

Encouraging Organisational Information Security Incident Reporting

FABIAN LUCAS BALLREICH, SECUSO, Karlsruhe Institute of Technology, Germany

MELANIE VOLKAMER, SECUSO, Karlsruhe Institute of Technology, Germany

DIRK MÜLLMANN, SECUSO, Karlsruhe Institute of Technology, Germany

BENJAMIN MAXIMILIAN BERENS, SECUSO, Karlsruhe Institute of Technology, Germany

ELENA MARIE HÄUSSLER, SECUSO, Karlsruhe Institute of Technology, Germany

KAREN V. RENAUD, University of Strathclyde, Scotland; University of South Africa, RSA; Abertay University, UK; Rhodes University, RSA

21st-century organisations can only learn how to respond effectively to, and recover from, adverse information security incidents if their employees report any incidents they notice. This should happen irrespective of whether or not they themselves triggered the incident. Organisations have started to inform their employees about their incident reporting obligations. However, there is little research that organisations can benefit from to make their reporting provisions maximally effective. For this work, we follow a multi-step approach. (1) We review the related research on reporting, including reporting reluctance, and the legalities of incident reporting in the European Union. (2) We explain how we developed variations of information texts that raise awareness of incident reporting obligations and aim to ameliorate reporting reluctance. (3) We conducted an online user study (n=257) to identify the most effective information text. (4) The most effective text was deployed by the CISO of a German energy company and we collected feedback from 24 employees to support a qualitative analysis. We discuss our experiences and the implications of such information text design. We make recommendations for encouraging information security incident reporting and suggest future work.

Additional Key Words and Phrases: Barriers to information security incident reporting; reporting reluctance, information security incidents, reporting obligation

ACM Reference Format:

Fabian Lucas Ballreich, Melanie Volkamer, Dirk Müllmann, Benjamin Maximilian Berens, Elena Marie Häußler, and Karen V. Renaud. 2018. Encouraging Organisational Information Security Incident Reporting. In *The 2023 European Symposium on Usable Security, October 16 & 17, 2023, Copenhagen, Denmark*. ACM, New York, NY, USA, 35 pages. <https://doi.org/XXXXXXXX.XXXXXXX>

1 INTRODUCTION

Cybersecurity is a concern to organisations globally [19]. Organisations deploy a wide variety of measures to prevent cyber-attacks and data losses. Despite their best efforts, employees sometimes make unforced errors or are deceived: inadvertently leaking sensitive data or damaging the IT infrastructure in some way. Under European law incident reporting for organisations that operate critical infrastructure is considered so important that it has been regulated and mandated to report incidents to the authorities if there are breaches. Thus, if data is leaked, such organisations in the

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

© 2018 Association for Computing Machinery.
Manuscript submitted to ACM

European Union¹ and the UK are required to report, by law². A failure by organisations to report information security incidents could result in punitive fines [38].

Organisations can only feasibly comply with reporting mandates if employees help to reveal past or ongoing information security incidents, whether caused by a mistake or because something anomalous comes to their attention. If employees report the incidents as soon as they occur, security teams can take remedial action and limit the potential damage [21, 25]. If employees fail in this responsibility, greater harm could ensue [14]. For example, if access credentials have leaked, swift reporting could speed up the disabling of the account and prevent the usage of these credentials to gain access to organisational systems. Keeping quiet allows hackers free rein to carry out nefarious and damaging activities. Due to the penalized legal duty to report and the necessity to limit possible damage at an early stage it is important to increase reporting rates under their employees and not only reduce the possible effect of incidents by default. Incident reporting of employees, hence, is an important aspect of the security concept of any organisation, not just of those operating critical infrastructures.

Requiring employees to report seems simple enough, and such reports undoubtedly improve organisational security [39], but it should be borne in mind that a range of motivations could prevent or deter information security incident reporting [28].

To increase the likelihood that employees will report information security incidents, some organisations disseminate information texts that emphasise their information security incident reporting obligations [37]. However, people will only act on these obligations if they are aware of *what* to report, and *how* to report. Moreover, such reporting should be - as far as possible - risk-free. If not, employees might well refrain from reporting incidents.

In this paper, an information text was developed and evaluated using a multi-step procedure as shown in Figure 1, which is intended to increase the willingness to report information security incidents and reduce concerns about personal risks through reporting. First, we conducted an analysis of the legal background with a focus on the reporting of incidents by operators of critical infrastructure as well as the employees reporting obligations to their employers. Based on this, various text versions were developed and improved in a multi-step approach, with each text consisting of a motivating and awareness-raising part. The authors of this work with different professional backgrounds as well as three CISOs from different organizations were involved in this. After that, we conducted an online user study using clickworkers to evaluate the different developed information texts. Here the emotions triggered by the respective texts as well as the participant's ability to recognise and correctly rate real-life scenarios were assessed. In addition, data on the previous knowledge of the participants in the area of incident reporting obligation was collected. A final text proposal was created based on the results of the user study.

This proposed text was then used to inform all employees of a German energy company, with their feedback being collected via an online questionnaire. Based on the those results and additional feedback from the company's Chief Information Security Officer (CISO), we conclude with lessons learned from the deployment of our information text.

