A New Approach to Improve Accuracy in Information Security Risk Management

Víctor Leonel Orozco López, Raul Ceretta Nunes
Computer Science Graduate Program (PPGI)
Federal University of Santa Maria (UFSM)
Santa Maria, RS, Brazil
e-mail: vlopez@inf.ufsm.br, ceretta@inf.ufsm.br

***Abstract*—Risk management constitutes a basis for decision making in a business continuity plan, since it creates a view that allows to identify and control risks that can compromise the assets of a given organization. Despite the existence of several methodologies to estimate the severity of these threats, preview evidence has demonstrated that the presence of human data sources for risk analysis can produce biased results, thus compromising the business continuity as a result of wrong-guided investments. In this work, we present an approach that reduces human biases by weighting risk evaluations using a reliability level of the sources, based on risk treatment performance. The experiments showed that the usage of reliability scores can effectively increase the accuracy of risk estimation, becoming a tool to minimize and/or eliminate those data sources that provoke the deviation of risk assessment results.**

Keywords–Business continuity; security; risk assessment; accuracy; decision making

I. INTRODUCTION

Business continuity management is a tool aimed to guarantee the delivery of services in presence of risk expositions. To achieve its goals, it requires the creation of a business continuity plan that describes strategies to control risks by mitigating their causes, effects and also ensuring the existence of contingent measures to reduce the impacts of catastrophic events [1].

Within the context of information security, the standard ISO 27005:2011 proposes the implementation of a risk management process that can be applied as a part of a business continuity plan [2], the main objective of which is to establish, prioritize and control those activities regarding to risks, enabling a balance between risk mitigation costs and risk mitigation actions.

One of the most important phases into a risk management program is the risk assessment phase, because the information generated at this stage guides all actions regarding to risks. The risk assessment phase is usually framed in two categories: quantitative risk assessments and qualitative risk assessments [3]. The last category has a significant prevalence because of the practical considerations in analysis and manipulation of data. Nevertheless, quantitative assessment claims for deterministic data. Thus, it is very common to map expert opinions to numerical values in terms of probabilistic functions [4].

Although the usage of expert opinions can provide information not perceptible with other sources, the data by itself could present biases due the subjective nature of human judgment [5], which in the context of information security means that security risks are wrongly estimated, leading to wrong investment and treatment actions.

To counteract this situation, this paper presents an iterative and incremental approach to improve the accuracy in risk assessments. Under the hypothesis that it is possible to establish the reliability score of a human opinion, we assume that reliability could be used to emphasize more reliable opinions, and propose a new approach to improve the performance of the resultant risk priorities.

For the measurement of the reliability levels, our work uses a combination of personalized views of trust and performance metrics as reputation, reducing the consequences in each risk assessment by refining the trust with updates based on risk treatment performance.

The rest of this paper is organized as follows. Section II introduces fundamental concepts for the scope of the paper and related work. Section III presents the approach for the increment of risk assessment accuracy. Section IV presents the experiments and results. Finally, Section V presents the conclusions of this work.

II. BACKGROUND

A. Risk management with ISO 27005:2011

The ISO 27005:2011 risk management process is composed by eight phases that aim to define, estimate and control those risks that threaten the assets of an organization [2].

In a regular implementation of the standard, the process is executed following this sequence: first, the scope of the risk management is defined by the context definition phase; second, the risks are identified, their priority is estimated and the actions to counteract them are defined in the risk assessment phase; third, a decision is made to define which risks will be mitigated and which others will be assumed, inside the treatment and acceptance phases; then all the decisions and actions are communicated to all stakeholders, implementing also a monitoring and review phase. This cycle is repeated if the default time period between risk assessments has expired or if the risk indicators are not presenting satisfactory results, where the decision to start another cycle is dependent on the policy of each organization.

B. From risk divergences to risk biases

Since the standard ISO works as a code of practice, a variety of methods has been developed for each of its phases, and in phases like risk assessment these differences can lead to divergent results between methods. Then, aiming to create a representative result between a set of methodologies, Amaral et al. [5] proposed a composition of common assessment methods. The creation of this composition achieved a

 ISBN: 978-1-61208-324-7

promissory normalization between the results of the methods, and it also evidenced that the results of risk assessments can be biased by the source of data, which in the case of the methods on the composition -Information Security Risk Analysis Method (ISRAM) [6], Austrian Risk Management Approach (ARIMA) [7], Failure Mode and Effect Analysis (FMEA) [8] and Automated Risk and Utility Management (AURUM) [9]- are interviews with experts, who had different background and competences that consequently led to biased risk opinions.

