

Evaluating the Effectiveness of Privacy and Security Promotion Strategies

M. Iacono[1] and M. Mastroianni[2(✉)]

[1] Dipartimento di Matematica e Fisica, Università degli Studi della Campania, "L. Vanvitelli", viale Lincoln, 5,81100 Caserta, Italy
[2] Dipartimento di Informatica, Università degli Studi di Salerno, Via Giovanni Paolo II, 132, 84084 Fisciano, Italy
mmastroianni@unisa.it

Abstract. Privacy and security concerns are one of the relevant action fields of regulators. The rise of privacy concerns is, due to the capabilities of computing systems to aggregate information to generate profiles or other aggregates that impact the personal life of people. This has led to regulations like the UE General Data Protection Regulation (GDPR) and to the spread of initiatives aiming to raise awareness in people. Data show that privacy problems are known to people; however, practice of privacy and security aware behavior seems to be oddly not part of the habits of the same population. In this paper we propose a model of privacy and security effectiveness promotion strategies and a related evaluation method. The strategies we are interested in aim at aligning actual behavior to awareness levels. We derive an example of strategy starting from literature data and propose an analysis method that is based on Pythia, a tool for the analysis of graph-based probabilistic cause-and-effect models.

Keywords: Privacy · Security · Privacy awareness · Security awareness · Privacy paradox · Risk analysis · GDPR

1 Introduction

Problems created by privacy, and, more in general, security violations may be highly severe and may seriously impact daily life of people. As a consequence, far before the introduction of the GDPR[1] privacy concerns had been raised by the scientific and social studies communities, by industry and by governments. For example, in Italy private and public initiatives and information campaigns were launched, targeting workers, students and citizens, after in 2005 the Codice dell'Amministrazione Digitale[2] law introduced and regulated Information and

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council, April 27, 2016, concerning the protection of individuals with regard to the processing of personal data, as well as the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4 May 2016.

[2] D.lg. 7 marzo 2005, n. 82, Codice dell'amministrazione digitale (G.U. n. 112 del 16 maggio 2005, Suppl. ord. n. 93).

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2023
O. Gervasi et al. (Eds.): ICCSA 2023 Workshops, LNCS 14109, pp. 134–148, 2023.
https://doi.org/10.1007/978-3-031-37120-2_9

Communication Technologies (ICT) as the main mean for the reorganization of public administrations, their processes and their interaction with private citizens and other subjects. Analogous initiative were enacted in many Countries.

This notwithstanding, an Eurobarometer[3] survey published in 2018 reveals a surprising discrepancy between data resulting from the answers to the questions on potential privacy problems and those resulting from the answers to the questions about behaviors: apparently, people exhibited high awareness about potential problems but did not enact virtuous and attentive behaviors, as should have been expected as a consequence.

Possibly, the Covid-19 crisis led to an even worse situation, as many citizens that were not familiar with online operations were forced to unfamiliar procedures without any kind of training or support, and this is also confirmed an Interpol report written in August 2020 about Covid-19 impact on cybercrime[4].

In [1] we identified possible levers that might help stimulating people to align their behavior to their knowledge about privacy and security procedures, including better software engineering approaches that conform to GDPR privacy-by-design and privacy-by-default requirements [2,3]. In this paper we propose a methodology and a modeling approach to evaluate the potential effectiveness of such levers by means of a quantitative approach based on an Influence Nets analysis tool [4,5]. At the best of our knowledge, this is a novel approach to the problem and contributes to bridge efforts by software industry, academia and regulator under the umbrella of a tool suitable to analyze complex scenarios subject to complex probabilistic influences.

This paper is organized as follows: Sect. 2 presents related work, Sect. 3 states the problem, Sect. 4 describes the modeling approach, Sect. 5 introduces a case study, Sect. 6 discusses the results of the analysis on the example strategy, and conclusions close the paper.

2 Related Work

The *Privacy Paradox* is a seemingly strange users' behavior that may be defined as *a concept in which online users state that they are concerned about privacy, but disclose personal data nonetheless* [6]. Many researchers deal with this topic, and an interesting starting point to deep into this topic is a systematic literature review [7] that explains the privacy paradox and identified a series of theoretical explanation attempts for the privacy paradox, including decision biases, lack of experience and illusion of control.

