Building Organizational Risk Culture in Cyber Security: The Role of Human Factors

Isabella Corradini[1,3(✉)] and Enrico Nardelli[2,3]

[1] Themis Research Centre, Rome, Italy
isabellacorradini@themiscrime.com
[2] Department of Mathematics, University of Roma Tor Vergata, Rome, Italy
nardelli@mat.uniroma2.it
[3] Link&Think Research Lab, Rome, Italy

Abstract. Experts stress the importance of human beings in cyber security prevention strategies, given that people are often considered the weakest link in the chain of security. In fact, international reports analyzing cyber-attacks confirm the main problem is represented by people's actions, e.g. opening phishing mail and unchecked attached files, giving sensitive information away through social engineering attacks. We are instead convinced that employees, if well-trained, are the first defense line in the organization. Hence, in any cyber security educational plan, the first required step is an analysis of people's risks perception, in order to develop a tailor-made training program. In this paper we describe the result of a two-stage survey regarding risk perception in a sample of 815 employers working in a multinational company operating in the financial sector. The results highlight the need of a strong organization's risk culture to manage cyber security in an efficient way.

Keywords: Human factors · Cyber security · Risk culture · Risk perception
Awareness

1 Introduction

In the era of social media, artificial intelligence and Internet of Everything (IoE), media attention is often focused on the benefits provided by technology. However, cyber security risks are becoming more and more difficult to manage. In this scenario people are considered the main risk, since technology in itself is neutral, but it can be used for good or for bad. In several international reports (e.g., [1, 2]) it is apparent the main problem is represented by human factors: a cyber-attack, even the most sophisticated one, is often based on some human vulnerabilities. For curiosity, distraction or stress, people open an attachment without being aware of the consequences of their behavior. Or they release sensitive information on a social network, without fully understanding the possibility of their use by cybercriminals. While technology becomes more and more sophisticate, well known security issues, e.g. password strength and protection, have still to be solved.

An effective security approach to cybersecurity cannot neglect the role of human beings. It is fundamental to build a strong cyber security culture in every organization [3],

T. Z. Ahram and D. Nicholson (Eds.): AHFE 2018, AISC 782, pp. 193–202, 2019.
https://doi.org/10.1007/978-3-319-94782-2_19

so that employees in their daily life are constantly aware of the possible outcomes of their actions and perform accordingly. In our vision, this means not just training people to do or not to do something: to obtain a real awareness, people have to use technology in an informed way [4], working mainly on their attitude and motivation. That is why the construction of a cyber security culture starts with an investigation of the organization culture and of employees' risks knowledge.

In this paper we describe the results of a two-stage survey regarding risk perception in a total population sample of 815 employers working in a multinational company (C) operating in the financial sector.

This survey is part of the "Risk Culture" project that we designed in cooperation with the Risk Management Team and Human Resource Team of C in order to train the company's workforce. We consider the concept of risk culture as "*the values, beliefs, knowledge and understanding about risk, shared by a group of people with a common intended purpose, in particular the leadership and employees of an organization*" [5]. This concept cannot be dealt with independently from the organizational culture, since it is related to how risks are managed in the organization [6]. Hence, developing an effective cyber security culture requires involving employees and stimulating them to actively participate in the security activities of their own organization. In the following paragraphs we describe the main results of our survey and the main lines of the project.

2 Methodology

An assessment phase was conducted together with the two teams cited above to collect information on the organizational context and cyber risks initiatives (surveys and training) already implemented by the company. This analysis allowed to design a specific tool (a questionnaire) adapted to the profile of the organization.

The questionnaire is composed by 15 closed-ended questions investigating the following areas:

1. individual factors affecting
   a. risk perception
   b. risk evaluation
   c. risk management
2. information technologies and cyber-risks
3. risks in the organization and in the private life
4. prevention measures and behaviors

Almost a half of the questions asks to evaluate all the response options using numerical rating scales (from 1 to 5), while in some cases there are many options to evaluate (from 5 to twelve). Moreover, 2 questions require a multiple-choice response (maximum three options); finally, 6 questions have a single answer. Some specific aspects, as the impact of cyber risks in the organization, were discussed during focus groups session training. High level management endorsed the survey and actively

participated to it so as to give a clear signal to the organization about the important role each employee plays in the security strategy [7].