Although the selection of fully deterministic sources seems as the shortest path to eliminate biases, there are situations where is not possible to establish a "hard data source", mostly because of lack of historical data regarding to risks. So, given the existence of environments where these opinions cannot be discarded, one way to affirm that the opinions are reliable depends on the expert himself, since the opinion generated by reliable origins is deemed as reliable [10].

However, the possibility to use the reliability of an expert inside its community, i.e., its trust score in relation to others is non-trivial. In fact, trust as a computational concept requires complex models with techniques like direct measurements, simple reputation models and recently social networks analysis [11].

C. Related works

The model presented by Workman [12] suggests that most of the security decision making literature is focused in situational factors, but it does not considers the biases that could affect these factors, suggesting that biases are a non solved research problem that needs more studies.

In the same context Banerjee [13], tries to reduce the biases by modifying the perceived scale of risks, based on the hypothesis that risk perceptions have a logarithmic behavior instead of linear, adjusting the mediocrity line of perceived risks.

With a managerial approach, Primão et al. [14] focuses the reduction of biases by using a controlled selection of risk assessment participants based on skills, using a contextualized definition of the required competences to be a risk assessment participant.

Focused on smart grids, Lopez et al. [15] proposes an alert mechanism that supervises patterns of behavior of the systems that belong to the smart grid. This mechanism generate alerts to trigger human actions, and most importantly, it assigns responsibilities for those actions by reputation scores. It recognizes the existence of individuals with different competences, using to construct the reputation with variables like feedback, criticality of the alert, operator's workload and the time of response for the incident.

Finally, Khambhammettu et al. [16] presents a framework for risk assessment in access control systems, which focus their contributions on making authorization decisions by comparing security risks for access requests based on a four dimensional approach: object-sensitivity, subject-trustworthiness and two additional scopes combining sensitivity and trustworthiness.

This work differs from them by the following reasons: i) It presents an approach that improves accuracy by reducing biases with reliability; ii) It does not require a selection of participants of risk management based on skills; iii) It does not reconfigure the perception scales; iv) Since the reputation is context dependent, this work uses specific variables from risk management context; v) It presents a reliability based approach that can use diverse sources of initial trust.

III. Risk management with improved accuracy

A. Hypothesis and big picture

Considering that is possible determine the reliability level of a person within an organization, this approach uses this reliability to improve the accuracy of risk management by emphasizing the opinions of those members with higher reliability. The approach is built upon the fact that trust and risk are closely related concepts, because trust is the disposition that a person has to rely on another person's opinions in relations that involve risks; namely a parameter that explains the ability of a person to estimate the risks severity in front of possibilities of deceptions and bad results [17].

To determine and use the reliability levels previous works were adapted, modifying their characteristics and introducing a social network analysis element as shown in Figure 1, that has as basis the work of Amaral et al. [5] in which the problem appeared.

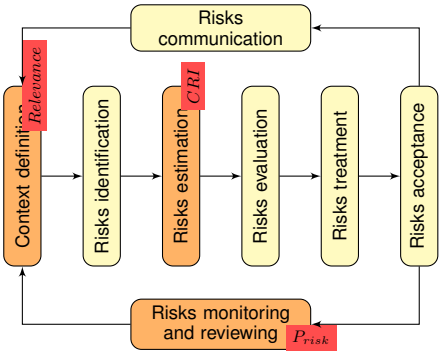

Figure 1. Trust based risk assessment.

This new version of the cycle uses the trust between members of the organization to determine the reliability of a person. For that, it is used an algorithm originally designed for recommender systems called TrustWebRank [18] adapting it to the risk assessment characteristics by remodeling its update function and presenting a global metric of reliability based on [19] ideas, denominated $Relevance$.

Once the $Relevance$ value is calculated, it is introduced into the risk assessment composition using a mathematical weight approach. This approach was selected because it overpasses the performance of other complex approaches while generating equivalent results [4]. From here, a coefficient that indicates the priority of a risk is obtained, denominated Composite Risk Index (CRI), that now reflects the evaluators reliability and is used to guide the investments.

To monitor and review the performance of the treatments, this approach uses Key Risk Indicators (KRI), present in many popular risk management methodologies like [20], representing instant metrics of risk events (those that facilitate apparition of risks).

 ISBN: 978-1-61208-324-7

Since the apparition of one risk can have multiple factors, the relation between KRI and $Risks$ is considered as many-to-many, thus this approach presents a performance indicator denominated Performance of risk (P_{risk}), based on the KRI benchmark presented by Talbot [21].

