The Hidden Potential of an Incident. Designing for Cybersecurity Incident Reporting

Alessandro Pollini[1*], Alessia Ciccone[1]

[1] *BSD design, Via Lazzaretto 19 20156 Milan, Italy*

Abstract

For a company, having a strong security system against cyber attacks is a top priority. The first form of protection adopted by organisations is certainly of a technical nature, with qualified personnel and software constantly monitoring systems to minimise possible vulnerabilities. In this context, there seems to be little room for man, who, on the contrary, is only considered a source of errors that cause security incidents. However, recent studies in human factors show the opposite, humans play a great role in protecting an organisation and have capabilities that machines cannot: focusing on these is the key to having a solid first line of defence. One of the best areas where the human component proves invaluable is in incident reporting, exploiting the ability of humans to notice adverse events before protection software detects them. Incident reporting, however, remains an end in itself if it is not met with a corporate culture that embraces safety-critical scenarios in order to learn from them, rather than merely correcting what went wrong. This study proposes the design of a reporting process that facilitates the task for the whistleblower, that involves the whistleblower in the resolution and analysis of the problem, and that uses the incident or risk as a case study to be presented to the company's employees, in the form of a story, through conversational storytelling. Through this, the organisation can gather opinions and bottom-up reflections and learn from them, consolidating a strong and resilient safety culture in the face of adverse events.

Keywords

Cybersecurity culture, Incident reporting, Software Plug-in, Human factors.

Damocles - First International Workshop on Detection And Mitigation Of Cyber attacks that exploit human vuLnerabilitiES Workshop at AVI '24, June 4, 2024 Arenzano (Genoa), Italy

* Corresponding author.

† These authors contributed equally.

alessandro.pollini@bsdesign.eu (A. Pollini); alessia.ciccone@bsdesign.eu (A. Ciccone); 0000-0001-8957-7866 (A. Pollini)

1. Introduction

In order to better understand what role people play in a cybersecurity incident, one must first enter the subject to assimilate the basics. The human behaviour that will be sought of understanding interfaces with a complex problem, the safety of computer systems and the data within them, thus having at least a basis of knowledge of definitions, processes, technical data, allows a complete view of the research area. The aim is certainly not to delve into the technicalities more difficult, but to have some fixed points to understand which threat you are talking about and to what solutions exist or could arise.

For companies, protecting themselves against cyber threats is vital: the theft of company secrets, sabotage of systems to compromise services and the integrity and copying of customer data to sell their identities on the dark web, are all examples of acts that are perpetrated and that can damage a company that depends on digital technologies to conduct its business activity [1]. Focusing on the human component in computer security is possible. On one hand the human is considered the weak link in the chain, on the other hand it has the potential to become the first line of defence against attacks. This is because humans have capabilities that machines do not have: they are able to recognise, improve and make decisions even when they have incomplete information at their disposal [2]. An organisation can put in field the most efficient automated systems, but a vulnerability may slip through their controls until there is sufficient data indicating an attack; a human, on the other hand, has the capacity to doubt, to notice behaviour potentially wrong and to rectify an error immediately.

The focus on human capabilities has meant that a fundamental task: the reporting of incidents. Although now in companies preventing attacks by building barriers is preferred and in fact almost no opportunity is given to the employee to fall into a 'trap', accidents, certainly to a lesser extent than to the past, they still happen. This happens, as noted above, because a security breach depends on so many factors that influence each other and very often the cause is paradoxically to be found in the very systems and policies that are intended to prevent them [3]. Having said that, all the premises made so far tighten into a funnel on one theme fundamental: to allow the active contribution of the human component in the security processes by focusing on one of the tasks that best defines it necessary part in the defence of an organisation.

Investigate the reporting of adverse events by employees is the primary focus of this research, which started from the broad scope of the cybersecurity and focused progressively more and more on the centrality of the human, found in this the scope to place a magnifying glass on a subject that is still little considered and which hides a broader discourse on security culture that will be explored in the following paragraphs.

Indeed, reporting does not only mean communication of a event, but includes a reflection on the pre-event phase, i.e. what drives one to do it and what drives one not to do it, and also a reflection on the next phase, so how the organisation reacts and how it manages to learning from accidents. In particular this research stems out from the following questions: how could people increase their level attention to the cybersecurity risks with the signalling instrument? How could the incident reporting artifact be based on trust, without the affecting organization control and limit human activities? How could organizations make reporting a source learning for allowing greater risk awareness?

This paper introduces the incident reporting human factors literature review (Par. 2), develop on the basis of an longitudinal preparatory research (Par. 3), and focus on the design of a web application for supporting incident reporting in large organizations (Par. 4). The evaluation through exploratory sessions the Anticipated Experience Evaluation (AXE) [4] is then described in Par. 5 with the presentation and discussion of the results, and the conclusive remarks (Par. 6).

2. Literature Review

2.1 Just Culture

A culture of security is equivalent to a informed culture, i.e. one in which every member of an organisation, at every level, does not forget, understands and respects the risks of its operations. In many cases, accidents can reach very low numbers, so a way to remain alert is to create a security information system that collects, analyses and

disseminates knowledge from accidents and near misses. Given this picture of the situation and what problems it could bring, some studies have proposed solutions, steps necessary for the construction of the of a signalling system.