Whereas section 2 reviews the latest research related to cybercrime reporting, section 3 provides some legal background on information security incident reporting particularly in Germany. Section 4 then provides details of the information texts and how it was developed. Section 5 explains how these information texts were evaluated. Section 6 then details how the derived proposal was applied and tested in a German energy company. Section 7 discusses the findings and provides lessons learned for the benefit of other companies.

¹[https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2020\)654198](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2020)654198)

²<https://ico.org.uk/>

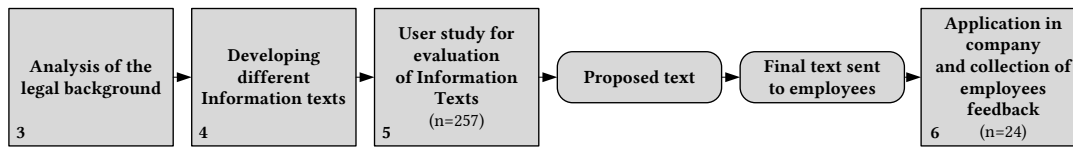


Fig. 1. Overview of all steps in this paper. The number on the left refers to the section that covers the step. Rounded boxes symbolize text versions.

2 BACKGROUND

When citizens experience cybercrime in their everyday lives it is highly important to be reported [25]. The higher the number of events they are aware of, the more insights are gained into the nature and scale of the crimes. This will inform policymakers, enabling the development of effective responses. Higher reporting can also help to develop cybercrime victimology. Some countries have established cybercrime reporting portals e.g., Nigeria [18], Taiwan [22], UK [26] and India [20] for their citizens. With these portals, they hope to encourage and ease reporting of cybercrimes. Though a key issue is how best to communicate the risks associated with such incidents to the user. There are differences between young and older adults with regard to risk perception and risk behaviour. For instance, elderly adults may benefit from explaining content through informational videos rather than just text [12, 13]. Such factors should therefore be included in the planning and evaluation of measures.

However the general public under-reports cybercrimes [2, 16, 22, 24, 27, 32, 35]. A survey carried out in 2006 in the UK revealed that only 13% of individual victims report cybercrimes [45]. This is curious because victims considered these crimes equivalent to traditional crimes like burglary in terms of their trauma and impact [4]. The described reluctance to report cybercrimes might well carry over into work life and thereby affect the reporting of information security incidents as well [17, 43]. There are a number of reasons for incidents to be under-reported in the corporate context, including:

- (1) To report, an employee needs to know *what* an information security incident looks like and *how* to report it [6, 7]. This seems to be hindered by the lack of a generally accepted and commonly known definition of such incidents and thereby the difficulty to give diverse practical examples.
- (2) Some victims may fear *sanctions* from their employers if they report that they themselves mistakenly triggered an information security incident [2, 36, 42].
- (3) Victims may feel *negative emotions* about falling victim to a cybercrime [46]. If they think no one will find out, they will probably try to avoid the embarrassment of reporting [8].
- (4) The organisation may have failed to hire a *person with demonstrable response capabilities* [29] or have hired someone who blames and shames employees who report incidents [33]. If employees lack faith in the organisation's incident responses or have seen them, they are likely to refrain from reporting.

In the private context, researchers have identified further reasons for reporting reluctance. In this case, it would be inappropriate to report to security officers within an organisation so it is likely that they would need to report to the police.

- (1) It might be that people do not have faith in the police or official authorities to address cyber crimes [46]. As such, they might choose rather report the crime to their bank, if it is fraud [22], or to their Internet service provider

- [45]. People may believe that reporting is futile i.e. they might not believe that the criminals will be prosecuted [8], given that the criminals might be located in another country where their police force has no jurisdiction.
- (2) Some victims may believe that the crime is minor and not worth reporting [46]. They don't want to spend the time engaging with reporting, nor risk being victim-blamed.

With respect to our study, the second list contains barriers that are more applicable to cybercrime reporting outside organisations. The fourth item mentioned in the first list is something that organisations ought to put in place *before* organisations launch any intervention to encourage employees to report incidents. As such, our information text ought to address barriers 1-3 of the first list in order to encourage reporting.

3 LEGAL BACKGROUND ON INFORMATION SECURITY INCIDENT REPORTING

Both the area of reporting IT security incidents by operators of critical infrastructures and the topic of employees' obligations to their employers are clearly regulated by law. Since it is mandatory that these regulations had to be taken into account when creating information texts and conducting a study, the applicable legal principles will be briefly presented. For the European Union, the cyber security reporting obligation for organisations that operate critical infrastructure is defined in Article 16 sec. 3 NIS Directive [9]. All member states have to transport the NIS directive into national law, i.e. also Article 16 and thereby defining the cyber security reporting obligation for organisations. How this has been implemented differs from country to country. As our research focuses on the German context, we summarise the situation in Germany: Article 16 sec. 3 NIS Directive is addressed in § 8b sec. 4 BSIG [10]. Here, it is mandated for organisations to report any disruptions to the availability, integrity, authenticity and confidentiality of their information technology systems, components or processes. Reports have to be submitted to the German Federal Office for Information Security immediately, i.e. without culpable hesitation.

