$\dots$	r_{1Ji}	r_{2Ji}	r_{3Ji}	$\dots$	r_{1JI}	r_{2JI}	r_{3JI}

Table 1: Cybersecurity contingency table

The measure we propose is based on the cumulative distribution function of the severity variable, conditionally to a specific combination of business line-event type. Before deriving the measure, we remark that, for ease of notation, in what follows we omit the indices j, i from the subscript of the frequencies r_{kji}.

For the j-th business line and the i-th event type, let $X \sim \{x_k, p_k; k = 1, 2, \dots, K\}$ be a categorical random variable with ordered categories x_k and probabilities $p_k = P(x_k)$, that represents a severity variable, with decreasing levels, $k = 1, 2, \dots, K$. We denote the parametric space of X as $\mathcal{P}_{K-1} \equiv (p_1, p_2, \dots, p_k, \dots, p_{K-1})$, $\sum_{j=1}^{K-1} p_k \leq 1$ and $p_K = 1 - \sum_{k=1}^{K-1} p_k \geq 0$.

Let $U \sim \{u_k = k, p_k; k = 1, 2, \dots, K\}$ be a discrete stochastic variable corresponding to X, with parametric space $\mathcal{P}_{K-1}$.

We define a *Criticality Index* for the categorical random variable X with the following expression:

$$I = \frac{1}{K-1} \sum_{k=1}^{K-1} (K-k) p_k = \frac{\sum_{k=1}^{K} F_k - 1}{K-1}, \tag{1}$$

where $F_k = \sum_{l=1}^{k} p_l$ are the values of the cumulative distribution function of U, for $k = 1, 2, \ldots, K$.

The index is based only on the cumulative probabilities of the ordinal variable X, and it is a natural measure of risk for ordinal variables, with values in $[0, 1]$. It thus provides a risk measure with extreme values that are univocally defined and intermediate values expressed as percentages.

We also remark that the lower and upper bounds of the measure occur in the two situations of minimal heterogeneity. In particular, $I = 0$ occurs when the risk event does not appear or it is concentrated only on values with lowest severity ($p_K = 1$ and $p_l = 0$ for $l < K$). $I = 1$ occurs when the risk event is concentrated only on values with highest severity ($p_1 = 1$ and $p_l = 0$ for $l > 1$). Note also that, in the case of maximum heterogeneity, when the frequencies of the event type in a business line are equal for all levels of severity, we obtain that $I = \frac{K+1}{2}$, a sort of mean value, that corresponds to a uniform distribution.

The described properties of the index make it natural to interpret and easy to use for the comparison of the risk level between different risk events and/or business lines.

We propose to estimate cybersecurity risk in each business line/event type combination by the sample version of the *Criticality Index*, obtained by replacing the probabilities p_k with their estimators $\hat{p}_k = r_j/n$.

More formally, the cybersecurity in a specific combination will be estimated by the following, for $k = 1, 2, \ldots, K-1$:

$$\hat{I} = \frac{1}{K-1} \sum_{k=1}^{K-1} (K-k) \frac{r_k}{n} = \frac{\sum_{k=1}^{K} \tilde{F}_k - 1}{K-1}, \tag{2}$$

where

$$\tilde{F}_k = \sum_{l=1}^{k} \frac{r_l}{n} \quad \text{for} \;\; k = 1, 2, \ldots, K,$$

is the empirical cumulative distribution function, $r_l = \sharp(\tilde{x}_i \equiv x_l)$ is the number of observations in the sample equal to the category x_l, with $r_l \in \mathbf{N}$ and $\sum_{l=1}^{K} r_l = n$ (n is the total number of risk events observed for the i-th event type and j-th business line).

Note that, starting from a matrix of business lines-event type frequencies we can derive a matrix of $\hat{I}$ criticality indicators of risk, one for each combination. Such matrix can be employed to compare the risks in different events of interest and in different business lines, producing an ordering among risks. This may be very useful, from an applied viewpoint, to prioritize and to implement interventions, in a control systems, to prevent failures and to reduce ex-ante the impact of risks.

From a mathematical viewpoint, [8] have derived the statistical properties of the above estimator and have also derived its exact and asymptotic distributions. They showed that the estimator is unbiased, consistent and asymptotically normal distributed: $\hat{I} \sim N(I, Var(\hat{I}))$, with variance

$$Var(\hat{I}) = \frac{1}{n(K-1)} \left[\sum_{k=1}^{K-1} (K-k)^2 p_k (1-p_k) - 2 \sum_{k=1}^{K-1} (K-k) p_k \sum_{l=1}^{k-1} (K-l) p_l \right]. \quad (3)$$

The above finding allows to derive confidence interval risk measures for cyber risk measures based on ordinal data. More precisely, asymptotic $(1-\alpha)\%$ confidence intervals can be obtained as:

$$\hat{I} - h_c \cdot s \leq I \leq \hat{I} + h_c \cdot s$$

where s is the estimator of the standard deviation of $\hat{I}$, obtained replacing p_k with $\hat{p}_k$ in Equation (3) and setting $h_c = \Phi(1-\alpha/2)$.