An example is given by O'Leary and Chappell [5] which, within the broad framework of security in general, describe the stages and the aspects necessary to set up an incident reporting system accidents. For Reason [6], the creation of a culture of signalling, only possible after establishing a just culture and this depends on the relationship an organisation has with the guilt and punishment. In order to further explore both assumptions that Reason [6] posits as necessary for a safety culture, they will be illustrated below are the conditions that favour or disfavour them, trying to understand what is the right way to implement them. Another example of guidelines to follow when designing a system of report is given by Pasquini et al [7], who list the five dimensions to implement a safety culture assessment.

Dekker [8] illustrates the basis for a just culture: the step forward to be taken is above all normalise and legitimise accidents, which are not failures or crises but are a normal part of the job and those involved should neither be punished nor stigmatised. Then employee involvement is crucial during the management of the incident, find a way to integrate the experience of employees in decisions on how to deal with consequences. Empowering and involving the operator himself in the post-accident phase is the way best to maintain morale, maximise learning and strengthen the basis of a just culture. Dekker then evolves the concept of Reason [6], basing however just culture on the investigation of the accident to understand what variables attribute responsibility, but frames it in a positive light: listening to the voice from below, it is possible to understand not only where the problem is, but also which are the capacities of individuals, groups or organisation that lead to positive results [9].

2.2 Factors for incident reporting failure

Hollnagel's model [10] confirms that safety traditionally had a counterproductive approach. It allows us to look at incidents from a different perspective and envisage a management that enable learning by all levels of an organisation, especially through a non-punitive culture. But precisely, as he states, this approach does not necessarily exclude the previous ones, so the choice of mentioning these three items serves to have as complete a picture as possible of how articulate the topic is and demonstrates the complexity of the design challenge. As already mentioned, incident reporting systems are designed to ensure continuous learning, relying on feedback from the workforce. But to understand the prerequisites for a successful reporting system one must first consider what the conditions for failure are.

First of all, in cybersecurity, the prerequisite for reporting is notice that something is wrong or react to warning signals, which is not always happens. Briggs et. al [11] investigate this very aspect and list possible reasons why a warning is ignored and not reported: a first point of view is that of productivity. In general, messages warnings and calls for action are often unexpected, potentially disruptive and not quantified in terms of the effort required. Moreover, they could be indicators of a real security threat, or could even be false alarms. For this reason, many users prefer to ignore this information when they believe that the costs of the action outweigh the benefits or when they consider that the commitment is too much and interrupt the execution of their main task.

A second approach is explained by Rogers' Protection Motivation Theory (PMT) [12] which assumes that users perform two important assessments: a threat assessment and an evaluation of the reaction. For the former, they assess both the severity of the threat and their own vulnerability to it and for the second, they assess their own understanding and responsiveness and effectiveness of the response. In relation to the first point of threat assessment, the average user may have a poor understanding of security threats and incident reporting is closely linked to misperceptions of threats and poor cyber security convictions. Regarding the second point, users may not be sure of the appropriate action to be undertaken, but they may also be unconvinced of the effectiveness of any action.

A third point of view is that of so-called social laziness, in other words, an individual user may not react to a request, perhaps assuming that it will be the others who will answer. One might also think that the failure to response will not be noticed or be personally identified: in fact users may be uncomfortable if their personal information were included in the incident report shared with the whole company if in this reigned a punitive

climate based on guilt. This means that inaction can result either from anxiety about being considered responsible for the outcome and by the lack of responsibility.

Perceived characteristics of the task can also contribute to the social laziness and failure to report errors. For example, unattractive or complex tasks often require the use of incentives to encourage employees to carry them out and reporting may be one of them. If no specific information on the complexity of the reporting task, users may assume potential complications or excessive work demands. Thirdly, the effectiveness of signalling may be unclear: the absence of change or responses to user action may reduce motivation to act, thinking that their reporting will not make a difference.

2.3 Factors in incident reporting success

A first prerequisite is trust. It is a fundamental element and is even more important when a truthful account of the error is required or errors and their (possibly personal) causes. Without trust, the report will be selective and will probably gloss over the fundamental human factors issues. In the worst case, where potential reporters do not trust the organisation, there it could be no signalling.

A second factor is confidentiality, as one of the essential foundations of trust. The reporters must be certain that their identity, as well as that of their colleagues, is protected and will be immune from disciplinary proceedings that could be initiated as a result of their reporting. A system of success is based on the knowledge that valid feedback on failures of the reporter or the system is much more important than the attribution of blame. The best way to achieve this, in certain cultures based on guilt, is anonymity, with the disadvantage that those analysing cannot contact the reporter again. Another way to build trust in the reporting system is to keep the organisation receiving the reports and the company separate. Preferably, this system should have no authority legal on its alerts. Reporting systems operated by other research institutions, such as universities, provide a third party disinterest that can earn the trust of the signallers. Trust can also derive from the supervision of an advisory group representing the interests of the signallers.

Motivation is also another fundamental factor. The signallers must see a value in reporting, they need to know how their reports will be used to improve security. One way to achieve this objective is to provide feedback to the reporting community. Many systems of reporting have newsletters describing security problems and highlight the improvements achieved thanks to the reports presented, thus informing the alerts and giving them at the same time a pat on the back.