B. Interaction between components

For the creation of this approach, the following assumptions were taken: i) The computation of $Relevance$ is executed prior to any analysis activity, and the first execution is achieved using an initial trust in the form of witness information (WI), i.e., the actual trust among peers. Then, the subsequent $Relevance$ values are a product of an aggregation of direct observations (DO), i.e., the performance of subsequent risk management cycles and the original witness information (WI). Both kinds of trust are explained in [22]; ii) The organization structure is represented by an informal social network, conformed by links that represent the interaction between the organization's members who act as agents; iii) The organization is willing to monitor its risk treatment performance to update its trust perception based on results, there is not conspiratorial groups, and the risk management is performed by a risk management committee in behalf of all the peers and organization divisions.

The reliability level given to an agent inside a social network is formally defined as trust centrality, and TrustWebRank computes it based on the feedback centrality, meaning that the direct trust T_{ij} between an agent *i* to the opinions r of an agent *j* can be adjusted by using the trust between neighbors *k* of *i* for the agent *j* and the trust that *j* has for its neighbors *k*, giving as a result an indirect trust value $\tilde{T}_{ij}$.

Although TrustWebRank can be executed in a step-by-step style by every pair of nodes, their creators presented an alternative based on matrixes given by (1), where $\tilde{T}$ represents the matrix of indirect trust values calculated with TrustWebRank, I the identity matrix, β an adjustment factor, and S a stochastic matrix of direct trust normalized values given by (2). The value for β is explained with detail at Section IV.

$$\tilde{T} = (I - \beta S)^{-1} S \tag{1}$$

$$S_{ij} = \frac{T_{ij}}{\sum\limits_{k \in N_i} T_{ik}} \tag{2}$$

Then, to create a global reliability value to use it as weight in risk opinions, the personalized values are collapsed to a global metric $Relevance$ (R). The relevance R_i of an agent i inside the organization structure is defined as the average of the indirect trust values of every agent l that belongs to the group of agents N, where N is the group of agents that have a trust value for i above the threshold $\tau = 0.01$ (as established by [19]). The equation of $Relevance$ is presented in (3).

$Relevance$ value could also be used to select the risk assessment committee members (as it is used in the following sections). Nevertheless, a selection based solely on their trust score is not mandatory.

$$R_i = \frac{\sum\limits_{l \in N > \tau} \tilde{T}_{li}}{|N > \tau|} \tag{3}$$

After the context definition and reliability quantification, the identification phase takes place by using brainstorming techniques between the members of the risk committee. The risks are now evaluated by the members of risk committee giving their opinion about the probability(P), detection(D), frequency(F), impact(I) and severity(S) of each risk using a standardized interview with questions in form of likert scales of five steps (very low, low, medium, high, very high), aiming to map their opinions to numerical values.

Once that opinions were assessed, these are used to create a risk ranking based on priority. This step is achieved by using a variant of the original risk assessment composition, which now considers $Relevance$, as is presented in (4). .

$$\begin{aligned} ARIMA &= ((I + ((P-1) * 0.5)) * 100) * R_i/5 \\ ISRAM &= ((P * I) * 100) * R_i/25 \\ AURUM &= ((P * I) * 100) * R_i/100 \\ FMEA &= ((S * O * D) * 100) * R_i/125 \end{aligned} \tag{4}$$

In this version of the equations, the risk estimations are calculated for each risk using all methods of the composition, and the results are condensed by using (5), where MTR corresponds to methods' total result and Mr to the group of methods used in the composition. Note that a group of MTR values will be generated, with a size of $n_p * n_r$, where n_p corresponds to the quantity of participants in the risk assessment committee and n_r to the quantity of risks

To guide the decision-making process, MTR values are collapsed again to obtain a composite risk index (CRI) for every risk r, where r is given by the average of the group MTR_r that corresponds to the MTR results concerning to the risk r as (6) shows, obtaining as a result a list of CRI useful to sort risks by priority.

$$MTR = \frac{\sum\limits_{m \in M_r} m}{|M_r|} \tag{5}$$

$$CRI = \frac{\sum\limits_{i \in MTR_r} MTR_i}{|MTR_r|} \tag{6}$$

With the introduction of $Relevance$ as a weight, the interval of values for CRI tends to shrink, nevertheless, this condition is ignored because CRI value is used only as a comparator of itself, i.e., index and does not have any other numerical significance. Now, using the CRI values, the assessment committee defines the risks treatment strategy with four possible actions -reduce, avoid, retain and outsource-, existing also a need to define how the performance of these actions will be monitored. For that, a P_{risk} indicator in form of benchmark was created, comparing the ideal state or risk events to their actual state using KRI indicators as the comparable elements.