For a qualitative analysis, the tool also includes open-ended questions asking to freely associate one term to each of four keywords, chosen in cooperation with the Risk Management Team and based on the results of the preliminary analysis of the cyber risks initiatives.

The keywords are the following:

- attitude
- relationship
- behavior
- trust

Before administering the questionnaire, an internal communication plan was developed to accompany the "Risk Culture" campaign. Hence, an email was sent to all company's employees to communicate and explain them the initiative and its goal.

The survey was realized in two different stages. In the first stage the wide majority of employees filled the questionnaire for a total of 730 answers. In the second stage a new group of employees filled the same questionnaire, for a total of 85 additional answers. These new employees were working in a company that was absorbed by company C after the first stage was completed. They are anyway comparable in terms of background and skills to those involved in the first one.

The total sample is composed by employees of all ages. The sample has the following demographic characteristics: *Gender* (F: 30%; M: 68%; n/a: 3%); *Age* (up-to-30: 5%; 31–40: 25%; 41–50: 48%; more-than-50: 19%: n/a: 3%); and level of *Education* (lower-secondary: 2%; higher-secondary: 59%; degree: 34%; n/a: 5%).

3 Quantitative Analysis

Most answers from both stages were homogeneous, so we present the main results for the total sample. Due to space limitation we discuss only some questions, referred to by their number in the questionnaire.

3.1 Area 1: Individual Factors

Questions of this area investigated the individual attitude to the concept of risk, considering individual factors able to influence people's perception, evaluation and management.

Question #2 investigated what influences people's risks perception. You can see distribution of answers (it was possible to select only one option, n/a = 7 out of 815) in Fig. 1 below:

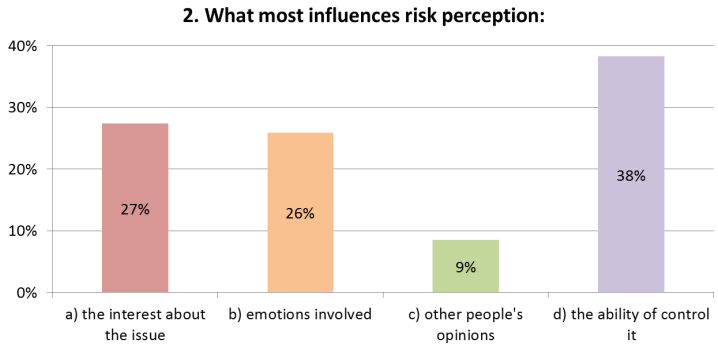

Fig. 1. The most important factor influencing risk perception.

The literature relative to the factors influencing people's risk perception [8, 9] and their application to security field [e.g. 10] reports that "risk perception" is a personal process influenced by one's own frame of reference. Accordingly, in this study, the factors most significantly influencing individual's risk perception are the ability of control (d), followed by the interest about it (a) and emotional processes (b).

Question #3 asked to rate on a 1 (negligible) to 5 (very high) scale how much is important to know, in order to evaluate a risk, each of a number of facts. Results (n/a = 11) are exposed in Fig. 2 below:

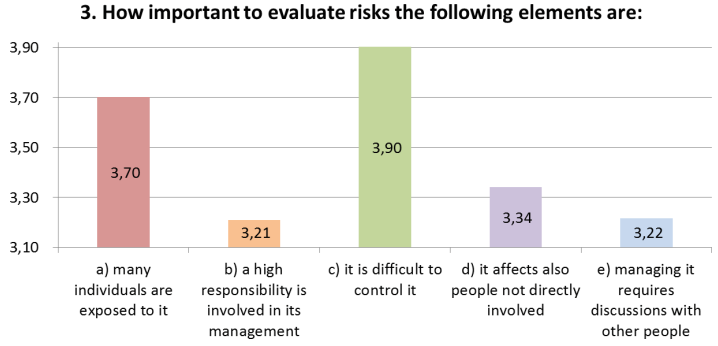

Fig. 2. To which degree one has to know various facts to evaluate a risk.

In line with the outcome of question #2, where the ability of control was the most influencing factor on risk perception, the difficulty of controlling the risk (c) obtained the highest value for this question, followed by the numbers of persons exposed to it (a).