The privacy paradox concept is also controversial. Solove [8] argues that it is a myth created by faulty logic, since the people's behavior in their everyday life is not an accurate metric of preferences because behavior is distorted by biases and heuristics, manipulation and skewing, and other factors. Author claims that giving individuals more tasks for managing users' privacy will not

[3] https://europa.eu/eurobarometer/.

[4] https://www.interpol.int/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf.

provide effective privacy protection, and instead argue that a regulation focused on regulating the way information is used, maintained, and transferred could have more impact on this issue.

Acquisti et al. [9] in their review also highlighted biases and illusory control as an attempt to explain the matter, and include in the explanations the *adaptation* of users. In this research some possible countermeasures are also proposed to be taken to mitigate the issue: i) soft paternalistic interventions, called *nudges*, by authors given from stakeholders such as government, companies etc.; ii) positive impact from privacy regulations; iii) use of privacy-enhancing technologies; iv) market-based data *propertization*[5] schemes that could induce positive response.

An empirical study conducted during Covid-19 pandemic [11] suggests that the users' behavior could vary depending on age and medical condition. In [12] has been studied the case of AIoT-enabled smart surveillance, and stated that transparency in mode and purpose of the information collected could efficiently moderate the privacy paradox effect.

3 Problem Statement

The name Eurobarometer refers to a series of public opinion polls conducted regularly on behalf of the European Commission and other EU institutions since 1974. These polls address a wide variety of topical issues relating to the European Union across the its member states.

The objective of the surveys referred in this analysis is to understand the awareness, experiences and perceptions of EU citizens on cybersecurity issues. Respondents were asked to talk about many specific cybersecurity issues, such as how important they think cybersecurity is to EU internal security, how much they worry about being victims of cybercrime and how they would react in a variety of situations if they were victims of these particular forms of cybercrime. Although the number of questionnaires in the survey is relatively low (around 27,000), this analysis can be a good starting point for understanding how EU citizens deal with Cybersecurity issues. Used data relate to the Europeans' attitudes towards Internet security survey, ref. 2207/480. The survey is based on data collected in October/November 2018, which, at the time the analysis was conducted, was the most recent survey available on the topic.

Eurobarometer surveys have first highlighted a worrying trend in user behavior. The number of EU citizens concerned about cybercrime is on the rise, as is the number of EU citizens who think they are well informed about cybercrime, but are less likely to protect themselves from cyber risks. The following Fig. 1 shows how the view of the respondents regarding concerns and information on cybercrime changed from 2013 to 2018, comparing it with the most basic rule of safe behavior: changing the password in Internet services. In 2018, 40% of users did not change their password (email, social networks, e-banking services...) in the last 12 months, while in 2017 this percentage was 37%. It should be noted

[5] The process of coming to treat something as if it were property under the law [10].

that, in the same period, the perception of the interviewees regarding the increase in risks is growing, as is the perception of being well informed about these risks.

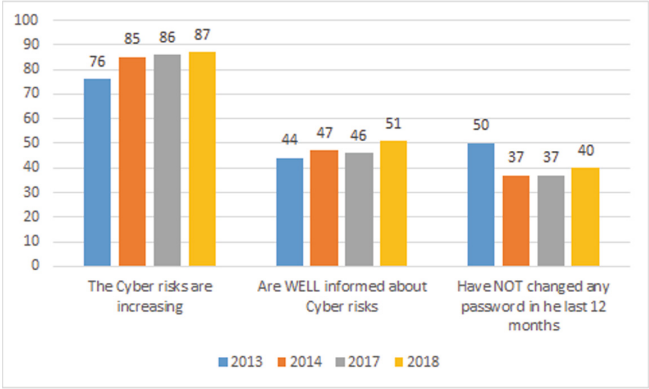

Fig. 1. Cybersecurity risks and users' behavior (Source: Eurobarometer).

Other relevant considerations can be made by analyzing user reaction to an attack. In the Eurobarometer survey there are two sets of questions relating to reactions. In the first group of questions, users were asked what in their opinion the correct behavior should be (respondent's perception); in the second group, users were asked what their real behavior was after they suffered an attack (real behavior). The results are quite surprising and are shown in Fig. 2. The reactions in the figures are grouped into three categories: Law Enforcement (the answer to the Eurobarometer questionnaire was "Call the police"), "Do nothing", same question in the EB questionnaire) and Others, which is the sum of all the other answers in Eurobarometer Questionnaire such as "Contact your Internet provider", "Contact your bank", "Contact a consumer association" and so on.