KRI indicators are instant measures of the status of events that could derive in risks, achieving its goal by capturing several representations of the state of those events between two risk assessment executions. Hence, the P_{risk} indicator for a risk r is modeled as the difference of the average of the group

of values V_{MaxKRI} that contains the greatest value reached by every KRI that has relation with r and the average of the group of values V_{Ideal} that contains the ideal value for every KRI that has a relation with r, presented in (7).

$$P_{risk} = \frac{\sum_{v \in V_{MaxKRI}} v}{|V_{MaxKRI}|} - \frac{\sum_{v \in V_{Ideal}} v}{|V_{Ideal}|} \quad (7)$$

In P_{risk} equation, if the average of V_{MaxKRI} exceeds or equals the average of the ideal state V_{Ideal} means that the risk was treated with good performance and P_{risk} value is positive. But, if the average of V_{Ideal} is above the average of V_{MaxKRI} means that the risk treatment was not enough to reach risk goals and probably the risk needed more investments.

With the measurement of risk treatment performance, it is possible to update the reliability of every participant based on the effectiveness of their opinion -i.e Direct Observations (DO)-. For that, TrustWebRank's equation of utility is simplified as $u_{ij} = P_{Risk}$, where j can be any agent that had an opinion about the risk, i.e., a member of the risk management committee, meaning that the trust of any agent i to the opinion of j is updated based on the results of the opinions of j.

For the purposes of risk analysis, it is desirable a *"slow positive-fast negative"* dynamic of trust, where the increment of trust is a slow process, but the decay in front of losses does not depend on many deception events [23]. This concept is achieved by introducing two trust limits $\kappa = 0.2$ and $\gamma = 0.6$ (established by simulation), a change from the original update intervals of TrustWebRank's function. Equation (8) formalizes the new update function, where $\breve{T}_{ij}$ corresponds to the updated direct trust value.

$$\breve{T}_{ij} = \begin{cases} T_{ij} + (1-\gamma)|P_{Risk}| \\ if\ P_{risk} > 0 \\ T_{ij} - (1-\kappa)|P_{Risk}| \\ if\ P_{risk} \leq 0 \end{cases} \quad (8)$$

IV. Experiments

To state if our proposal effectively increases the accuracy of the risk assessment, we evaluated its performance comparing it to Amaral et.al. [5] approach. Both approaches were evaluated in a testbed to answer the following research questions:

- Does the accuracy of risk management is increased?
- Does the size of the committee represents influence?
- Does the approach reproduces the "slow positive-fast negative" behavior?
- Does the approach works against wrong trust scores?
- Is the initial trust a factor for the effectiveness?

For the execution of the testbed, it was necessary to select fair metrics of comparison and obtain them from a simulation.

A. Simulator

To create a simulation that avoids convergences to ideal but unrealistic results, the simulator combines a set of random but parameterizable generators for the trust between peers, treatment performance and risk opinions with a network generator algorithm. The architecture is detailed at Figure 2.

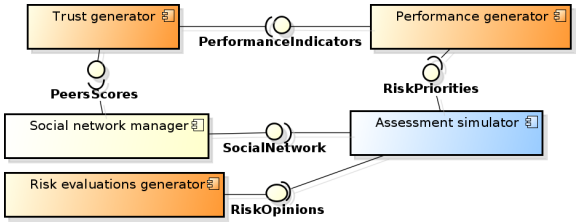

Figure 2. Simulator components

By using Kleinberg's small world algorithm [24] implemented with JUNG [25], the social network manager represents organizations' structures as social networks, selected due its usage of power-law distribution, commonly accepted as a good representation of real world social networks.

The generators of trust scores, performance metrics and the risk opinions were designed in a form that avoids any direct influence over the results using *profiles*, sets of intervals which represent sets of values that correspond to common conditions for every element of the simulation (behavioral profiles for trust scores, criticality of risks for risk evaluation and gain/loss profiles for risk treatments). The corresponding intervals of values for every profile are detailed at Table I.

TABLE I. Intervals of simulation profiles

Category	Profile ID	Interval
Trust profile	KNOWN	[0,0.3)
	COMPANION	[0.3,0.6)
	FRIEND	[0.6,1]
Risk evaluation profile	RANDOM	[very low, low, medium, high, very high]
	SECONDARY	[very low, low, medium]
	CRITICAL	[high, very high]
Performance profile	GOOD	[0,0.5)
	BAD	(-0.5,0)

B. Evaluation criteria

To achieve the creation of a fair testbed, we selected some indicators from CIS [26] as base of comparison, specifically those that have direct relation to risk management and can be adequately represented by simulation.