In order for companies to be able to comply with legal reporting obligations, the cooperation of their employees, who are generally the first to learn of information security incidents, is essential. Note that sometimes they might even cause them. With respect to their employees reporting incidents, countries or individual organisations may already have some legal requirements or policies. These may be so general that they cover reporting on cyber security incident reporting already. In Germany, for instance, employees are subject to a duty to notify their employers, i.e. the duty to provide information without being asked [15, 40]. This arises as a legal secondary duty from the employment relationship [31, 34, 40]. Furthermore, German employees are required to protect the organisation's interest in the integrity and thus to avert damage in the form of imminent disruption or damage to its operating resources [31, 34]. As a consequence, reporting is mandatory in order to prevent further and more far-reaching damage to the organisation. As such, to comply with the duty to mitigate damage incumbent on employees, reporting is required [34, 40]. All these duties also apply to information security incidents that are caused by employees or are observed by them.

Note that while our focus is on Germany, comparable situations exist in other countries (cf. [5] for the US or [23] for Australia).

4 INFORMATION TEXT DEVELOPMENT PROCESS

The goal of the information text was to address those factors identified by related work that might well deter information security incident reporting. The text should raise *awareness* on *how* to report information security incidents, and *what* information security incidents are (covering anomalies they notice, as well as incidents they have triggered). Furthermore,

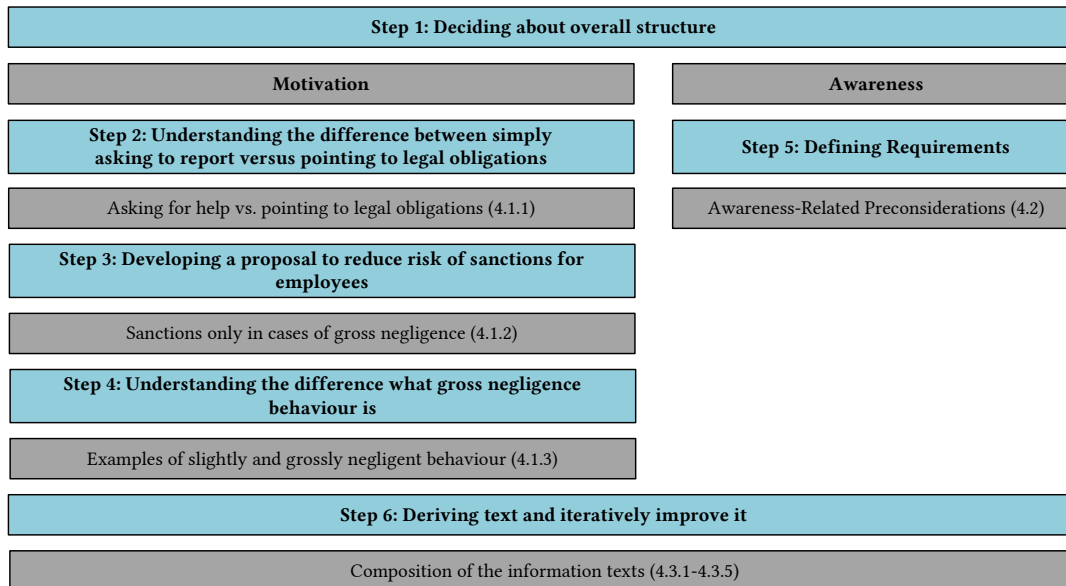


Fig. 2. Conducted process for developing different information texts. Blue boxes contain process steps 1-6. The left side contains steps for motivating to report incidents, and the right side contains steps for raising awareness i.e. to whom to report. Grey boxes refer to sections the result of each step is covered in.

it should *motivate* employees to report (i.e. address their fear of sanctions)³. Figure 2 provides an overview of the multi-step process used to develop the information text. The process was conducted by the authors of this work, who have backgrounds in security, law and information systems. In addition, three CISOs from different organisations, who were known from previous projects, were asked to provide written feedback and suggestions for improvement on the individual parts of the texts developed. In Step 1, we commenced developing the information text with the motivational parts to address reservations right at the outset, and then to continue with the informative content including how to report and details about incidents. We first focused on the motivational part and the understanding of the legal situation (see Section 4.1). Note that it might be most motivating for employees to report incidence if the text says that there will be no sanctions at all, independent from who and what behaviour may have caused the information security incident. However, that might be not acceptable for the legal and/or human resource department of the organisation, as this would mean even repeated gross negligence behaviours could not be sanctioned by the employer. As such, we focused first on understanding the differences between simply asking employees to report security incidences versus pointing them to their legal obligations to do so (Step 2, see Section 4.1.1). Afterwards, we developed a proposal to communicate the reduction in the risk of sanctions for employees (Step 3, see Section 4.1.2). As this proposal distinguishes between *slightly* and *grossly* negligent behaviours in terms of sanctioning, we next focused on understanding the differences between those in the context of information security incidences (Step 4, see Section 4.1.3). Afterwards, we focused on

³Note, related work also identified 'feeling ashamed' and 'lacking person in charge' as factors which keep employees from reporting incidence. We consider the last one as a precondition to start informing employees with any text about their obligation to report incidents. The first one is related to the organisational culture. While we also consider this as an important factor, an information text has little impact on the culture. In case of issues, these need to be addressed with large campaigns.

the awareness part. Here, initially, we derived (Step 5, see Section 4.2) from the awareness literature for both aspects (*how* to report and *what* to report). Finally, we deduced text proposals for the five different parts (Step 6, see Section 4.3). Note that for parts 1 and 3 we proposed different options. The reasons are discussed in corresponding subsections.