The first observation that emerges from these figures is the high number of "Do nothing" reactions in real behavior. If it is intuitive to explain this behavior in the case of fraudulent e-mails (e.g., phishing), which can be perceived more as a annoyance rather than a real threat, it is alarming that the reaction of over 30% of users who encounter abuses is to "Do nothing". The "Do nothing" reaction of many users who suffer online fraud or identity theft also deserves further study. Another thing to note is the distance between users' perception and their actual behavior when comparing the pair of rows drawn in Fig. 2. In many cases, users know that it is necessary to report the problem to law enforcement agencies and, in particular, to more serious cases, such as identity theft, bank fraud, ransom demand, but in real cases they choose to call another actor (the Internet provider or the bank, for example), or even do nothing.

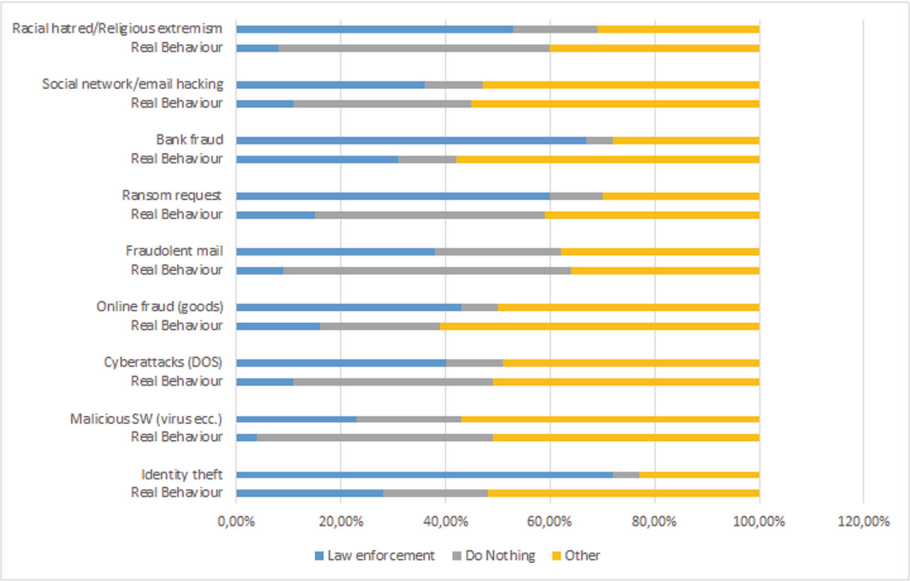

Fig. 2. Reaction to attacks, users' perception vs. real behavior (Source: Eurobarometer).

4 Modeling Approach

The verification of the effectiveness of the proposed actions requires an extended experimental campaign that would impact in vivo on the population, with significant and expensive large-scale interventions by governmental authorities. Enacting a strategy would involve the need for new laws, reorganization of governance processes at all levels and a control system over processes. Consequently, each proposal should be evaluated and compared with alternatives by means of a sound modeling approach capable of supporting a decomposition of the influencing factors and levers into intermediate steps and possible global influences in a quantifiable impact between single related factors and their mutual interference, in terms of a probabilistic framework.

A suitable methodology may consist of the following steps (see Fig. 3):

1. framing the problem;
2. identification of primary and secondary objectives;
3. identification of intermediate influencing objectives;
4. identification of actionable levers;
5. identification of the influence links;
6. definition of the probability with which each of the factors may independently verify or evolve;
7. weights assignment;
8. evaluation of the effects of levers application;