Ease of signalling is another important aspect to consider when developing an incident reporting system. It is desirable also be sent electronically, as the alert can be inserted more easily into a database. Ease of use is also influenced by the structure of the reporting form: if a form is long and requires a lot of time to be compiled, users are less likely to make the effort required. If the form is too short, it is difficult to obtain all the information necessary information on the incident. In general, the more specific the questions, the easier it is to fill out the questionnaire. More questions perceptions, judgements, decisions and actions are not subject to this limitation and give the reporter more opportunities to tell his entire history. This method is most effective in collecting all information about an incident, but takes longer to complete and usually requires more analytical resources within the system reporting. The use of these open questionnaires is probably best limited to situations where there is an enthusiastic reporting population and/or expressive.

3. Preparatory Research on Cybersecurity Culture

The human being is the best source of information on which an organisation can rely, because it is able to provide aspects that machines fail to detect. The true nature of accidents and risks so it might be difficult to detect, but at this investigation, aimed at understanding the conditions under which they occurred and whether the action could have been performed differently by colleagues in the same situation: if it could not have been otherwise, then it is not possible the attribution of blame.

The Cybersecurity Matters project was conducted within one of Italy's largest telecommunications companies and is an awareness pathway that, by means of conversational storytelling, promotes awareness of the role of the

human component in the cybersecurity and returns a snapshot of the maturity of the organisation in the field of computer security. The course is precisely characterised by the conversational storytelling component, i.e. participants have conversing with a conversational agent, via a chat, answering the questions they were asked. The answers collected allowed a survey of participants' behaviour, choices and attitudes. Cybersecurity Matters, therefore, implement a survey of the corporate population, that, starting from the assumptions of human factors, aims to: analyse data on the behaviour adopted in precise decision-making contexts, with respect to day-to-day security-critical scenarios and be a support for training in order to stimulate greater sensitivity and awareness on the issue of cybersecurity and respect to the value of the individual. Cybersecurity Matters' data collection is divided into two phases: the initial phase of interviews with different stakeholders to collect sufficient data to develop the narrative content of conversations and the actual collection of answers through conversation with the agent. The two results were then compared at the end to see if there were correspondences or differences.

- In the organisation, the level of awareness of cybersecurity issues is not considered homogeneous by those within it, with proactive, sensible, and detached people, depending on their role. Despite participation in training on the topic is very high, there is a gap between theory and practice: many times some risky behaviours are not perceived as such, seeing them as something distant, not direct, to a group of persons or a specific activity.

- IT security takes second place to efficiency and to the needs of the business, indeed it is sometimes considered to be in the way. This vision can be seen from the company's top management, who do not take the of a safety culture.

- Employees are confident that the company has put in place the best protection technologies and consequently feel safe. In addition, cybersecurity experts are considered a point of reference and routinely consulted. This probably entails a delegation of responsibilities to technology and experts.

- The environment is not considered to be based on guilt and punishment, but on learning.

- The majority of respondents believe that cybersecurity risks come largely from within the company.

Once this initial information was obtained, it was the inspiration to create narratives that the corporate population would find in the interaction with the conversational agent, divided into three stories. Participation in the stories was proposed to 2980 people and the sample that actually adhered is 1005 people.

These enabled the following data to be collected:

1. People with greater self-confidence are on average less likely to fall victim to cyber attacks. Technicians are naturally the most confident because they have a greater knowledge of the subject, non-experts are only partially aware of all the risks that can be taken and do not feel that they are actors who can make a difference.

2. The feeling of fear aroused by the communication of risks, while on the one hand an incentive to prevent them for fear of the consequences, is also a reason for blockage: the activity freezes due to lack of knowledge and awareness of the real risks.

3. Faced with operational uncertainty, one prefers to act autonomously, which on the one hand is positive because the individual puts himself at stake to ensure the company's performance, but on the other hand may not have knowledge of all the necessary information and not establishing a dialogue with others does not allow the whole organisation to learn.

This set of insights is valuable for this project since it offers the possibility of having data taken from the field and from a very consistent knowledge-base otherwise difficult to obtain due to the limited availability that could have a private company in providing such sensitive information. The research represented the starting point for the qualitative data collection phase. Although the insights just listed paint an extensive picture of the

organisation's IT security maturity, elements for the specific topic of incident reporting can be drawn however, considering that it is information about the security culture of the company. It is, as has already been stated, the foundation for a culture of reporting so having some initial information on this allows me to better frame this aspect.

3.1. Insights from Research

The authors have led to the identification of key insights that will serve as a point of starting point for problem definition.

1. Attention is higher. A fairly shared opinion is that the focus and sensitivity to security issues IT has grown a lot compared to the past because the dangers have increased.

2. Control over people. The technicians confirmed what was found also in literature: the human is the weak link. For this reason, the most common practice is to control and make up for human shortcomings with technology. So much so that non-technical people feel closed and protected inside technological walls and think they do not ever come across a security incident if not through phishing. This scenario denotes a lack of trust in people.