We remark that it may be necessary to aggregate different event type risks in a single business line or to aggregate different business line risks in a single event type. The proposed measure allows this calculation. Formally, let $\hat{I}_{ij}$ be the sample estimate of the risk index for the i-th event type and for the j-th business line. To aggregate the risks of each event types in a specific business line we can express the overall business line risk as a geometric mean of the risk measures associated with each event type in that business line, as follows:

$$\hat{I}_j = \left(\prod_{i=1}^{I} \hat{I}_{ij} \cdot n_i \right)^{1/I} \tag{4}$$

where n_i are the frequencies of each event type.

Similarly, to aggregate different business line risks in a specific event type, we can express the overall event type risk as a geometric mean of the measure of risk associated with each business line in that event type, as follows:

$$\hat{I}_i = \left(\prod_{j=1}^{J} \hat{I}_{ij} \cdot n_j \right)^{1/J} \tag{5}$$

where n_j are the frequencies of each business line.

The previous expressions show that risks over different units may be assumed to interact in a multiplicative way, as if they were units of an integrated system, and this is consistent with the fact that cyber risks, triggered by one event, typically impact, sooner or later, the whole system.

From a methodological viewpoint, we propose the geometric mean because it is a necessary condition to preserve stochastic dominance ranking when aggregating distribution functions [13]. This is very useful in the context of cyber risk, based on ordinal data.

3 Application

In this section we apply our proposal to real data provided by a telecommunication company that, for brevity, we anonymously call ”T”. T installs telephone exchange systems and offers post-installation technical assistance for upgrading and problem resolution in different event types, that include, in particular, Network communications. The service is offered to a wide range of customers, that are grouped in several business lines.

The main research problem of T is to estimate, for each business line and for each event type, a measure of operational risk, based on ordinal data collected by the customer care center.

To this aim, we were supplied a data set, composed of observations on 1126 customers (PBX systems), whose generating process can be described as follows. A customer from a specific business line calls the customer care of T to signal problems in user experience. Problems which may be triggered by cybersecurity attacks, especially when the event type Network communication is involved. The customer care center operators input to the system a reference to the call, listing the PBX number of the customer and the level of severity of the problem as reported by the customer (high, medium, low).

The structure of the data collected is thus a data base which contains, for each customer, the severity of the reported problems. Note that a single customer could report more then one problem in a given period of time.

We focus our analysis on the event type Network communication as a problem of this kind may likely due to a cyber attack. The considered data can be grouped as in Table 2 below: each row shows a business line and each column reports how many times a Network communications problem has been reported, for levels of severity equal to high (H), medium (M) and low (L). In Table 2 we also report, following expression (1), the estimated *Criticality Index* $\hat{I}$, and the corresponding asymptotic standard error (SE).

Table 2 about here

From Table 2, note that Construction is the business line with the highest level of risk, followed, at a considerable distance, by Defence and Health. Therefore, a mitigation

Business Line	H	M	L	I	SE
Banking	23	128	4	0.561	0.023
Computers	3	26	0	0.552	0.040
Construction	1	1	0	0.750	0.250
Cooperatives	13	93	2	0.551	0.024
Defence	34	149	7	0.571	0.023
Education	0	19	4	0.413	0.056
Electronics	1	14	0	0.533	0.046
Government	0	13	0	0.5	0
Health	43	222	8	0.564	0.018
Hotels	10	108	3	0.529	0.021
Industry	13	94	7	0.526	0.028

Table 2: The *Criticality Index* estimates and the corresponding standard errors for different business lines and the Network communication event type.

intervention to prevent cyber risk should prioritise the construction business line, and the customers in that business line.

We remark that, besides the criticality index, the analysis of its precision, described by the inverse of the standard error, is also very important. Indeed Table 2 indicates that business lines with a low total problem reporting, such as Construction, Education, Electronics and Government are less precise. Note that the standard error of Government is equal to zero since there is minimal heterogeneity for the severity variable.

Furthermore, as discussed in Section 2, the criticality index can be easily aggregated over different business lines. We can, for example, apply the geometric mean to derive an overall measure of risk for the Network communication event type and compare it with the risk of other event types. Doing so, we obtain a value of 0.541, which indicates a ”medium” overall risk. A level that can be compared with that of other event types.

To evaluate the robustness of our results we have compared them with what could be obtained with the approach proposed by [9] in the context of operational risks. We applied their Stochastic Dominance Index (SDI) to our data, and applied their suggested Bayesian procedure to derive a confidence interval, by means of a Gibbs Sampling algorithm with R=10000 interactions.

In Table 3 we report, for the business lines that have at least about 30 reported problems, and for the Network communication event type, our criticality index and its associated asymptotic confidence interval along wiht the SDI value, and the related Bayesian confidence interval.

