the computer itch

ARTICLE TYPE

Cite this: DOI: 00.0000/xxxxxxxxxx

Are we happy because we don't know?

Author Mariana Ávalos Arce,*[a]
Site https://the-other-mariana.github.io/

1 The FAIR Survey

FAIR Institute conducted the third annual Risk Management Maturity Benchmark survey back in 2019, with the purpose of obtaining insightful information about the current state of risk management from the analysis of the answers given by the survey respondents. FAIR Institute fellow, Jack Freund Ph.D., wrote said insights in the article *2019 Cyber Risk Management Maturity Benchmark Survey Results*[1]. Let's explore this article and analyse the results it presents, hopefully providing some new discussions and the reasons behind said numbers.

2 The Sample

The survey respondents play a central role behind the data presented in Freund's article[1], mainly because the sample is one of the broadest concerns in any statistical matter[3]. In this case, the respondents sample consisted of 211 individuals who were, at the time of the survey, part of an organization that wanted to partake on this study. One of the key factors in determining the conlcusions of the survey were the type of role these respondents had in the organization: the main job title in the sample was something related to Cyber Security Specialist, which represented the 20% of the answers, followed by Risk Officer (18%) and Risk Analyst (14%). As a side note, C-Level Executives were only 5%. For context, more than half of the respondents worked for organizations with more than $B of annual revenues, with Finance being the most common industry (30% of respondents), followed by Technology and Healthcare with 11% of the sampled companies.

It was noted[1] that the survey sample size in 2017 and 2018 was of 126 and 114, respectively. The average maturity index results in these years were 33.3 and 28.9, with this year declining to 30.1 with 211 respondents. Indeed the was a decline of 3.2 points, but not statistically important. The fact that, even though the sample grew by a little more than 40% with respect to 2018, the results kept steady, tells us that the sample is statistically representative of the population from where the respondents were taken from. This means we can trust the respondents as being the average individuals that we can take from the whole world of 1B revenue finance-tech companies, and not some random outliers from the excellence section or the total opposite. Now that we confirmed that our subjects can be trusted, let's explore what their answers tell us.

3 Inside The Companies

Once we know the basic demographics of the sample, we can get to know the companies a little more: what's it like inside? Several questions regarding the inner workings of the subject's companies were carried out, and two of them were crucial: 1) does the board of directors have at least one member with background in cyber/information security?, and 2) how satisfied do you believe your board of directors are with current level of information risk reporting? The answers can be seen in Fig. 1.

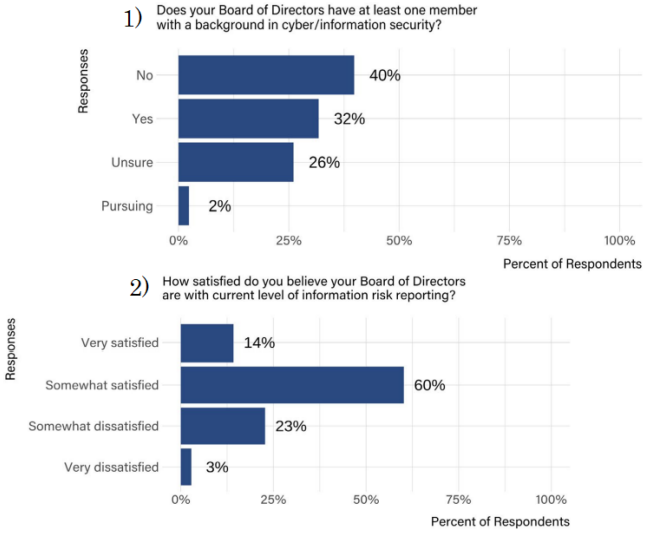

Fig. 1 Source: 2019 Risk Management Maturity Benchmark Survey by FAIR Institute.

These numbers tell us that most of the board members are not *experts* in information security, but somehow are satisfied with the level of risk reporting. However, in the article[1] we see that the maturity results obtained in 2017, 2018 and 2019 (28.9, 33.3, 30.1) are results skewed to the left side of the complete spectrum of a hundred total points, that is, the results lie in the weakest third of the axis, telling us that maturity is still at its

[a] *Universidad Panamericana Campus Guadalajara, Guadalajara. E-mail: 0197495@up.edu.mx*

lowest points. If the results are not particularly satisfactory, why are board members satisfied?

The answer is that the board members do not have a strong background in the field of security risk management. But is expertise required for a good maturity index? We know that an expert is someone who knows the exact terminology for a subject, and in the field of risk management, there is an important relationship between risk terminology and risk levels of maturity, shown in Fig. 2.

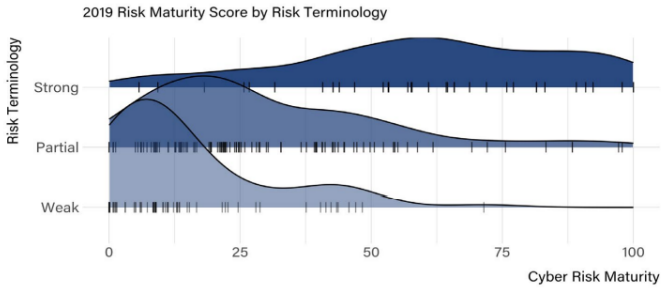

Fig. 2 Source: 2019 Risk Management Maturity Benchmark Survey by FAIR Institute.