3. Awareness. In order to stimulate people to report, it is necessary to focus on awareness and training, from the since very often it is precisely the lack of risk awareness to determine the failure of people to react. Training is certainly done in the different companies, through onboarding and periodic lessons, but all non-technical interviewees think it is interesting up to a certain point: to make it they have to interrupt work, they see no use for it in the workplace because they think they are in a bulletproof box in closed corporate systems and thus see a interest only in managing their own devices personal outside work.

4. Non-standardised reporting. The reporting methods are all different and all are based on the free narrative made by people. For technicians, a standardised method is not possibility because the dangers of computer security do not are standard, they are constantly evolving. There is still need a fairly clear figure to be analysed and a report easier and faster. The only means of signalling equal for all is the reporting of spam mails.

5. What to report. The opinions of technicians are divided, on the one hand states the need to receive reports only for incidents - data breaches -, so as not to overload of work the IT team, on the other hand there is an openness also to the reporting of near misses and false positive. We learn from the literature that when a system is not standardised needs also report risks and that critical events with positive outcomes are a rich source of learning.

6. Reporting culture. The non-technical respondents all said they were willing to report any incidents immediately, but at the at the same time they do not know what report and what happens afterwards. There is therefore a lack of clarity in the systems. Technicians confirm that the measures disciplinary measures are limited to a warning in case of unintentional error and arrive at 'consequences' for events, confirming the traditional approach found in the literature to blame the individual and its error; in fact, in two testimonies of non technical we see the already established practice or the desire to remain anonymous.

4. Tellp Design Project

4.1. Design Concept

The idea is for a tool that allows this, an application software that is easy to reach and locate on the screen and that does not is intrusive in daily activities. The solution that best suits these needs is a system plug-in, installed on corporate devices, which is placed in the toolbar of the operating systems in use, so as to always be at hand, but not in the way. Through this application the user is able to choose whether to report a cybersecurity incident, i.e.

an event whose harmful consequences it has been able to ascertain, or a risk situation, i.e. the case when it has been noticed an event that could lead to negative consequences.

The name chosen for the application is Tellp, a play on words that comes from the combination of the word 'tell' and the word 'help'. Tellp sums up what lies at the heart of the whole concept, namely telling for help, but also the principle that telling others helps people to feel less lonely. The symbol in the logo replaces the two 'Ls' of the word Tellp with a simple and distinctive sign that takes up the outline of the two letters written in italics. But the sign also recalls union, like a thread connecting two individuals, and symbolises what the idea wants to bring into a company: unity between people, mutual cooperation and support, teamwork, feeling that we are all part of a single organism. Tellp represents the design proposal to accomplish the goals in Table 1, by the implementation of the incident reporting envisioning scenario presented in Par. 8.2.

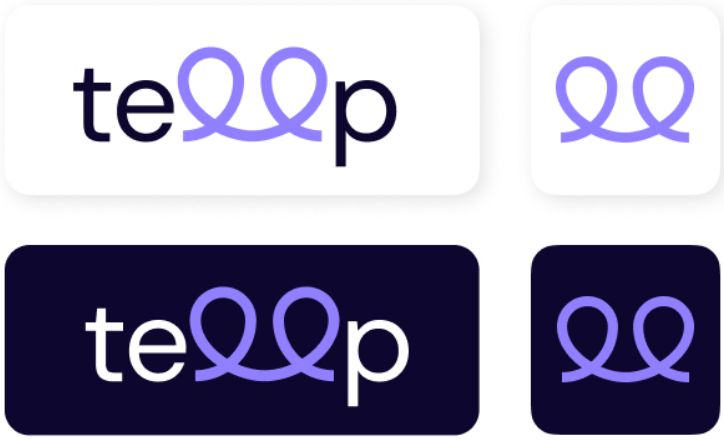

Figure 1: Tellp's logotype and symbol in its positive and negative configurations

Figure 2: Tellp's mockup.

Table 1
Design goals

	Goals
1	To facilitate reporting by employees by bringing them closer to the IT team
2	To provide the IT Team with complete data and timely to be analysed and use to assess and resolving the situation
3	To promote participation of the reporter, and any people involved, in the analysis that follows the event to avert punishment and culpability;
4	To share the incident to all the corporate population for allow learning to all levels of the organisation;
5	Getting feedback on what happened by the entire corporate population so that it participates in providing valuable bottom-up data in the definition or modification of policies;
6	To implement security policies closer to the abilities, aptitudes and real behaviour of people.

Main values guiding the design are therefore the need to talk and confidence, the need to receive support quickly and easily with feedback punctual, the need to confront others and not suffer guilt and disciplinary consequences and the need for the whole organisation to learn critical cybersecurity scenarios. Such a complex problem, therefore, does not can be addressed with a single solution, such as a user interface, but with a more total idea of a service or marking process. The user from the beginning to the analysis of the event, and then allow the sharing of what happened so that everyone can gaining awareness. The idea is to exploit the technological tool as a signalling support, but to place it within a system made of people and relationships between them. The idea therefore develops in several stages, which illustrate the whole process.