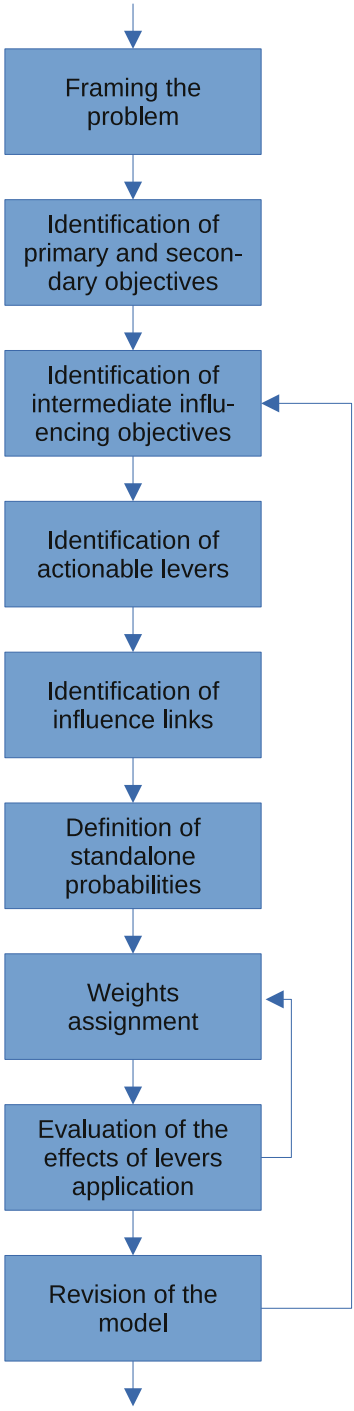

Fig. 3. The steps of the proposed methodology.

9. revision of the model.

Framing the Problem: in this step the relevant elements of the existing scenario are collected, investigated or measured, in order to state the situation as-is. Sources may be official or research document, existing data, experts, panels, reports.

Identification of Primary and Secondary Objectives: once the scenario is defined, primary goals, that is, the targets on which the strategy is meant to act in order to modify them or their effects, must be clearly defined, in order to allow the analysis of the influences. Targets may be facts, actions, effects of actions, measures. As the scenario definition phase may point out that other effects may derive by the application of the strategy, secondary targets may be defined and observed, as additional results, checks to be used for verification, expected effects to be monitored et cetera, including undesired or negative effects.

Identification of Intermediate Influencing Objectives: in this step the intermediate actions or facts that constitute the chain of consequences between levers and targets are discovered. This step, as well as the next ones, requires the intervention of domain experts, both for the definition and the quantification of the elements of the chain of consequences.

Identification of Actionable Levers: levers are the actions that can be used to enact the strategy. Actions should be in the actual availability of the entity that will enact the strategy, and may consist, for example, in investments, regulation, activation of resources, decisions, initiatives, policies.

Identification of the Influence Links: in this step the nature of the influences between the intermediate factors is identified, in terms of potential contributions to the verification of the influenced factor if the influencing factor verifies. This is done by analyzing the domain and assuming hypotheses derived by previous knowledge, documents, experiments, literature, technical reports.

Definition of the Probability with Which Each of the Factors may Independently Verify or Evolve: in this step each of the factors and targets is assigned a probability about the chances that it will act or happen independently from any influence, that is, in isolation. This probability may be already known or in need to be estimated by domain experts.

Weights Assignment: in this step each of the influences is assigned a positive or negative strength, defining the contribution of the influencing factor over the influenced factor if the influencing factor acts or does not act. This strength transmits or mitigates the consequences of influencing factors over an influenced factor modifying the probability of the destination factor as a conditioned probability[6]. The estimation of the strength requires domain experts.

[6] In the case study used to demonstrate this approach, CAST logic is applied to combine the influences.

Evaluation of the Effects of Levers Application: a what-if analysis may be performed to investigate the effects of the levers. This may lead to reconsider the weight of the influences of the model, also acting as a first debug step, and to cycle back to the *Weights assignment* step.

Revision of the model: the results of a sensitivity analysis may suggest missing influences in the model. This may lead to reconsider the structure or the influences of the model, also acting as a second debug step, and to cycle back to the *Identification of intermediate influencing objectives* step. The results of the previous steps might also inspire considerations on relations between the modeled entities and suggest the definition of new influences to be established between related levers or actions, contributing to define new or alternative policies; this may lead to fork new, alternate versions of the model, to be compared, on which it is necessary to cycle back to the *Identification of intermediate influencing objectives* step.