Incidents quantity. A high-priority risk that falls outside the first third of priorities is considered as incident due its likeness to receive few investments.

Cost of incidents. For illustrative purposes a fixed value of $ 1000 is attributed to every incident.

Time from discovery to containment. Represented as the number of steps to reach a zero value for $Relevance$, indicating the ability to discard bad opinions.

Also, to enhance the elimination of tendentious results, the simulator was configured to represent the following structure:

1) Social network size: 50 agents;
2) Risk assessment committee size: 10 agents;
3) Quantity of risks: 15 risks.
4) Priority of risks: 3 CRITICAL risks (r_1, r_2, r_3), others considered as SECONDARY risks;
5) Trust profiles: 2 agents with FRIEND profiles, others considered as COMPANION agents;

 ISBN: 978-1-61208-324-7

C. Preliminary simulations for trust dynamic

In order to define proper values for the control parameters described at section III-B, the simulator was configured to minimize the influence of relevance, treatment performance and risk estimations by producing fixed values. Latter, the simulator executed 10 continuous risk management cycles for 10 different values for each of the control parameters (γ, κ and β), using 0.1 as the distance between the evaluated values, obtaining the results presented in Figures 3, 4 and 5, which present the relevance of the risk committee participant with the higher initial trust value.

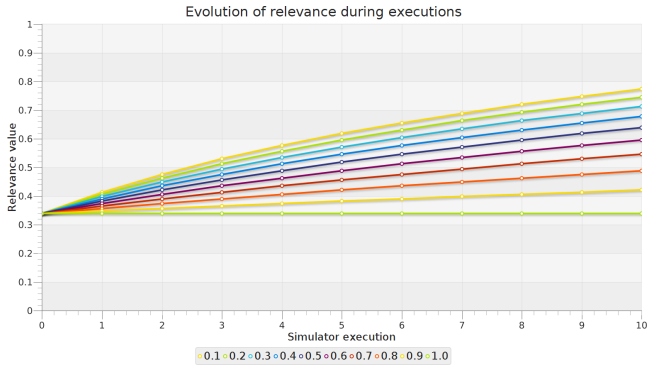

Figure 3. Relevance scores for different γ values

Figure 3 presents the evolution of relevance for γ. In this simulation, while larger is the value of γ, lower will be the speed with which the coefficient of relevance increases, reaching a point where there is no increase in the case that $\gamma = 0.1$. It can also be observed that the original value of TrustWebRank $\gamma = 0.6$ is located at an intermediate point between a rapid increase of trust and a lack of confidence trust, so it is conserved.

Figure 4. Relevance scores for different κ values

Figure 4 presents the evolution of relevance for different κ values. It is observed that while larger is the value of κ, lower is the decrement of relevance. Considering that a fast decrement of trust is desired to penalize wrong opinions, a value of $\kappa = 0.2$ was selected. With this value, it is possible to discard wrong opinions at the fourth execution, observing also a minimum relevance on third execution. This value was selected instead of $\kappa = 0.1$ to give a little margin for future modifications.

Finally, Figure 5 presents the evolution of relevance for

Figure 5. Relevance scores for different β values

different β values. Unlike the previous simulations, the increase of β does not create an uniform variance of relevance. Is also noted that while most β values on the range [0,0.6] have similar behavior, those starting from $\beta = 0.7$ present a significant increment, being observed an intermediate value at $\beta = 0.8$ and an extreme value at $\beta = 0.9$. In consequence the $\beta = 0.8$ was selected.

D. Trust weight impact

Since the bias which affects the accuracy is caused by the proportion between good and bad opinions, this test aimed to state if the proportion between good risk evaluators and the committee size has an impact on the effectiveness. The simulator was configured to represent a bias like good opinions that are neglected by its proportion in relation to the total of opinions. Therefore, the simulations reproduced an assessment where the risk r_1, r_2 and r_3 are rated CRITICAL only by the agents with FRIEND profile, and as SECONDARY by the rest of the committee members; setting all other risks with a SECONDARY profile for all of the committee members.

With these parameters, we evaluated committees of different sizes from 6 to 18 members, testing 50 different graphs for every committee size; considering as a representative value of every size the sum of the incidents on all structures. Table II shows the results for two reliable opinions and Table III for four reliable opinions.