4.2. Envisioning Scenario

Incident Reporting

Reporting to the technical team must be quick and easy, it must ensure that the reporting user does not feel abandoned after having done so, so the see the value and usefulness. It must therefore include feedback from the who, for their part, must be sensitive, non-judgmental and know how to calm down. In the first case the user is immediately put in voice contact with the technician, so as to tell the incident as naturally as possible, answer questions immediately techniques and receive immediate feedback on what they can do. In the second less urgent case, the software leads the user to answer a questionnaire reconstructing the fact to send the report. It is important to give this choice to the user because, as Pasquini et. al. [7] suggested, in a context where the line between what to report and what not to report is blurred and the consequences are not directly visible, such as cybersecurity, a solution is to give employees the opportunity to also report risks.

Figure 3: Reporting an incident by speaking directly to an IT technician or reporting a risk case by leaving a voice recording and answering a brief questionnaire.

Technical Analysis and resolution

Technical analysis and resolution phase introduces that whether it is an accident or a risk, the technicians analyse the situation giving priority to incidents. In the case of the accident, the resolution must be timely so as not to further damage data or systems, over this informs the reporting user that everything has also been resolved thanks to to its contribution. In the case of risk, the task of technicians is to assess its level - high, moderate or severe -, and check whether it actually had no consequences: if it did, it became an accident. Even in this case, the technicians give feedback to the reporter, thanking him for the communication. At the end of both types of analysis, the technical team draws up the report with the technical analysis that will be needed in the next step.

Audit and storytelling

The next stage takes its cue from what usually follows an adverse case, such as in the clinical field, the audit. Who reported the incident, any other persons involved, human resources managers and technicians get together to reconstruct what happened, whether it is a accident or a risk that had no consequences, because it is important for an organisation to learn from what goes right [10]. During this audit all points of view are welcomed without judgement, but above all without blaming or punishing the protagonists of the event. On the contrary, the whole reconstruction serves to produce a 'case study' in a participatory manner, in so that it can be shared with the rest of the corporate population. And the best way to convey the narrative of an event is precisely the storytelling.

Why storytelling? Neuroscience suggests so. The most immediate is that we are social creatures who regularly relate with strangers, so stories are an effective way to convey information and important values from one individual or community to another. Stories are able to personal and emotionally charge and involve the brain more, and thus are better remembered, than the mere display of a series of facts [13]. Stories can motivate us, like the characters, to look inside ourselves and make changes to become better people [13].

Therefore a great way to bring an organisation to learn from an event is to tell about it. That is why the result of the audit phase must not be a record, a factual account, but a narrative. The narrative is made in the first person by the protagonist, whose identity is concealed by a pseudonym, and follows a fixed narrative structure to be used always, so as to facilitate its drafting.

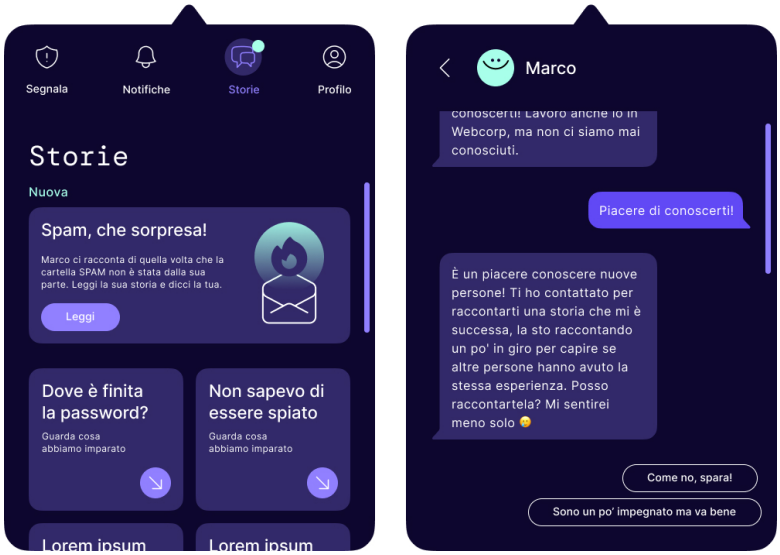

Figure 4: All the episodes are collected in "Stories". Every story is a chat that narrates the episode from the protagonist's point of view.

Data collection and learning

After the corporate population has participated and answered questions of the story, response data are collected, analysed, aggregated and provided participants with a visualisation that returns to them the value of their contribution. Also on the software application, everyone can find these data available whenever you want and understand how their opinions are valuable to the organisation so that it can learn at all levels. In fact, the results of this participation serve policy makers of cybersecurity as a fundamental basis from which to implement new ones or modify existing ones so that they are closer to capacity, the attitudes and behaviour of employees.

Figure 5: Data collected from the stories are shown in a simple visualization.

4.3. Prototyping

The interface design concludes the concept development phase and proceeds to the prototyping. The prototype is the representation of the design idea, the main purpose is to to make the design space explorable, in a tangible way, and to communicate the story of our vision our users and stakeholders to get their feedback [14]. In particular, my work of prototyping was carried out entirely on Figma, the most widely used software for interface design, starting from the screens designed in the previous phase. Here, interactions and basic micro-interactions were added, those necessary to switch between screens, for a medium/high fidelity prototype: i.e. the design of the interfaces is final and complete in detail, the interactions all present the necessary functions for the experience, but lacks refinement in the animations.