5 Case Study

In order to evaluate the impact of the proposed levers that can be used to improve the situation, we analyzed the influences between the goals and the levers. The analysis has been performed by organizing a panel of experts, including the authors. The panel supported the authors in the application of the methodology to the case proposed by the authors in [1] with an evaluation of the probabilities and the strength of influences and by assessing the proposed model. Moreover, the panel discussed the outcomes of the evaluation performed by the authors. The scenario has been modeled as an Influence Net and has been evaluated by means of Pythia [5].

The model is depicted in Fig. 4.

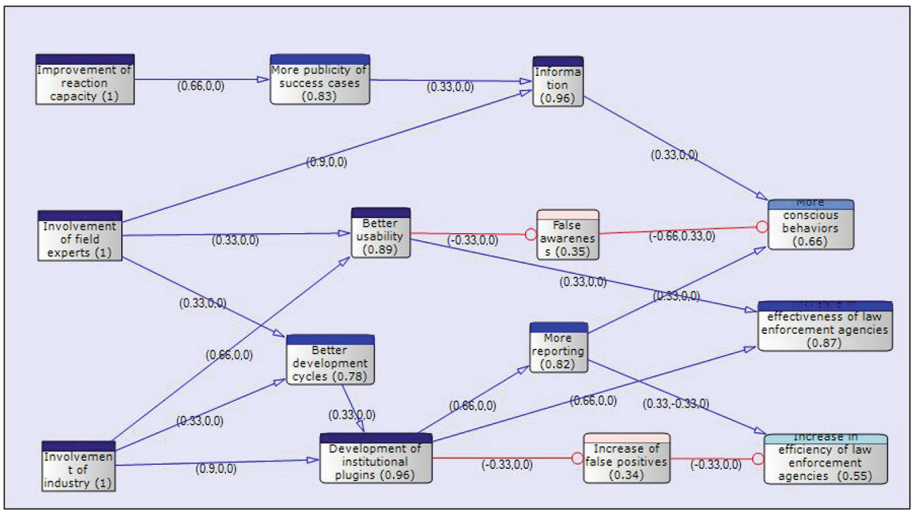

Fig. 4. The Influence Net for the proposed scenario

5.1 Targets Definition

The primary target effect of the model, coherently to what proposed in ?, is action *More conscious behavior*; secondary target effects are actions *Increase in effectiveness of law enforcement agencies* and *Increase in efficiency of law enforcement agencies*, as they are global measures of the potential effects of the strategy on the global level of the overall system defined by the regulations to react to privacy and security threats and to contrast their effects. *More conscious behavior* represents a change in users' behavior in terms of a greater coherence with security and privacy oriented policies, and with their knowledge about them. *Increase in effectiveness of law enforcement agencies* represents an increase of the overall degree of effectiveness of the complex of authorities, forces and institutions that apply a posteriori actions in contrast of privacy or security violations (e.g. courts, police, policy makers et cetera). *Increase in efficiency of law enforcement agencies* represents an increase of the overall efficiency of the said complex in terms of resources (people, funds, equipment) needed to investigate and, in case, sanction violations.

5.2 Levers

Used levers are a synthesis of the ones proposed in [1]. *Improvement of reaction capacity* represents the implementation of better procedures for immediate reaction to violations, both on the technical and the administrative point of view, but in the model the focus is on the administrative procedures, including publicity of success cases and avoided threats as a deterrent. For example, focusing on the Italian case, the national CERT, Agenzia per l'Italia Digitale, and the Autorità per la cybersicurezza nazionale might be involved in such a process. *Involvement of field experts* represents the contribution of academia and reference experts to improve both the methodological and design-related knowledge and understanding of ex-ante contrast of privacy and security related problems, including, for example, privacy-by-design and privacy-by-default compliant design techniques, as required by the GDPR. *Involvement of industry* represents the activation and orientation of targeted industrial contributions to the production of better solutions, stimulated by public funds or proper regulations.

5.3 Decomposition and Identification of the Influence Links

We identified as significant intermediate actions that may influence actions *Information* and *Increase of false awareness*, as the macrocomponents that emerge from the Eurobarometer results, and *More reporting*. *Information* represents a raise of the degree at which users are informed about privacy, security and related threats, good practices and protection tools. *Increase of false awareness* represents a raise of the phenomenon witnessed by Eurobarometer according to which users are informed, but do not behave consequently as a false sense of consciousness is letting them ignore caution and good practices. *More reporting*

represents a raise in the amount of potential violations or threats reported by users while using services or accessing the web.