TABLE II. RISK COMMITTEE SIMULATIONS WITH TWO RELIABLE OPINIONS

Committee Size	Incidents Qty.	Est. Value	Incidents Qty. w/Trust	Est. Value w/Trust	Trust/ Original
6	22	$22,000.00	18	$18,000.00	0.82
7	25	$25,000.00	13	$13,000.00	0.52
8	26	$26,000.00	18	$18,000.00	0.69
9	34	$34,000.00	29	$29,000.00	0.85
10	38	$38,000.00	20	$20,000.00	0.53
11	37	$37,000.00	27	$27,000.00	0.73
12	37	$37,000.00	37	$37,000.00	1.00
13	47	$47,000.00	28	$28,000.00	0.60
14	48	$48,000.00	30	$30,000.00	0.63
15	52	$52,000.00	38	$38,000.00	0.73
16	45	$45,000.00	47	$47,000.00	1.04
17	56	$56,000.00	42	$42,000.00	0.75
18	48	$48,000.00	42	$42,000.00	0.88
	Total incidents Value	515 $515,000.00	Total incidents Value	389 $389,000.00	

From Table II, it can be observed that the relation *reliable agents/total agents* has a proportional influence on the

TABLE III. RISK COMMITTEE SIMULATIONS WITH FOUR RELIABLE OPINIONS

Committee Size	Incidents Qty.	Est. Value	Incidents Qty. w/Trust	Est. Value w/Trust	Trust/ Original
6	1	$1,000.00	0	$0.00	0.00
7	1	$1,000.00	0	$1,000.00	0.00
8	1	$1,000.00	0	$0.00	0.00
9	4	$4,000.00	1	$1,000.00	0.25
10	5	$5,000.00	0	$0.00	0.00
11	7	$7,000.00	2	$2,000.00	0.29
12	6	$6,000.00	1	$4,000.00	0.17
13	6	$6,000.00	4	$1,000.00	0.67
14	7	$7,000.00	2	$6,000.00	0.29
15	12	$12,000.00	7	$5,000.00	0.58
16	15	$15,000.00	5	$8,000.00	0.33
17	14	$14,000.00	8	$7,000.00	0.57
18	12	$12,000.00	6	$4,000.00	0.50
	Total incidents Value	91 $91,000.00	Total incidents Value	36 $39,000.00	

effectiveness of good opinions, where the number of incidents grows as the size of risk committee grows. This relation is also replicated by our approach, but it presented better results reaching a reduction of incidents with a relation of 389/515 = 0.76 (24% improvement of accuracy), representing a reduction of $11500 with the defined cost per incident.

In the same line, Table III shows that the increase of the quantity of reliable agents, also increased the accuracy of the assessments, generating a relation of 36/91 = 0.40 (60% improvement of accuracy) that represents an increase of 36% for the effectiveness in relation to the first test.

E. Resistance to bad bootstrap trust

A condition that was evident in the tests of past section is that under undesirable conditions like wrong trust scores between peers, the process can derive in wrong emphasis to opinions that could lead to poor results. Thus, to state the resistance of our approach in front of bad bootstrap opinions, we inverted the agents opinions, meaning that the two agents with FRIEND profile, qualify risks r_1, r_2, r_3 as SECONDARY (wrong qualification) and the other agents that present less $Relevance$, qualify them as CRITICAL (good qualification). Besides this, any other risks opinions were set as SECONDARY.

Figure 6 shows the variation of the $Relevance$ value for 10 consecutive executions over the same graph, presenting the evolution for the whole risk assessment committee. The simulation shown that $Relevance$ values for agent 29 and agent 11 suffered a decline as a consequence of their bad opinions, demonstrating that our process is able to adjust the relevance scores properly. Moreover, is observed that the relevance scores of the wrong opinions reached similar values to those presented by agents with good opinions in the second execution, and they were definitively eliminated at execution four, presenting also a “slow positive-fast negative” behavior.

F. Absence of bootstrap trust

Considering the existence of environments where peer trust measurement cannot be carried out easily, in this test we reconfigured the conditions from the previous section but now setting the trust between peers with a fixed value of 1.