4.1 Legal Preconsiderations

The general obligation for organisations to report incidents is similar all over the European Union and in the UK. However, additional legal requirements may be relevant, which differ from country to country. The goal of this subsection is to better understand the situation in Germany (given that the information text was evaluated in Germany). Note that while the process to develop such an information text is generalisable, the actual text may change depending on the country.

4.1.1 Asking for help vs. pointing to legal obligations. An obvious, simple, and socially sound approach to improving willingness to report incidents was to ask employees to report them, thereby assisting the organisation. However, depending on the wording of this request, there is a fundamental problem. Such an approach could be misunderstood by employees in that it could give the impression that it is only a request and not, as it is in reality, a legal obligation on the part of employees. If reporting obligations are neglected, it could be argued that employees were unaware of the obligatory nature of this request. Until this obligation is clarified, for example in a personal conversation after an incident, employees would have a free shot at failing to report, without the company being able to take sanctions against them, no matter how severe the incident was. This is neither in the interest of cybersecurity nor of the company. Hence, the wording needs to be unambiguous so that employees understand that the consequence for not reporting could include sanctions. Against this background, the reference in the information texts to the obligation to report and possible consequences of its neglect could not be omitted across the board, even if this could be perceived as threatening by employees.

4.1.2 Sanctions only in cases of gross negligence. Employees ought to report incidents but this might entail reporting their own misconduct or mistakes. They might well dread that if they report, they could subsequently face consequences under their country's employment law.

This prospect may well discourage employees from complying with their duty to report incidents. In these cases, this is *a fortiori*, not in the employee's interests to report, nor in the employer's interests for such considerations to prevent reporting. Due to this, an employee might decide not to fulfil their reporting obligations and not to take required countermeasures to deal with the information security incident. If the incident goes unreported and therefore undetected, there is a risk that damage will spread to other systems and exacerbate the harm. To avoid this, it has been proposed, in the legal literature, that consequences be waived under labour law, depending on the degree of employee culpability (see [30, p.8]).

The principles of company damage compensation have been developed by courts in Germany, and also have a legal basis in Austria with §2 of the Employees' Liability Act (Dienstnehmerhaftpflichtgesetz) [1]. Under these principles, an employee would only face consequences for damages they caused, under labour law, where malicious intent and/or gross negligence can be proven. If the employees have only been (slightly) negligent, they would not be subject to any punitive consequences under employment law. Negligence can be defined as "the disregard of the care required" (cf. § 276 sec. 2 Bürgerliches Gesetzbuch (BGB)). Gross negligence is a particularly serious breach of the objectively required diligence[40]. Even if the legal-dogmatic derivation in the case of information security incidents is different from the

case of company damage compensation, it is likely that this would increase the willingness of employees to report information safety incidents and thereby improve organisational cybersecurity as a consequence.

4.1.3 Examples of slightly and grossly negligent behaviour. In order to understand the proposed offer to only sanction grossly negligent behaviour, it is important for the employee to understand the difference between slightly and grossly negligent behaviour. This is particularly pertinent in the cyber security context. Thus, for employees who might not be familiar with the differences, it is helpful to provide examples. We developed examples based on actual court decisions and the legal literature. To this end, a literature search was conducted to reveal court decisions in this respect. This involved a targeted search for judgments and legal articles that dealt with the legal assessment of information security incidents. The articles and decisions identified in this way were analyzed in a second step to determine what behaviour triggered the incident in question and how the culpability of the person triggering the incident was assessed by the court or the author. After analyzing the identified decisions and articles, the corresponding triggers of the incident were abstracted and compared. Where the comparison revealed that the incident was caused by similar or identical triggers, the examples were combined into a case group. Then, the degrees of culpability assigned by the court were compared. A subjective check aligned these with the statutory definitions with regard to their classification. If the comparison showed a plausible assignment and the trigger of the information security incident was assigned to the identical form of fault in at least three sources, the abstracted case group was made the basis of one of the examples. For this purpose, a life situation was designed on the basis of the abstracted facts of the case, which contained the legally relevant key points, placed in a context that would be easy to understand.⁴ All developed examples can be found in the Appendix.

4.2 Awareness-Related Considerations

In this part of the text, employees should be informed about how to report and what should be reported, i.e. what is an information security incident.

Regarding the first aspect, we agreed that reporting should be as easy as possible, i.e. ideally there is only one entity (e.g. the CISO or the service desk) mentioned to get in touch with; while this can be done via telephone, email or web portal. It is important to provide several channels e.g. to address cases in which the end device cannot be used anymore due to a malware infection. Furthermore, we agreed that the type of information needed to (formally) report an incident should not be mentioned as this may easily come across as not doable or too complex and may keep employees from reporting. Once the person has contacted the responsible entity, they can ask for the necessary information to proceed.

Regarding the second aspect, we agreed that a concrete list of security incidence that an organisation wants their employees to report is more valuable than an abstract description of what an information security incident is. In order to come up with a proposal for such a list, we searched for actual incidents that were reported by organisations and/or media as well as those having been discussed at German courts. There are two types of incidence: (1) those that can be detected and as such reported by everyone, even without technical know-how or having participated in some security training; and then those that may require additional information. We identified for the first list the following for incidence: (1) Loss of computing devices, (2) Loss of storage devices, (3) Additional devices such as routers, (4) Being blackmailed or coerced to break security rules like providing sensitive information e.g. passwords. For the second list, the following two types of incidences were identified: (1) Malware on computing devices, and (2) Identity theft.