In turn, *More publicity of success cases* has been identified as a factor that may influence *Information*, and may be a consequence of *Improvement of reaction capacity*. This action represents the contribution of media to the diffusion of positive results obtained by reaction among the population, that produces a spread of information reaching also generic citizens.

Better usability has been identified as a factor that may influence *Increase of false awareness*, as, paradoxically, better usability of software promotes routine behaviors, and routine behaviors produce mechanical actions, leading to ignore anomalies or to underestimate the consequences of own actions, as they become a habit. *Better usability* is influenced by both *Involvement of field experts* and *Involvement of industry*, respectively because of the theoretical/methodological and the implementation contributions to this factor. *Better usability* also impacts on *Increase in effectiveness of law enforcement agencies*, as better user interfaces may guide users to avoid bad habits or mistakes that produce exposure to threats and reduce the number of low impact violations, with a lower ordinary workload for contrast authorities.

Another joint effect of *Involvement of field experts* and *Involvement of industry* might be the development of proper methodological software engineering solutions and practices, such as the targeted privacy-by-design and privacy-by-default advocated by the GDPR, represented by *Better development cycles*. This might include the *Development of institutional plugins* to detect threats or produce automatic reports for the law enforcement agencies, which have as a consequence *More reporting* and *Increase in effectiveness of law enforcement agencies*, but may also produce *Increase of false positives* because of malicious or inexpert users, with a negative impact on *Increase in efficiency of law enforcement agencies*. *Development of institutional plugins* might also directly be a consequence of *Involvement of industry* under the push of regulation or as a byproduct of a will for less exposure to legal actions and liability that might involve authorities.

5.4 Probability and Weights

The panel did examine and review the proposed structure for the model and discussed both the probabilities and the weights of the influences, on the basis of an evaluation of the scenario based on the experience, reaching a consensus. In some cases there has been no consensus, so a mediation has been reached as a conservative compromise.

For the sake of space, the results of the analysis about actions probability is summarized in Table 1. In the case of action *False awareness* the baseline probability is set to 0.5 because no consensus has been reached by the panel. Similarly, the results of the analysis about strengths is summarized in Table 2. The reported strengths are relative to the case in which the influencing action is enabled, while in the case in which the influencing action is not enabled the strength of the influence is 0.0, with the only exception of one case, in which respectively the strength is indicated if the influencing action is enabled or not enabled.

Table 1. Baseline probability of actions

Action	Baseline probability
More publicity of success cases	0.20
Information	0.50
More conscious behavior	0.20
Better usability	0.10
False awareness	0.50
Better development cycles	0.20
More reporting	0.10
Increase in effectiveness of law enforcement agencies	0.50
Development of institutional plugins	0
Increase of false positives	0
Increase in efficiency of law enforcement agencies	0.50

Table 2. Influences between actions expressed as strengths of an Influence Net

Influence	Action	Strength
Improvement of reaction capacity	More publicity of success cases	0.66
More publicity of success cases	Information	0.33
Involvement of field experts	Information	0.90
Involvement of field experts	Better usability	0.33
Involvement of field experts	Better development cycles	0.33
Information	More conscious behaviors	0.33
Better usability	False awareness	-0.33
Better usability	Increase in effectiveness of law enforcement agencies	0.33
False awareness	More conscious behaviors	-0.66
Better development cycles	Development of institutional plugins	0.33
Involvement of industry	Development of institutional plugins	0.90
Involvement of industry	Better usability	0.66
Involvement of industry	Better development cycles	0.33
Development of institutional plugins	More reporting	0.33
More reporting	More conscious behaviors	0.33
More reporting	Increase in efficiency of law enforcement agencies	$\pm$0.33
Development of institutional plugins	Increase in effectiveness of law enforcement agencies	0.66
Development of institutional plugins	Increase of false positives	0.33
Increase of false positives	Increase in efficiency of law enforcement agencies	-0.33

6 Analysis and Results

The as-is situation of the influence net, considering the effects of the three levers, is in Fig. 4. The primary target has an overall probability of 0.66, 3.3 times the baseline probability: the hypothesized interventions may consequently be beneficial. Secondary targets are also impacted: the probability of increasing the effectiveness is 0.87, with respect to a 0.50 baseline, while the probability of increasing the efficiency is 0.55 with respect to a 0.50. In the first case, the model suggests that the proposed interventions do not have a negative impact on effectiveness and efficiency of contrast initiatives (helping instead it a bit to be more effective).