The prototype will serve, in the phase of presenting the concept to users, to give them the opportunity to interact with the project by making them identify with the end user and the reference scenario. In this way, stakeholders can see the constructed vision realised and will be able to judge how well it meets their expectations, their wishes and needs, providing information with a high level of validity and applicability [14].

The next step, therefore, is to involve stakeholders in the testing and evaluation of the concept. The next phase is crucial because, for the definition of the solution, the designers should obtain in-depth feedback on how the concept is perceived by the potential target audience [4].

4.4. Evaluation

Before involving the stakeholders, however, it is necessary to define the method of user experience evaluation. There are several and the one chosen in this case is the Anticipated Experience Evaluation (AXE), devised by Lutz Gegner and Mikael Runonen at Aalto University [4]. This method stems from one of the main challenges of user experience evaluation: describing the experiences with words is a difficult task, and making the user imagine a fictitious experience makes it even more challenging. If you ask a person to imagine and explain an experience, there will be a bias caused by the wording of the interviewer.

Another problem concerns the answers given by the participants, as words can be interpreted in infinite ways [4]. Thus, the AXE method aims to address these challenges proposing the use of image pairs as stimuli in user interviews. The AXE approach can be divided into three main phases: concept briefing, concept evaluation and data analysis.

The experiment was conducted following the steps and guidelines of the AXE method [4]. Participants in evaluations should ideally represent members of the intended target group. For this reason, the first choices immediately fell on two of the people interviewed during the qualitative research phase: one of the technicians and one of the non-expert employees. An expert in human factors and cybersecurity was also contacted to also have a more precise evaluation from this point of view. Once participants were chosen, they were contacted and told the purpose, the duration of the session.

Details of the evaluation session:

- Tool: Figma and Figjam
- Mean: Google Meet
- Total participants: No. 3
- Interview duration: 60 min

4.4.1. Protocol

Expert evaluators were introduced to the session according to the following protocol.

- Introduction to evaluation: preparation and setup to explain which instrument is used, in this case Figma and Figjam to facilitate remote interaction, and warn that the session will be recorded. Explanation of the reason for the evaluation and session protocol;

- Concept presentation and prototype testing, with the description of the concept, its purpose, functions and context in which is used. The description must be as faithful as possible to a real product. This aspect is very important because the description has an effect on the way the participant interprets a concept. Like introduction to the project, then, the respondent finds a small description which explains what Tellp is, what it does and for what purpose.

- Representational use scenario: a narrative in which a person uses the product in a specific context. The usage scenario takes the form of a short story that follows a classic plot. The story was accompanied by visual material, showing various design aspects of the product and its social and physical context of use. History is written using pronoun 'you' in the second person, to immerse the participant in the scenario. Specifically, each respondent was explained step by step the entire signalling process from signalling to learning by the organisation, asking them to imagine themselves in that situation.

- Prototype: the prototype was shown and the interviewees to interact with it during the scenario presentation. Step by step, at all stages of the usage scenario involving interaction with the interface, the story was suspended to let the respondent interacted autonomously with the application prototype.

- Evaluation session: explanation of the assessment instructions: the participant was explained that the questions placed consisted of pairs of opposing images to be compared. The question can be answered by placing an X along the line between the two images, close to the one that was considered most akin to the concept. Then participants had to indicate with an arrow the direction in which, according to the participant, the project should have aimed at. Finally, the participant had to explain why he chose it. The participants rated 6 pairs of images taken directly from the AXE method guide, plus one addition of your choice. The participant was not told how to interpret the meaning of the images, but was allowed to deduce it independently. After the choice, it has been asked why and, if necessary, specifically what elements of the project made that impression. Each response was never commented on or directed towards a desired result.

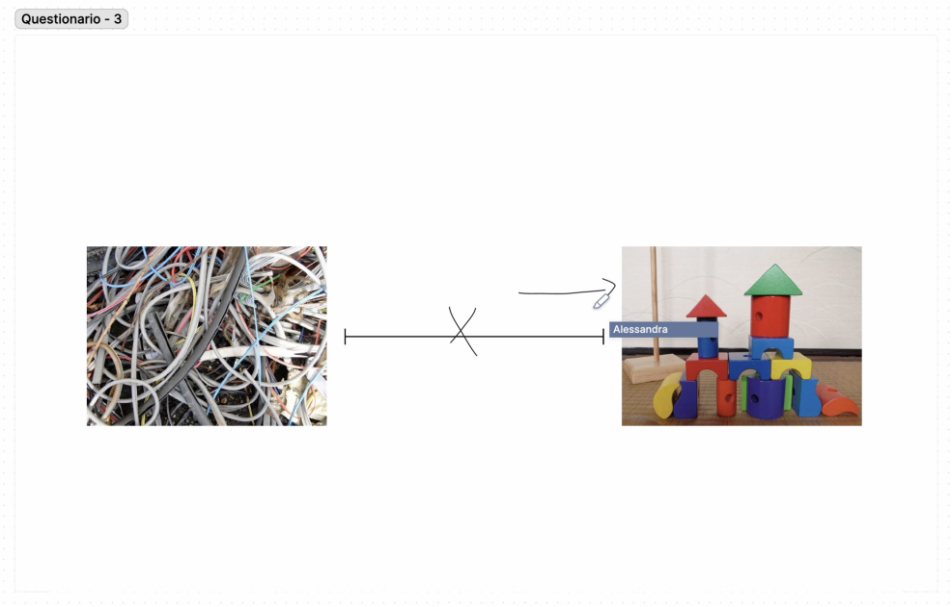

Figure 6: An example of the type of questions asked and the answer given by the evaluator.