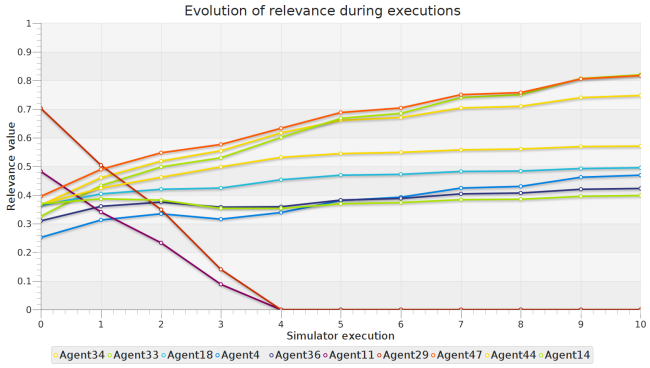

Figure 6. Relevance scores evolution over time

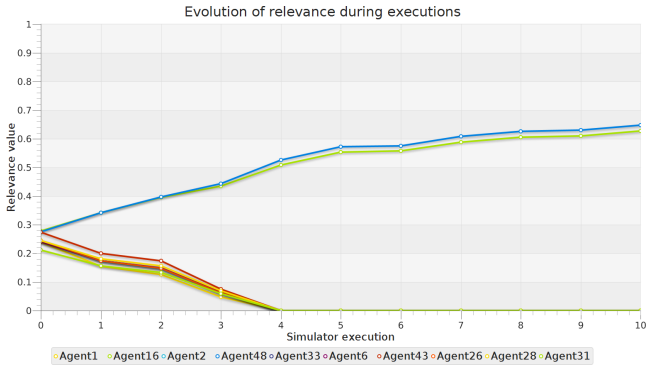

Figure 7. Relevance scores without bootstrap trust

Figure 7 shows that in presence of fixed trust opinions between peers, all agents receive almost uniform relevance values, presenting subtle differences as a product of the social network structure. Despite this, the simulations demonstrated that our procedure is still able to update the relevance scores, based solely on the subsequent events performance.

G. Non-linear evolution

The experiments presented above show that our approach achieves the desired behavior and effectiveness, thus we decided to run a test that considers change of opinions between executions of risk assessments. For this, we took as a basis the conditions presented in Section IV-E, but now, setting the risk evaluations as RANDOM. Generating the results presented at Figure 8.

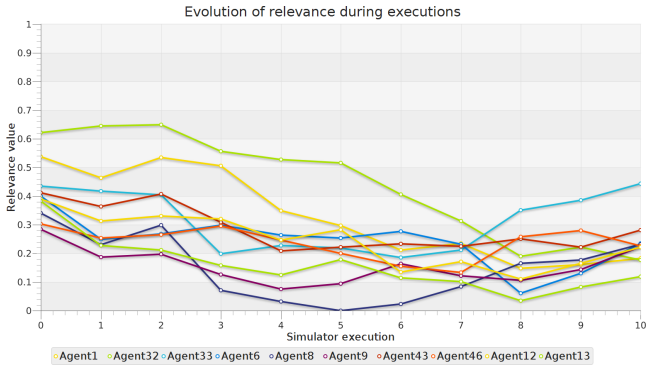

Figure 8. Relevance scores with random changes of opinion

In Figure 8, it can be observed that negative performance results had a greater impact in relation to the positive performance results. However, the results also show that the trust update process managed properly the increases and decreases of trust, where those agents with constant bad opinions like agent 1 and 32 reached the mid section of relevance scores even though they were the peers with high relevance at beginning.

V. FINAL CONSIDERATIONS

In this work, it was evidenced the importance of subjective data and its inconveniences for information security risk assessment methods. The usage of human subjective data can increase the risk computation biases and, consequently, compromise the business continuity.

To reduce the effects of this condition and increase the accuracy of risk management and consequently the business continuity, this work uses reliability as a mathematical weight to qualify human opinions about risks.

Simulation results showed that the emphasis on the reliable risk evaluators increases the accuracy of risk management, where the effectiveness of the approach lies in the relation *reliable agents/total agents*. The evidence showed that the solution has a proportional behavior with respect to the number of good reviews, achieving an accuracy increase of 25% for two reliable evaluators and 60% with four reliable evaluators.

The simulations also showed that the approach is resistant to wrong initial reliability, and the approach can be used without initial reliability scores at all, since the "slow positive - fast negative" update model is able to adjust the reliability.

Until now we have identified only two constraints of this approach. The first one is the absence of an ideal period of convergence for the trust updates, since every organization can have different policies for their risk assessment, i.e., monthly, quarterly, annually, dynamically. However, the simulations demonstrated that the approach can discard bad opinions in less than six executions, and there is a possibility to speed-up the update for good and bad treatments performance, with the κ and γ parameters that control the speed of the update. The second constraint is the fact that the solution executes its updates of trust based solely on performance results (because we aimed a fully independent approach).

In addition to work on the limitations, future works for the creation of more complex notions of trust are planned, to consider other dimensions of analysis like integrity, compliance, competencies, selfishness, reciprocity and others. Furthermore, it is suggested to evaluate the proposal with different trust quantification methodologies and risk assessment models, aiming to support other contexts with different characteristics that are not present on information security context.

REFERENCES

[1] M. Blyth, Business Continuity Management: Building an Effective Incident Management Plan. Wiley, 2009.