On these premises, a sensitivity analysis has been performed to understand what is the actual role of the three levers according to their intensity (or absence). The model suggests a very low sensitivity of the primary target with respect to an improvement of the reaction capacity, that is, an investment on first intervention procedures and infrastructures, as the overall oscillation of the final probability is 0.001: consequently, the contribution of this lever is not relevant. This may be motivated by the fact that people is not sensitive to technical procedures and emergency management with respect to the overall information that is available to the public, the baseline probability of spontaneous increase of which has been estimated by the panel to a value of 0.50 considering that workers receive training and that regulation is gaining popularity among the population because of the visible consequences of GDPR requirements in terms of consent forms both online and offline; the structure of the model excludes influences on the secondary targets. The oscillation due to the involvement of experts (including education, research and technical/professional initiatives) and of industry is one magnitude order wider, respectively 0.035 and 0.029.

The impact of an increase of the effectiveness of the law enforcement agencies depends on the involvement of field experts with an oscillation of 0.004, exhibiting a low sensitivity, while the oscillation of the contribution of industry is very relevant and quantifiable in 0.104. This may justify public funding targeted to stimulate industry towards an active collaboration with policy makers in the directions represented by the model.

The efficiency of the law enforcement agencies is a concern, due to the fact that the model exhibits a direct negative influence with a common root with an action that in turn has a positive impact on the previous target. Even if there is a chain of influences between the field experts contribution lever and this target, the only lever to which this target is sensitive, with an oscillation of 0.045, is industry intervention: this may be motivated by the fact that there is a common intermediate action that mediates their influences, with a complex influence subnetwork on which the industry lever has a direct and indirect influence.

If no lever is actually present, the model provides overall probabilities of 0.58, 0.74 and 0.21.

We decided to investigate the effect of a different estimation for the baseline probability of the efficiency target, in order to understand its inertia with respect to influences. With its baseline probability set to 0.20, the resulting overall

probability of the target is 0.33; if set to 0.10, 0.25. Consequently, the proposed levers produce anyway a positive overall impact.

6.1 A Proposal to Improve the Effectiveness of the Law Enforcement Agencies

The analysis of the model points out the low impact of an investment on improving the reaction capacity. This insight stimulated further work that led to a proposal of modification of the model, hypothesizing an influence of this lever on the effectiveness secondary target: this corresponds to a direct collaboration between first reaction and contrast authorities, that is between technicians and jurists, that we hypothesize with a moderate strength quantified in 0.33 and consisting in direct and organized communication and regular data and statistics exchange. A suitable model is provided by the introduction of Autorità per la cybersicurezza nazionale in Italy.

In this case, the overall probability of obtaining an increase of effectiveness is 0.91, and the best case is obtained when all levers are enacted, while the worst case is 0.83, when only the first lever is applied (clearly as an obvious consequence of the introduction of the new mechanism). The highest influence is anyway due to the introduction of institutional plugins; consequently, this new influence mitigates the dependency of effectiveness from private initiatives.

7 Conclusions

When the socio-technical perspective has to be considered, evaluating the effects of actions cannot be based the analysis of architectural or functional specifications. The effects of system-wide decisions on technical issues need a different quantification and proper modeling approaches. In this paper we adopted a tool suitable for evaluation of chains of consequences in socio-political systems and a support methodology to evaluate the suitability of a promotion strategy for privacy and security in the perspective of socio-technical systems. We explored how a proper analysis of the results provided by the tool and of sensitivity to levers may inspire and support insight-based improvements, besides informed decisions.

Future work includes the implementation of a more detailed model to obtain further insight and a better analysis of possible oscillation causes, that we expect wider if including a finer decomposition of objectives and levers, a time-based analysis of the same model, with alternative strategies, including proper cost hypotheses, and further quantitative investigation about the possible causes of the privacy paradox, to improve the model structure and define and evaluate more detailed strategies, with special references to the levers that software engineering may provide.