⁴The examples can be found in: State Labour Court Düsseldorf, Judgement from 29.08.2017, 14 Sa 334/17; State Labour Court Berlin-Brandenburg, Judgement from 01.09.2016, 10 Sa 1902/16; District Court Bonn, Judgement from 11.11.2020, 29 OWi 1/20; Higher Regional Court Thüringen, Judgement from 18.08.2004, 2 U 1038/03; District Court Darmstadt, Judgement from 26.05.2020, 13 O 244/19

Once we agreed on the list, we discussed how best to present this information to employees. We agreed that it might be unrealistic to assume that one remembers all this information after having read it only once. Providing it in the intranet is important but might not be enough if an information security incident occurs and employees have no access. Therefore, we decided to provide that information in a poster which should be placed next to other posters that one typically finds in the offices such as those related to fire alarms and medical emergencies. See Appendix for the poster.

4.3 Composition of the Information Texts

Each information text consists of five parts depending on the content, whereas for some parts (1 and 3) multiple text options are available. The parts are described in the following. Figure 3 shows the composition of the different information texts. Which one is the most promising one will be analysed in the user study described in Section 5. The English translation of the actual text is provided in the Appendix.

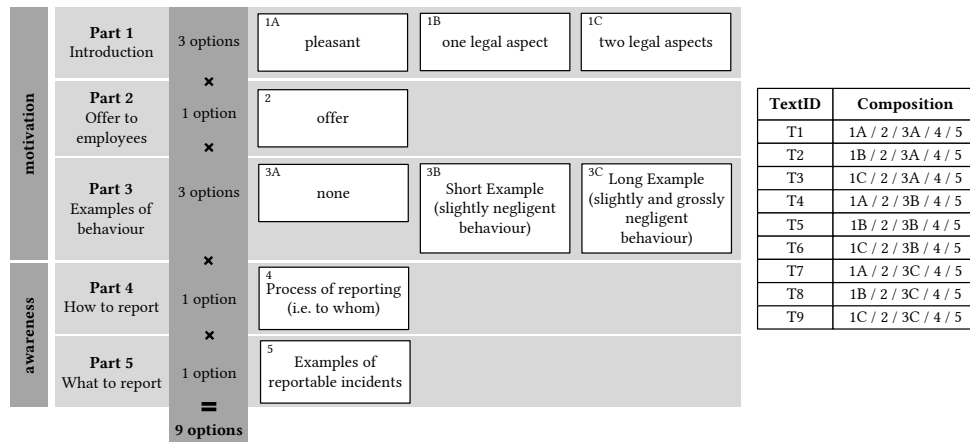


Fig. 3. Each created information text consists of five parts. There are multiple options for parts 1 (Introduction) and 3 (Example of behaviour). The table on the right side shows all nine possible combinations of the options and the respective defined TextIDs.

4.3.1 Part 1: Introduction. In this part, we want to introduce the obligation for employees to report incidents. While the conclusion from the considerations in Section 4.1.1 is that it is necessary to clearly speak about the obligations to be safe from a legal point of view, we worried, that starting the information with very legal-ish text might cause too many negative emotions, we developed three different options which differ according to their degree of formality for the introduction. The idea was to run a user study to see whether the most formal one really causes significantly more negative emotions or not, and then decide which one to include in the final proposal.

4.3.2 Part 2: Offer to Employees. As explained in section 4.1, we want to increase employee motivation to report incidents by waiving consequences under certain circumstances, depending on the degree of employee culpability and potential negligence. Therefore, in this part, we explain that the employer will refrain from sanctioning employees who report incidents caused by their own (slightly) negligent behaviours.

4.3.3 *Part 3: Examples of Behaviour.* We agreed that it is necessary to provide examples of (slightly) negligent and grossly negligent behaviour as this might not be common knowledge. However, the consequence is that the text gets very long and long text is less likely to be read. Therefore, we decided to have two different options, with examples. The short option (102 words) mentions only examples of (slightly) negligent behaviours, the long option (361 words) also addresses gross negligence. The idea was to run a user study whether it is necessary to provide such information at all and if yes whether the short text is enough or if it needs to be recommended to include the longer text. As such, this part consists of three different options.

4.3.4 *Part 4: How to Report.* This part basically explains how reporting is organised and to whom employees should report incidents taking the requirements identified in Section 4.2 into account. It includes the advice that if employees are unsure about whether an incident is considered to be reportable or if they notice something out of the ordinary, they can contact the CISO or the IT department who will be happy to assist.

4.3.5 *Part 5: What to Report.* The last part gives several examples that were derived as described in Section 4.2 of reportable information security incidents referring to the poster in the Appendix. It is recommended to print it and post it in the office.

5 EVALUATION OF INFORMATION TEXTS

In this Section, we commence by introducing the research questions including the hypotheses and discussing the design of the user study. Afterwards, we address the applied analysis methods, summarise the results and produce a final proposal for the most effective formulation of an information text to encourage incident reporting.