[2] ISO, ISO/IEC 27005:2011 – Information technology – Security techniques – Information security risk management, 2011.

[3] T. S. Coleman, A Practical Guide to Risk Management. Research Foundation of CFA Institute, 2011.

[4] R. T. Clemen and R. L. Winkler, "Combining Probability Distributions From Experts in Risk Analysis," Risk Analysis, vol. 19, no. 2, 1999, pp. 187–203.

[5] E. H. Amaral, M. M. Amaral, and R. C. Nunes, "Risk Assessment Methodology by Composition of Methods," in Brazilian Symposium on Information Security and Computer Systems, 2010, pp. 461–473.

[6] B. Karabacak and I. Sogukpinar, "ISRAM: information security risk analysis method," Computers Security, vol. 24, no. 2, 2005, pp. 147–159.

[7] A. Leitner and I. Schaumuller-Bichl, "ARiMA - A New Approach to Implement ISO/IEC 27005," in 2009 2nd International Symposium on Logistics and Industrial Informatics. IEEE, Sep. 2009, pp. 1–6.

[8] D. H. Stamatis, Failure mode and effect analysis: FMEA from theory to execution. ASQ Quality Press, 2003, vol. 38, no. 1.

[9] A. Ekelhart, S. Fenz, and T. Neubauer, "AURUM : A Framework for Information Security Risk Management," SciencesNew York, vol. 0, no. September 2008, 2009, pp. 1–10.

[10] D. Ko, L. Kirsch, and W. King, "Antecedents of knowledge transfer from consultants to clients in enterprise system implementations," MIS quarterly, vol. 29, no. 1, 2005, pp. 59–85.

[11] R. S. Burt, M. Kilduff, and S. Tasselli, "Social network analysis: foundations and frontiers on advantage." Annual review of psychology, vol. 64, Jan. 2013, pp. 527–47.

[12] M. Workman, "Validation of a biases model in strategic security decision making," Information Management & Computer Security, vol. 20, no. 2, 2012, pp. 52–70.

[13] A. Banerjee, "Equivalence of Risk: A Mathematical Approach," in The 29th International System Safety Conference, 2011.

[14] A. P. Primão, R. C. Nunes, and V. L. O. López, "Definition Risk Assessment Committee Based on Competencies," in XII SEPROSUL South American Week of Industrial and Production Engineering, 2012, pp. 1–10.

[15] J. Lopez, C. Alcaraz, and R. Roman, "Smart control of operational threats in control substations," Computers & Security, vol. 38, Oct. 2013, pp. 14–27.

[16] H. Khambhammettu, S. Boulares, K. Adi, and L. Logrippo, "A Framework for Risk Assessment in Access Control Systems," Computers & Security, no. Sec 2012, Apr. 2013, pp. 1–18.

[17] M. Lund, B. r. Solhaug, and K. Stø len, "Evolution in relation to risk and trust management," Computer, 2010, pp. 49–55.

[18] F. E. Walter, S. Battiston, and F. Schweitzer, "Personalised and dynamic trust in social networks," Proceedings of the third ACM conference on Recommender systems - RecSys '09, 2009, p. 197.

[19] J. Chandra, I. Scholtes, N. Ganguly, and F. Schweitzer, "A Tunable Mechanism for Identifying Trusted Nodes in Large Scale Distributed Networks," in 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications. IEEE, Jun. 2012, pp. 722–729.

[20] ISACA, The Risk IT Framework. ISACA, 2009.

[21] M. J. Talbot, How to Performance Benchmark Your Risk Management: A practical guide to help you tell if your risk management is effective. CreateSpace Independent Publishing Platform, 2012.

[22] I. Pinyol and J. Sabater-Mir, "Computational trust and reputation models for open multi-agent systems: a review," Artificial Intelligence Review, vol. 40, no. 1, Jul. 2011, pp. 1–25.

[23] C. Jonker and J. Treur, "Formal analysis of models for the dynamics of trust based on experiences," in 9th European Workshop on Modelling Autonomous Agents in a Multi-Agent World, MAAMAW'99, 1999, pp. 221–231.

[24] J. Kleinberg, "The small-world phenomenon," in Proceedings of the thirty-second annual ACM symposium on Theory of computing - STOC '00. New York, New York, USA: ACM Press, 2000, pp. 163–170.

[25] J. O'Madadhain, D. Fisher, and P. Smyth, "Analysis and visualization of network data using JUNG," Tech. Rep. Ii, 2005.

[26] The Center for Internet Security, "CIS Security Metrics," The Center for Internet Security, Tech. Rep. 28, 2010.

 ISBN: 978-1-61208-324-7