3.2 Area 2: Information Technology and Cyber Risk

Question #5 investigated on the same 1–5 scale the perception with respect to social networks. Results (n/a = 8) are exposed in Fig. 3 below:

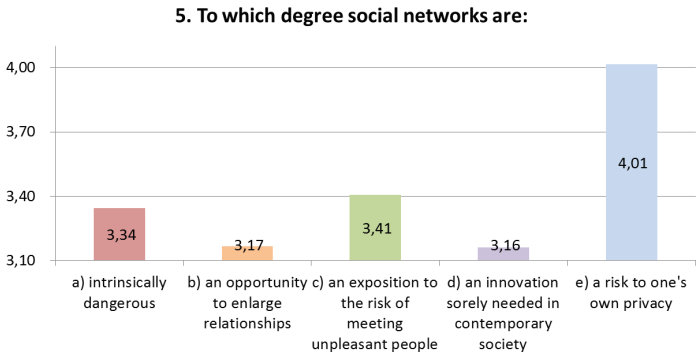

Fig. 3. Perception of the role played by social networks.

where you can see that answer (e) received the highest average value, while (c) was the next one.

Privacy is considered an important topic for most of the sample. In fact, social networks were evaluated as a risk to one's own privacy. This result is probably due to the importance that sensitive data (both customers' and employees' ones) have for the company, operating in the financial sector hence highly exposed to cyber risks. This situation explains most of the following results.

3.3 Area 3: Risks in the Organization and in the Private Life

Cyber-risks people worry about were investigated by *Question #7*, which asked to rate each possible risk on a scale 1 (negligible) to 5 (very high). See the results (n/a = 8) in Fig. 4 below:

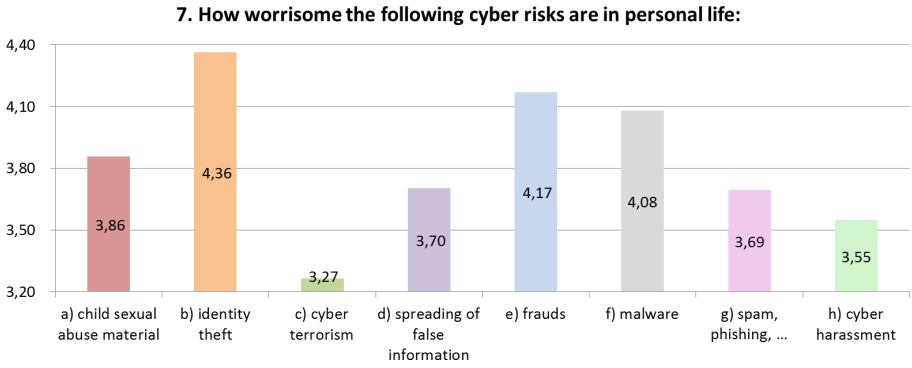

Fig. 4. Perception of the risk for personal life of various cyber-risks.

where identity theft, frauds and malware are considered the risks people should mainly worry about. You can note that "cyber terrorism" obtained a low value compared to the others, most probably depending from the fact the employees' answers to this question were strictly related to a personal viewpoint. Looking at the answers to the next question (#8), you can instead see that "attacks against critical infrastructure" (typically implemented by terrorists) received a much higher evaluation.

Question #8 explored instead which cyber risks one should worry about in organizations and to which degree. The same 1 to 5 scale was used. You can see results (n/a = 12) in Fig. 5 below:

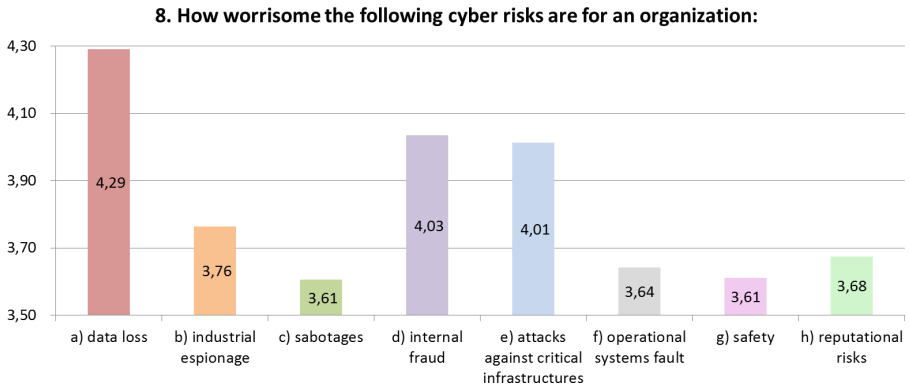

Fig. 5. Perception of the risk for organizations of various cyber risks.