Therefore, from the plot in Fig. 2, we can deduce that there is positive correlation between the risk maturity index and the levels of usage in risk terminology: the strongest the risk terminology usage, the higher the maturity index. Nevertheless, there is indeed a larger standard deviation in the plot of strong terminology than the standard deviation for the weak or partial terminology usage. This means that there is more variability in the maturity index result given a strong terminology usage than a weak one. Thus, a weak risk terminology usage **invariably** results in a risk maturity of around 8 points, and a strong risk terminology surely means a higher maturity index, but it can go from 60 to 80 points, since it tends to vary. We can also draw the conclusion that maybe the strongest risk terminology usage, the more variables tend to affect the exact level of maturity.

Thus, there is a correlation between expertise and maturity index according to the plot discussed. We know that the 40% of boards do not have this expertise according to Fig. 1, which may explain the unsatisfactory results in the maturity index in all the years were the survey has been conducted. But we also know that very little is done to fix this, because if we take a closer look at the last option in Fig. 2, we see that **only 2% of boards are looking to gain expertise in the field of security risks**, even though it is a latent problem that invariably means a lower maturity level in risk management. But does it bring any other consequence?

4 Other Factors

Expert judgement can be one of the techniques that is used for Risk Identification phase inside risk management[2], and the lack of this will therefore affect the early stages of risk management. The additional consequences of a weak early stage of a process can be seen in the execution of **precise forecasts**. This is confirmed by the survey results, were only 17% of total respondents confirmed the usage of economic forecasting in their risk reports[1].

The article[1] also examines which Risk Quantification Models are being used by the companies that responded to the survey, noticing that 32% of them use the NIST 800-30 model, which is a semi-quantitative model. Using a semi-quantitative model for quantitative analysis would mean to bring inconsistencies in the analysis purpose. This fact is better understood when we see another related answer: 60% of respondents claim that their risk analysis is narrative-based, as opposed to quantitative reporting. Therefore, the majority of companies use semi-quantitative models because their risk reporting has been proved to work better if story-oriented, probably because their board of executives have no expertise regadring risk analysis, and thus can better understand with common terms and not pure numbers, which may very well explain with more detail, but require years of experience in the field.

The nature of risk management should be proactive and preventive, but article notices that by having C-level board make the decisions, the company chooses to solve economic problems first[1], and this shows the opposite of the purpose of risk management, because the company proves to be reactive rather than proactive. This explains that the mean of Decision Making Visibility is tilted towards the weak area of the axis, where 83% of the companies are, hinting that decision boards seem to not always choose what is recommended by the analysts.

The regulatory environment seems to also have an effect on the current situation of risk management inside these companies. According to the article[1], the amount of strong regulations went through 42%, 49% and 38% in 2017, 2018 and 2019, respectively. This tells us that there has been a decline in the regulatory requirements, which might be the other half of the explanation of the satisfaction of risk reporting, even though the boards are not exactly experts in the matter, and the maturity index is not in the strong side of the axis either.

But not everything seems to be catastrophic: the article[1] also shows that, regarding Risk Quantification Models, 27% of the companies interviewed use their own quantitative models instead of the international guides like NIST 800-30 or the FAIR model. By using custom-made statistical methods to analyze risks, the companies show that they do more than just following the steps in a guide: the analysts make their own conclusions, their own terms, their own metrics. This has an effect on the companies results in the survey, since the analysis of the separate components in the study show that throughout the three years (2017, 2018 and 2019), all the areas regarding analysis (data quality, analysis quality and landscape intelligence) had an increase in points, whereas components like execution, prioritization and expectation had a stronger decline. The areas regarding overall risk analysis had an actual increase, meanwhile

more early-stage components decreased. The people behind the analysis seem to have the required expertise, but the people with more decision-making roles seem to take other routes that often vary their results.

5 To Finish

The horizon of risk management seems to have a long way to go, and companies are getting prepared one step at a time: while they show expertise in the analysis areas, the executive boards seem to be lacking the years of experience in security risk management. This was the basic idea of the article: the main problem of the companies today regarding risk management is their executive boards' expertise in the field, where their focus is the business and economic aspect of the problems, and not the risk-related themes. This leads to a weak use of risk terminology, which takes a company to storytelling reporting rather than quantitative analysis, which in turn explains the semi-quantitative models used by a significant number of the companies that participated in the study. All these opportunity areas seem to explain the low level of maturity, since they showed to have a positive correlation with the risk management maturity index. The executive boards should start wondering if their current satisfaction has anything to do with their unwillingness to increase their background in information security, because we all have got something to learn.

Notes and references

1 Freund, J. (2019). 2019 Cyber risk management maturity benchmark survey results. *FAIR Institute*, pages 1–19.

2 Goossens, L. H., Cooke, R., Hale, A. R., and Rodić-Wiersma, L. (2008). Fifteen years of expert judgement at tudelft. *Safety Science*, 46(2):234–244.

3 Kwak, S. G. and Kim, J. H. (2017). Central limit theorem: the cornerstone of modern statistics. *Korean journal of anesthesiology*, 70(2):144–156.