5.1 Research Questions and Hypotheses

Our user study aimed to evaluate the in Section 4 created different information texts and to determine a proposal. Therefore we define the following research questions with the corresponding defined hypotheses

RQ1 *How does each of our information text perform, in terms of raised positive and negative emotions (measured using the Positive and Negative Affect Scale)?*

- $H_{1,0}$: There is no significant difference in terms of causing **positive** emotions for texts with a **pleasant introduction (option 1A)** in comparison to texts with **one legal aspect (option 1B)**.
- $H_{2,0}$: There is no significant difference in terms of causing **negative** emotions for texts with a **pleasant introduction (option 1A)** in comparison to texts with **one legal aspect (option 1B)**.
- $H_{3,0}$: There is no significant difference in terms of caused **positive** emotions for texts with a **pleasant introduction (option 1A)** in comparison to texts with **two legal aspects (option 1C)**.
- $H_{4,0}$: There is no significant difference in terms of causing **negative** emotions for texts with a **pleasant introduction (option 1A)** in comparison to texts with **two legal aspects (option 1C)**.
- $H_{5,0}$: There is no significant difference in terms of causing **positive** emotions for texts with **one legal aspect (option 1B)** in comparison to texts with **two legal aspects (option 1C)**.
- $H_{6,0}$: There is no significant difference in terms of causing **negative** emotions for texts with **one legal aspect (option 1B)** in comparison to texts with **two legal aspects (option 1C)**.

RQ2 How does each of our information texts perform, in terms of increasing capability to correctly rate information security incidents?

- $H_{7,0}$: There is no significant difference in terms of capability to correctly rate information security incidents for texts with **no example (option 3A)** in comparison to texts with **short examples (option 3B)**.
- $H_{8,0}$: There is no significant difference in terms of capability to correctly rate information security incidents for texts with **no example (option 3A)** in comparison to texts with **long examples (option 3C)**.
- $H_{9,0}$: There is no significant difference in terms of capability to correctly rate information security incidents for texts with **short examples (option 3B)** in comparison to texts with **long examples (option 3C)**.

5.2 User Study

In this section, we first explain the design of the user study and the questionnaire, applied for the evaluation of the different information texts. Afterwards, we describe the ethical considerations as well as the limitations.

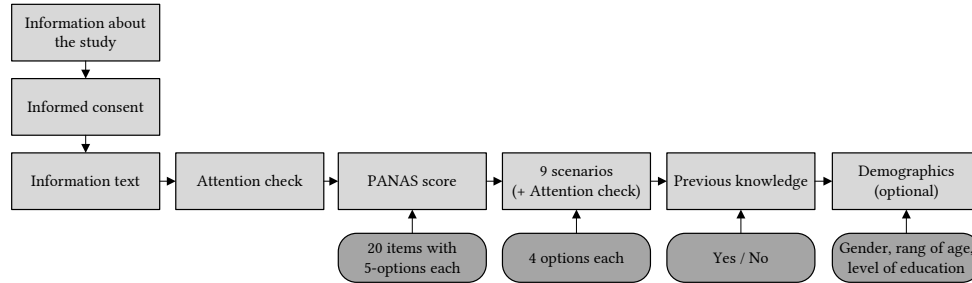


Fig. 4. Process of the user study (n=257). First randomly one information text was shown. PANAS score for valuation of emotions. Rating of nine different scenarios as (slightly) negligent, grossly negligent, intentional or none of the options. Previous knowledge about incident reporting and demographics.

5.2.1 Study Design and Questionnaire. Figure 4 depicts the flow chart of the user study. After the participants were informed about the purpose of the user study randomly one of the nine different information texts was presented, followed by an attention check question. Hereafter we evaluated the emotions triggered by the respective information text using the Positive and Negative Affect Scale. For assessing participants' ability to recognise incidents and rate scenarios as slightly and grossly negligent we presented them with nine different scenarios one after another and an additional attention check question. Each scenario has to be rated as (slightly) negligent, grossly negligent, intentional or as none of the three options. All scenarios had been developed by again applying the approach described in 4.1.3. However, those were different compared to the scenarios used in the information texts, which is why the participants had to make a transfer effort during the assessment. Subsequently, the participants were asked, if they had already been informed about information security incidents or reporting obligations in general. The questionnaire ended with questions about demographics.

5.2.2 Ethics. The participants of this study were recruited using the Clickworker platform and paid 5€ for their participation, which was pretested to take about 30 minutes. This corresponds to an hourly fee exceeding the minimum wage in Germany at the time of the study. To ensure data quality, the questionnaire included two attention questions.

One question was presented directly after the text, and another during the rating of the scenarios. Although there is no mandatory ethical review process at our institution, we ensured that there was no harm being done to the participants. Therefore, we provided full information about the objectives of the study and asked them for their informed consent. Participation was anonymized and they could withdraw at any time.

5.3 Results

In this section, we first provide demographic information about our participants, followed by the statistical analysis and results for both research questions.

5.3.1 Participants. The user study was conducted in June 2022 using the Clickworker platform whereby the sample population was randomly selected. For selecting participants the only applied restrictions were the age (18 years or older) and the country of origin (Germany). There were no constraints based on i.e. gender, educational level or current employment status. Of the 311 participants who completed the study, we had to exclude 54 from the analysis because they did not open the given examples for (slightly) negligent and grossly negligent behaviour in part 3 or the examples of reportable information security incidents in poster format in part 5. Since 126 and 128 of the remaining 257 participants stated that they were male or female, the sample can be considered as distributed equally with respect to gender. 67 and 140 participants said that they were younger than 30 years of age, or between 30 and 50 years of age. 50 participants considered themselves between 50 and 65 years of age, and 7 stated that they were 65 or older. About half of all participants (126) had an academic degree and 65 said that a high-school diploma was their highest level of education. Asked if they have been informed about information security incidents or reporting obligations in general, 109 answered yes, whereas 148 did not receive any information in the past.