The highest scoring risks is represented by "data loss" (a), followed by "internal fraud (d) and "attacks against critical infrastructures" (e). This result shows employees have a high level of attention to "data" within their organization, probably – as previously observed – due its activity in the financial area. In fact, during the training sessions the participants stressed the importance of protecting organization data, since they think that phenomena as data breach, thefts, viruses, human errors can compromise the company, also from a reputational viewpoint.

3.4 Area 4: Prevention Measures and Behaviors

The most important prevention measures in an organization to handle cyber risks were investigated by *Question #13*, which asked to select at most 3 options among the proposed ones. The distribution of answers (n/a or other fill-in elements = 58) is shown in Fig. 6 below:

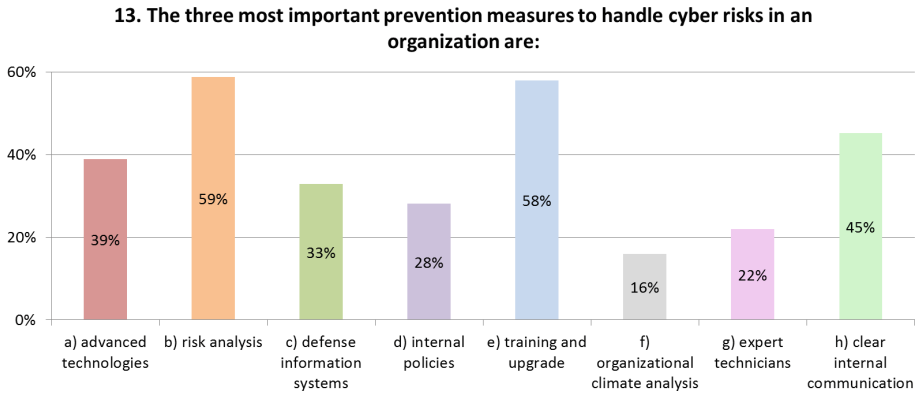

Fig. 6. Perception of the risk for organizations of various cyber-risks.

where you can see that "risk analysis" (b) and "training and upgrade" (e) are considered the two most important prevention measures to handle cyber risks in the organization, followed by a "clear internal communication" (h). The last one appears interesting, since communication is a vital way of enhancing employees' attention to security risks, that are often considered something only security experts should care about.

Question #12 asked to rate on the same 1–5 scale how much is important, in order to obtain an optimal security level, each of a number of classes of prevention measures. You can see results (n/a = 9) in Fig. 7 below:

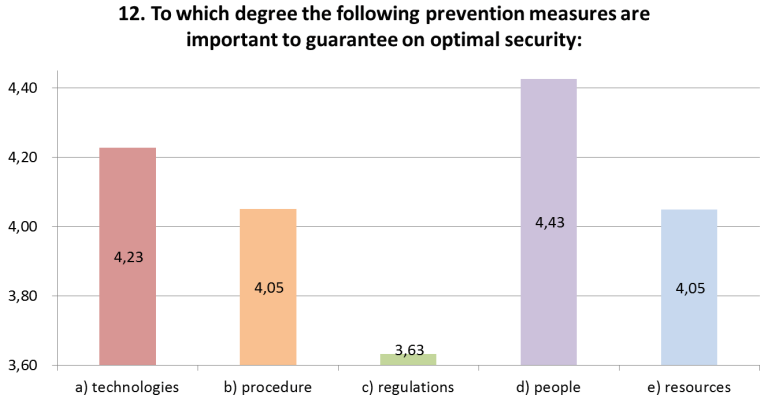

Fig. 7. Degree of importance of various prevention measures.

where the answer "people" was considered highly important. There was here a slight difference between the two stages: while in the first one "people" was clearly rated as the most important one, in the other one it came out in second position, but very close to the top one, i.e. "procedures". This is not surprising, given that procedures

are effective as a prevention measure not by their mere existence but only when executed by people. Technologies were rated as the third most important prevention measure.

4 Qualitative Analysis

For what regards the qualitative part of the survey, we now describe the outcomes of the investigated keywords: attitude, relationship, behavior, and trust.

We standardized the terms provided as answers to the keywords by first "stemming" them (that it, by bringing each term back to its root) and then coalescing synonyms and semantically close terms. Please remember that we asked to associate to each keyword just one term, but in some cases, people provided sentences or part of them. The following table shows the outcome of this process in terms of the number of both overall terms and distinct terms. Moreover, to help understanding the significance of the results for each keyword, we have shown the expected frequency of selection for each distinct term under a uniform distribution assumption (Table 1).