Table 3 about here

Looking at the results in Table 3, note that our index and the SDI produce a consistent ranking, indicating similar priorities of intervention.

Business line	I	CI	SDI	Bayesian CI
Banking	0.561	0.517-0.606	0.708	0.685-0.728
Computers	0.552	0.473-0.630	0.701	0.654-0.734
Cooperatives	0.551	0.503-0.599	0.701	0.676-0.723
Defence	0.571	0.527-0.616	0.714	0.692-0.735
Health	0.564	0.529-0.599	0.709	0.692-0.726
Hotels	0.529	0.488-0.570	0.686	0.665-0.706
Industry	0.526	0.472-0.580	0.684	0.657-0.711

Table 3: I and SDI risk measure estimates and their respective confidence intervals (CI)

However, the confidence intervals associated with the two indices are different: while I has intervals whose length decreases with the number of problems in the business line, the SDI has similar length intervals. Statistical theory and intuition suggest that interval length should vary with the sample size: the more the data, the more precise the measurement and, therefore, the smaller the confidence interval should be. In this sense, we can say that I is better than SDI.

Indeed, from a mathematical viewpoint, the two indices are calculated in a different way: the SDI is based on the observed frequencies, whereas our proposed *Criticality Index* is based on the observed frequencies, conditional on the total of that business line and, therefore, it more correctly take into account the relevance of the considered business line, and not only the distribution of the severity.

Another advantage of our proposed method with respect to the SDI measure lies in the simpler computation of confidence intervals.

As described in Section 2, when $n \simeq 30$, as is the case for many business lines, is not strictly necessary to apply a Bayesian approach to derive confidence intervals. Bayesian confidence intervals, albeit elegant from a mathematical viewpoint, require Monte Carlo simulations, which are computationally expensive, and also introduce an extra variability due to Monte Carlo sampling. Bayesian confidence intervals may instead be useful for ”rare” problem business lines, for which an asymptotic confidence interval is not possible.

4 Conclusions

We have proposed a novel measure, the *Criticality Index*, which can measure cybersecurity risk, on the basis of ordinal data, that only require a ranking of the perceived risks, rather than a quantitative measure.

The index has nice mathematical properties, and could be easily aggregated by means of a geometric mean. From an applied viewpoint, the confidence intervals that can be built on it reflect the sample size precision contained in the data.

Our proposed measure can thus be employed as a simple and effective measurement to prioritise cyber risk, as our application to the Network communication risks of a telecommunication company has demonstrated.

Further research work involve the application of the proposed method to other cybersecurity contexts and data.

References

[1] Afful-Dadzie, A., and Allen, T.T. (2017). Data-Driven Cyber-Vulnerability Maintenance Policies, Journal of Quality Technology, 46: 234-250.

[2] Alexander, C. (2003). Operational risk: regulation, analysis and management. Prentice Hall, New York.

[3] Cebula, J.J., and Young, L.R. (2010). A Taxonomy of Operational Cyber Security Risks, Technical Note CMU/SEI-2010-TN-028, Software Engineering Institute, Carnegie Mellon University, 1-34.

[4] Cerchiello, P., Dequarti, E., Giudici, P., and Magni, C. (2010). Scorecard models to evaluate perceived quality of academic teaching, Statistica & Applicazioni, 8: 145-155.

[5] Cox, L.A.Jr (2012). Evaluating and improving risk formulas for allocating limited budgets to expensive risk-reduction opportunities, Risk Analysis, 32: 1244-1252.

[6] Cruz, M. (2002). Modeling, measuring and hedging operational risk. Wiley, New York.

[7] Edgar, T.W., and Manz, D.O. (2017). Research Methods for Cyber Security, Elsevier.

[8] Facchinetti, S., and Osmetti, S.A. (2018). A risk index for ordinal variables and its statistical properties: a priority of intervention indicator in quality control framework, Quality and Reliability Engeneering International, In press.

[9] Figini, S., and Giudici, P. (2013). Measuring risk with ordinal variables, Journal of Operational Risk, 8: 35-43.

[10] Giudici P. (2003). Applied data mining for business and industry. Wiley, New York.

[11] Hubbard, D.W., and Seiersen, R. (2016). How to Measure Anything in Cybersecurity Risk. Wiley, New York.

[12] Hubbard, D.W., and Evans, D. (2010). Problems with scoring methods and ordinal scales in risk assessment, Journal of Research and Development, 54: 2-10.

[13] Jean, W.H. (1980). The geometric mean and stochastic dominance, Journal of finance, 39: 527-534.

[14] Kopp, E., Kaffenberger, L., and Wilson, C. (2017). Cyber Risk, Market Failures, and Financial Stability, IMF Working Paper WP/17/185, 1-35.

[15] MacKenzie, C.A. (2014). Summarizing Risk Using Risk Measures and Risk Indices, Risk Analysis, 4: 2143-2162.