Acknowledgments. This paper is part of the research activity realized within the project PON "Ricerca e Innovazione" 2014–2020, action IV.6 "Contratti di ricerca su tematiche Green", issued by Italian Ministry of University and Research. Part of this work has been finalized in Sala della Regina at Camera dei Deputati, Italy, where Mauro Iacono was attending a meeting; it has been revised after the precious comments formulated while sitting together close to the tower of Pisa by professor emeritus Alexander H. Levis, to which Mauro Iacono wishes to express his gratitude, also for being a continuous inspiration and reference. The Pythia simulator used in this paper has been developed with the support by the Air Force Office for Scientific Research under contract no. F49620-01-1-0008, by the Air Force Research Laboratory, Information Directorate, under contract no. F30602-01-C-0065, and by the Office of Naval Research under contract no. N00014-06-1-0081.

References

1. Iacono, M., Mastroianni, M.: Il curioso caso della divergenza tra consapevolezza e comportamenti in materia di sicurezza informatica dopo la crisi pandemica: quando non bastano norme ed esperienza, Edizioni Scientifiche Italiane, pp. 107–118 (2022)
2. Campanile, L., Iacono, M., Marulli, F., Mastroianni, M.: Designing a GDPR compliant blockchain-based IOV distributed information tracking system. Inf. Process. Manage. **58**(3), 102511 (2021). https://doi.org/10.1016/j.ipm.2021.102511, https://www.sciencedirect.com/science/article/pii/S0306457321000194
3. Campanile, L., Iacono, M., Mastroianni, M.: Towards privacy-aware software design in small and medium enterprises. In: 2022 IEEE International Conference on Dependable, Autonomic and Secure Computing, International Conference on Pervasive Intelligence and Computing, International Conference on Cloud and Big Data Computing, International Conference on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), pp. 1–8 (2022). https://doi.org/10.1109/DASC/PiCom/CBDCom/Cy55231.2022.9927958, https://doi.org/10.1109/DASC/PiCom/CBDCom/Cy55231.2022.9927958
4. Zaidi, A., Mansoor, F., Papantoni-Kazakos, T.: Theory of influence networks, J. Intell. Robot Syst. **60**, 457–491 (2010). http://dx.doi.org/https://doi.org/10.1007/s10846-010-9425-8, https://doi.org/10.1007/s10846-010-9425-8
5. Mansoor, F., Zaidi, A.K., Wagenhals, L., Levis, A.H.: Meta-modeling the cultural behavior using timed influence nets. In: Computing, S., Modeling, B. (eds.) Springer, pp. 1–9. MA, US, Boston (2009). https://doi.org/10.1007/978-1-4419-0056-2_19
6. Øverby, H.: The Privacy Paradox, pp. 1–2. Springer, Heidelberg (2019). https://doi.org/10.1007/978-3-642-27739-9_1619-1
7. Gerber, N., Gerber, P., Volkamer, M.: Explaining the privacy paradox: a systematic review of literature investigating privacy attitude and behavior. Comput. Secur. **77**, 226–261 (2018). https://doi.org/10.1016/j.cose.2018.04.002, https://www.sciencedirect.com/science/article/pii/S0167404818303031
8. Solove, D.J.: The myth of the privacy paradox. Geo. Wash. L. Rev. **89**, 1 (2021)
9. Acquisti, A., Brandimarte, L., Loewenstein, G.: Secrets and likes: the drive for privacy and the difficulty of achieving it in the digital age. J. Consum. Psychol. **30**(4), 736–758 (2020)
10. Paul, E.F., Miller Jr, F.D., Paul, J.: Freedom of Speech: Volume 21, Part 2, vol. 21, Cambridge University Press, Cambridge (2004)

11. Fernandes, T., Costa, M.: Privacy concerns with COVID-19 tracking apps: a privacy calculus approach. J. Consum. Mark. **40**(2), 181–192 (2023)
12. Zhang, F., Pan, Z., Lu, Y.: Smart surveillance for personal data digitalization: contextual personalization-privacy paradox in smart home. Inf. Manage. **60**(2), 103736 (2023). https://doi.org/10.1016/j.im.2022.103736, https://www.sciencedirect.com/science/article/pii/S0378720622001446