Table 1. Significant terms proposed and number of distinct terms for each of the keywords.

Keyword	Number of proposed terms	Number of distinct terms	Expected frequency of each term
Attitude	582	125	0.80%
Relationship	583	122	0.82%
Behavior	579	124	0.81%
Trust	584	165	0.61%

The keyword "*attitude*" has been associated mostly with the terms "positive" (12% of all proposed terms) and "proactive" (12%). Next in frequency are terms "responsibility" (5%) and "collaboration" (4%), showing the perceived importance of the central role played by individuals in the organization to ensure a proper management of risks. Note that 6% of answer proposed "behavior", most probably deriving from the fact that it is used in common language as synonym of "attitude".

While it is somehow expected that the most frequent term associated to keyword "*relationship*" has been "communication" (18%), more relevant is the fact that the next two terms are "cooperation" (6%) and "sharing" (4%), showing an understanding of the fact that without them a proper relation cannot be established. Having good relations is fundamental to establish a good organizational climate, which plays an important role for cyber risk prevention and management. Note that 5% of answers proposed "connection", once again on the basis of the fact that in common language the two terms, in Italian, are synonyms.

The two terms more frequently associated with keyword "*behavior*" were "fairness" (11%) and "responsibility" (7%). While the occurrence of "fairness" is expected, the fact that "responsibility" was highlighted shows that there is a clear understanding of the fact that human factors are fundamental for an appropriate risk management.

The term "education" (7%) was also highly selected, stressing the importance of training to build appropriate behavior. Once again, 8% of answers selected a term "action" which is the way behavior is implemented.

The keyword "*trust*" is mainly associated with security (10%) followed by reciprocity (6%) and reliability (4%), which were the three terms with higher frequency. Of particular interest is the fact that this keyword was characterized by the highest number of distinct terms.

5 Conclusions and Perspectives

Building a cyber security culture in the organizations cannot be tackled without people's involvement and the assessment of their risks knowledge. Moreover, it is important to carry out training in risk management, focusing especially on practical experience and the development of adequate communication abilities.

On the basis of the outcomes of the survey presented and discussed here we designed a security awareness program adapted to specific needs of the company.

We therefore run hands-on workshops using interactive methodology learning (case studies, brainstorming and work groups) and implemented communication initiatives (video, flyers) to motivate people to actively participate in the training activities and to help disseminate awareness on these issues to their colleagues.

We are now working on measuring the long-term impact on the organization of the security awareness implemented initiatives.

References

1. Verizon, Data Breach Investigations Report (2017). http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
2. PwC, The Global State of Information Security® Survey (2018). https://www.pwc.com/us/en/cybersecurity/information-security-survey.html
3. Enisa, Cyber Security Culture in organizations (2018). https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations
4. Corradini, I., Nardelli, E.: A case study in information security awareness improvement: a short description. In: 7th International Multi-Conference on Complexity, Informatics and Cybernetics: IMCIC-ICSIT, vol. I (2016)
5. The Institute of Risk Management: Under the Microscope. Guidance for Boards. https://www.theirm.org/media/885907/Risk_Culture_A5_WEB15_Oct_2012.pdf
6. APRA, Australian Prudential Regulation Authority, Information Paper, Risk Culture (2016). http://www.apra.gov.au/CrossIndustry/Documents/161018-Information-Paper-Risk-Culture.pdf
7. Corradini, I., Zorzino, G.: Hybrid and Awareness: basic principles. In: Hybrid Warfare and the evolution of Aerospace Power: risks and opportunities, CESMA (2017)
8. Slovic, P.: The perception of risk. Earthscan Publications (2000)

9. Slovic, P., Fischoff, B., Lichtenstein, S.: Facts versus fears: Understanding Perceived risk. In: Kahneman, D., Slovic, P., Tversky, A. (eds.) Judgement Under Uncertainty: Heuristics and Biases, pp. 463–492. Cambridge University Press, Cambridge (1982)
10. Schneier, B.: The psychology of security. In: Vaudenay, S. (ed.) Progress in Cryptology-AFRICACRYPT 2008. Ser. Lecture Notes in Computer Science, vol. 5023, pp. 50–79. Springer, Heidelberg (2008)