4.4.2. Evaluation results

Regarding the whole process, from reporting to the final result, the general idea behind the Tellp concept was accepted by all respondents positively. The most frequent comments were concerned that you do not force reporting, do not guilt, do make the user feel comfortable in a stressful situation. The user, according to the interviewees, does not feel under indictment because the system allows for less anxiety and be more aware of the fact that mistakes can happen to everyone and why we value the contribution of the individual.

What drives the user to use this solution is sharing. The organisation of steps in the process seemed very clear, simple, orderly to everyone. The idea seemed innovative, current and feasible, useful and successful, in step with today's needs, because reporting is a long-standing problem for all organisations. Analysing a fact in such a simple way is useful because accidents and risks always happen in a company and therefore the use of the instrument and the resulting learning translates into dexterity skills against the attacks.

The objective was grasped by all as making team play to sensitise the individual and the masses. Being something in which everyone is involved, it allows for more conscious behaviour, making team against cybersecurity risks instead of standing alone.

Once the interviews were over, the next step was to listen to the recordings in order to analyse them. The analysis session data is used to break down the recording into smaller pieces of information through the transcription and encoding. The information obtained consists of pieces that are filtered into categories, dimensions and subjective evaluations [4].

Once the transcription is complete, the text has been divided into more manageable segments to bring them into categories, qualitative dimensions and relevant subjective evaluations. The categories represent different facets of the concept or activity related to the concept itself; the dimensions are different perspectives of perceived experiential quality of the concept on the part of the participants; subjective evaluation refers to the fact that the participants bring with them a positive or negative judgement [4].

The results of the interviews divided into categories according to this scheme were then aggregated to derive insights summarising the reactions and opinions of the respondents.

5. Discussion

This paragraph presents and discusses the main results of the research according to main dimensions found.

- Role of the human component. All interviewees noted a central role of the human component, although involving the use of a technological tool and being immersed in a very technical topic. Technology is seen as supporting people which must remain the focus. The human component therefore gave a feeling of warmth first for the main interaction that takes place between human beings, starting with the willingness of technicians to listen, and then because it implies the summation of experiences, a sharing that leads to the result. The person was seen as central since the system only works with the participation of the people.

- Reporting. Reporting was perceived positively by all respondents, seen as an action that the user is motivated to do, especially if there is awareness behind. The positive aspect lies in the fact that it is possible to speak, to tell by voice both on the call and in the recording audio: 'there is a personalisation not a depersonalisation' and reduces the stress of the task. One respondent pointed out that it could serve report a technical problem the nature of which is unknown, whether of cybersecurity or not. With the two possibilities given, it is assumed that everyone has a certain level of technical knowledge to discern about what it is. So if one does not know the nature of the problem and is reported as a risk, the user will have a longer response time, and this is dangerous if it turns out to be an accident or is otherwise a problem that remains for a while if it is only of a technical nature.

- Sharing the story. Respondents also reacted positively to the concept of sharing history with all colleagues because it evokes a sense of collectivity visible in reporter, who does not feel alone. In particular for one respondent the story made him empathise, made him more aware of what he could happen, and thought it might be the same for others, noting how very often accident data is read with distraction or boredom, instead, told in this way, they are more involving and participatory. The sense of community was also seen in the fact that in all employees, seeing their actions and responses valued, they feel part of the change in the organisation. One respondent pointed out that there is no incentive to participate in the stories. After the first few times when membership could be high, people might get bored and lose interest.

- Interaction. In general, the interaction seemed to everyone to be simple, smooth, easy understanding, intuitive, pleasant and requires no special skill or effort. The experience was positive for everyone, the dominant impression was that in general worked well. One respondent complained of an incomplete choice in the responses to the request to indicate the devices involved in the risk. They may want to choose more than one answer.

- Look and feel. From an aesthetic point of view, everyone agreed on the visual pleasantness of the interface, with adjectives such as 'beautiful', 'well done'. In particular a interviewee noted that cool colours suit both the subject and the corporate context. From the point of view of textual content, copy and titles, in interaction with the prototype it was possible to note that they were well accepted, e.g. one comment concerned the question "Do you need help?", considered very welcoming. In restitution cards, in particular those concerning open answers, one respondent noted that there is no real their own valuable information. In addition, it is not very clear that all those data will actually be useful for something. In addition, at the end of all restitution it must be more explicit that those will be used to improve something.

Although the evaluation could involve a very small number of people, their feedback is nevertheless a partial validation of the project because they were the first real external and disinterested opinions. Surely the positive balance is a good sign: the fact that three people among potential users and experts, have overall well received a project in its first version is a confirmation of a correct intuition and bodes well. It is the critical issues encountered, however, that are even more useful to understand what can be corrected and on which points more attention should be paid.

6. Conclusions

In a world like today's, so intrinsically connected to the virtual, organisations cannot remain vulnerable to cyber attacks, if these have recently seen an important increase in the their frequency and severity we can certainly expect the future to have new developments in store. But during this research, it became evident how the claim to defend a complex socio-technical system only with technological solutions has weak foundations, from the since such systems have a variety of elements them and that a single front of defence is not sufficient.