5.3.2 RQ1 - Selection of Introduction Option . For the evaluation of emotions triggered by the information texts, we used the German version of the *Positive and Negative Affect Scale* scale (PANAS) [3, 44]. We calculated the values for the positive and negative affect for each of the three different options for introduction including all possible combinations of parts 2 to 5. For example, the texts T1, T4 and T7 (see Table in 3) were considered as one group for the option *pleasant* and compared to both respective other groups of introductions. Both values are based on 10 different items each, which are rated on a 5-point scale of 1 (not at all) to 5 (very much). Both values range from 10 to 50, with a higher value representing stronger emotions with respect to their affiliation.

Since six Participants had to be excluded from this analysis due to incomplete answers, we ended up with 83 participants with the *two legal aspects* (T3, T6 and T9), 90 with the *one legal aspect* (T2, T5 and T8) and 78 with the *pleasant* introduction (T1, T4 and T7).

For both the positive and the negative affect, we tested the necessary assumptions for the one-way analysis of variance (ANOVA) between the three groups of introductions.[11] (1) Each participant of the user study only got an information text with one of the three possible introductions, therefor independence of the samples is given. (2) Dependent variables at least interval scaled and, (3) the distribution within the groups is normally distributed. (4) For both values, the positive and the negative affect, the homogeneity of variance was tested using Levene's test within the three groups.

The one-way ANOVA revealed no significant differences across the three groups for the positive affect ($F(2,248) = 1.138, p=0,322$), nor for the negative affect ($F(2,248) = 1.349, p=0,261$). Therefore $H_{1,0}$, $H_{2,0}$, $H_{3,0}$, $H_{4,0}$, $H_{5,0}$ and $H_{6,0}$ could not be rejected.

Group	n	positive affect		negative affect	
		mean	sd	mean	sd
pleasant	78	29.41	6.89	15.9	5.42
one legal aspect	90	27.78	7.12	15.03	5.64
two legal aspect	83	29.41	6.89	16.61	7.72

Table 1. Descriptive values of positive and negative affect for all text versions with pleasant, one legal aspect and two legal aspects introductions.

The descriptive values for positive and negative affect are: for the pleasant (pos: mean=29.41, sd=6.89 / neg: mean=15.9, sd=5.42 / n=78), for the one legal aspect (pos: mean=27.78, sd=7.12 / neg: mean=15.03, sd=5.64 / n=90), as well as for the two legal aspects introduction (pos: mean=29.41, sd=6.89 / neg: mean=16.61, sd=7.72 / n=83). As mentioned in Section 4.1.1, the two legal aspects introduction represents the preferred option from the employer’s perspective, with respect to legal compliance. Therefore, we decided to choose this introduction for the proposed information text, if it did not cause a significantly stronger negative affect nor a significantly lower positive affect compared to both other options. **Since we could not show a significant difference for both values, we decided to use the most legal introduction for the proposed information text.**

5.3.3 *RQ2 - Selection of Example Option*. For assessing participants’ ability to recognise incidents and rate scenarios as slightly and grossly negligent we presented them with nine different scenarios one after another. Based on the legal pre-considerations outlined in Section 4.1.3 we, therefore, created seven scenarios, which describe slightly negligent behaviours, as well as two grossly negligent scenarios. For each scenario, the participants had to rate them as (1) slightly negligent, (2) grossly negligent, (3) intentional or (4) none of the three options. With respect to the presented option of part 3, we formed the groups: (1) no example, (2) short example, and (3) long example. For every group, we calculated the dependent variable *correctly rated scenarios* as the total number of correctly rated scenarios per participant, in the sense that the selected option matches our particular definition. Consequently, this variable ranges from zero to nine, whereby a higher value is defined as an increased ability to rate scenarios correctly.

The necessary assumptions for the one-way analysis of variance were tested as explained in Section 5.3.2. For the one-way ANOVA, there was a significant difference across the three groups ($F(2,254) = 6.84, p < 0.01$). Afterwards, we conducted pairwise t-tests to check the differences between the means of the variable. Due to multiple comparisons, we used the Bonferroni correction method to adjust alpha levels. The t-tests revealed a significant difference between the “no example” and “long example” ($p < 0.05$), as well as between the “short example” and “long example” ($p < 0.01$). However, no significant difference emerged between “no example” and “short example” ($p = 0.926$). Thus $H_{8,0}$ and $H_{9,0}$ are rejected, but $H_{7,0}$ could not be rejected.

Considering the descriptive statistics, it can be seen that the highest value (mean=5.22, sd=1.3, n=83) emerges for the long example, followed by the short example (mean=4.71, sd=1.2, n=96) and the option without an example (mean=4.51, sd=1.29, n=78).

Our examination supports the provision of extensive examples because this significantly increases the participant’s ability to correctly rate presented scenarios. There was no difference in measured ability when a short example or no example was given. Therefore, we included the long example in the final information text.