The assumption of focusing on the fundamental component of any organisation comes into play here. The human component, very often considered the weakest link, is instead the most valuable variable for a company. The way in which humans can prove so valuable is incident reporting, central theme of this study. During the course of the research, it became clear that a signalling system is deeply rooted in the culture security of a company and that therefore, to work on this front, one must keep it in mind.

The project was therefore configured as a service, a process that takes into account the mechanisms that lead to the formation of a culture that is just and respects skills, attitudes and behaviour of human beings. Human-centred design has made it possible to design a system that supports the reporting of the incident, provides an accurate analysis, free of judgement and blame, and points mainly on sharing stories to build empathic bonds between the employees of a company.

The ultimate goal of the project was not to look at the critical scenarios of cybersecurity as extraordinary and closed cases in a small context, but as events that can happen to everyone, so it is worth learning from them at all levels and sufficient awareness to strengthen the security culture. In this context, the assumption is that if the

organisation listens to all its voices is more inclined to build security that they are no longer detached from people, who are not barriers to their activities, but which take into account these last, the needs, the capacities of all.

Setting up the Tellp project made it possible to realise these assumptions and through them evaluate the value and viability of the idea. The feedback raised positive and the timely critical points that can only satisfy and make hope that, with the right corrections, the project can reach a form more comprehensive. Certainly more reasoning is needed in the future on the clarity of what to report and how, so as to remove the residual effort in the signalling that this project actually still carries.

In addition, one must actually think about how to maintain the population company involved and motivated to participate. Finally, one could certainly improve the usability of the interface in response methods and refine the return of data in a way that provides more valuable information. But in the end of this study, it can be assumed that, with due modifications, the idea could meet the needs identified in the research phase.

So, in the end, this project can be proposed as a valid proposal to the current vacuum in critical incident reporting systems of cybersecurity in companies and is a good starting point for continue to implement new solutions in this area.

References

1. I. Agrafiotis, J.R. Nurse, M. Goldsmith, S. Creese, D.M. Upton, A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate, J. Cybersecur., 4, tyy006, 2018.

2. V. Zimmermann, K. Renaud, Moving from a "Human-as-Problem" to a "Human-as-Solution" Cybersecurity Mindset. International Journal of Human-Computer Studies, 2019. doi: https://doi.org/10.1016/j.ijhcs.2019.05.005

3. M. A. Sasse, S. Brostoff, D. Weirich, Transforming the 'Weakest Link' — a Human/Computer Interaction Approach to Usable and Effective Security, BT Technology Journal, 19, 2001. 10.1023/A:1011902718709.

4. L. Gegner, M. Runonen, For what it is worth, Anticipated eXperience Evaluation, 8th International Conference on Design and Emotion: Out of Control - Proceedings, 2012.

5. M. O'Leary, S. L. Chappell, Confidential incident reporting systems create vital awareness of safety problems, ICAO journal, 51(8), 11–27, 1996.

6. J. Reason, Achieving a safe culture: Theory and practice, Work & Stress: An International Journal of Work, Health & Organisations, 12:3, 293-306, 1998. DOI: 10.1080/02678379808256868

7. A. Pasquini, S. Pozzi, L. Save, Mark-Alexander Sujan, Requisites for successful incident reporting in resilient organisations, In: E. Hollnagel, J. Paries, D. D. Woods, J. Wreathall, (eds.) Resilience engineering in practice : a guidebook, Ashgate studies in resilience engineering, Farnham, Surrey, England; Burlington, VT: Ashgate, pp. 237-254, 2011. ISBN 9781409410355

8. S. W. Dekker, Just culture: Who gets to draw the line?, Cognition, Technology & Work, 11(3), 177–185, 2009. https://doi.org/10.1007/s10111-008-0110-7

9. S. W. Dekker, Employees: A Problem to Control or Solution To Harness?, Professional safety, 59, 32-36, 2014.

10. E. Hollnagel, R. L. Wears, J. Braithwaite, From Safety-I to Safety-II: A White Paper, The Resilient Health Care Net: Published simultaneously by the University of Southern Denmark, University of Florida, USA, and Macquarie University, Australia, 2015.

11. P. Briggs, D. Jeske, L. Coventry, The Design of Messages to Improve Cybersecurity Incident Reporting, In: T. Tryfonas, (eds) Human Aspects of Information Security, Privacy and Trust, HAS 2017, Lecture Notes in Computer Science(), vol 10292, Springer, Cham, 2017. https://doi.org/10.1007/978-3-319-58460-7_1

12. R. W. Rogers, A Protection Motivation Theory of Fear Appeals and Attitude Change1, The Journal of Psychology, 91:1, 93-114, 1975. DOI:10.1080/00223980.1975.9915803

13. P. Zak, How Stories Change the Brain, Greater Good Magazine, The Greater Good Science Center at the University of California, Berkeley, 2013. https://greatergood.berkeley.edu/article/item/how_stories_change_brain

14. A. Rizzo, Ergonomia cognitiva: Dalle origini al design thinking, Il Mulino, 2020.