5.4 Final Proposal

As a result of the user study, we proposed a text to inform employees about their obligation to report information security incidents via the recommended route in the organisation. The text consists of five parts. It commences with a formal introduction and also contains the longest example. The text can be found in the Appendix.

6 APPLICATION IN CORPORATE CONTEXT

In this section, we commence by introducing the company in which the information text was deployed as well as the changes to the proposal made by the company's CISO. Afterwards, we explain how the information text was distributed inside the company, describe how the employee's feedback was collected and address the results of the qualitative analysis that we have carried out.

6.1 The Company

We evaluated the information text in cooperation with a medium-sized municipal energy supply and service company in Germany, that employs around 240 people. A large proportion of the employees are not involved in the administration of the company itself but are responsible for the operative business, i.e. working for grid or warehouse management. The level of employee IT usage is strongly dependent on the respective department and their assigned responsibilities, meaning a heterogeneous profile in this respect. The company has implemented an Information Security Management System (ISMS), employs a full-time Chief Information Security Manager and, as a public company, is very socially and employee-friendly and has an active error culture. This company was chosen because it is very comparable to many companies found in Germany in terms of size and structure of employees. In addition, there had already been successful cooperation with the company as part of previous projects.

6.2 Changes to the Proposed Information Text by the CISO

Before deploying the information text we proposed in Section 5.4, the company's Chief Information Security Officer modified the information text for use in the evaluating company's context. The changes, which can be found in the Appendix, were based on discussions with other stakeholders in the company and under the sole responsibility of the CISO. The structure of the text was changed so that the sentence about the proven non-reporting of incidents is located in part 2 instead of in part 1, without changing the sentence itself. Furthermore, in part 2 of the text the word 'sanctioning' was replaced by 'legal consequences against', because - as the CISO pointed out - the new phrasing seems to sound less strict than the old one. Furthermore, the CISO applied minor changes, such as highlighting keywords with bold font and adding contact information for the CISO and the Chief Information Officer (CIO).

6.3 Distribution

The final information text was sent end of September 2022 to all personal email accounts in the company with both, the examples for (slightly) negligent and grossly negligent behaviour as well as the examples for reportable information security incidents, as attachments. As the examples for reportable incidents are designed in poster format, the CISO also put them in his offices, meeting rooms and other public areas.

6.4 Employee Feedback

In this section, we first explain the methodology and the design of the questionnaire for collecting feedback on the text, followed by describing ethical considerations and limitations.

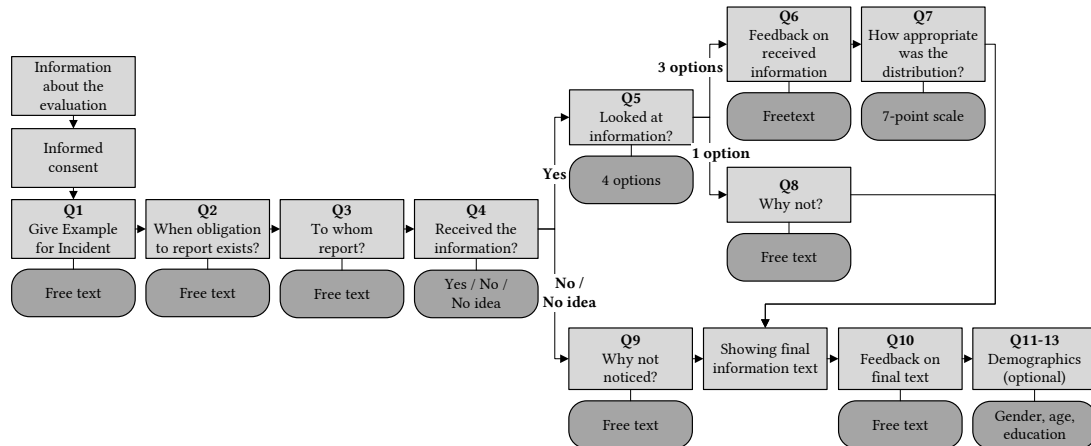


Fig. 5. Process of the collection of the employee feedback (n=24). First questions about general knowledge of incidents and reporting. Different paths depend on the given answers in Q4 and Q5. Everyone finally was shown the actual text and asked for feedback.

6.4.1 Methodology and Questionnaire. Because of remaining restrictions due to the coronavirus and to support the employee's willingness to participate in an easy way, we decided against personal interviews and collected feedback using a questionnaire. Figure 5 depicts the flow chart of the questionnaire, which was used. Depending on their previous answers through the questionnaire employees were asked a subset of seven questions which also accepted free text answers (see Q1-3, 6, 8-10 in Figure 5). To identify interesting aspects of the different answers given by the employees, we followed an inductive coding approach, whereas the objective of this approach is to find frequent or significant aspects of a text.[41] The answers to the seven questions have been open-coded independently by two researchers resulting in two separate codebooks. The researchers reviewed both codebooks, whereby consistency and further refinements of codes and their definitions were discussed. Hereafter, the coding was iterated again and disagreements were resolved in discussions between researchers. The final codebook, including description and examples for each used code, could be found in the Appendix.

6.5 Ethics

The information text was approved by the CEO of the company as well as by the members of the works council⁵, before it was emailed to all employees. Participation in the feedback questionnaire was voluntary and could be completed during work hours. Only anonymized data was collected. Hence, for the employees, there were no adverse consequences if they chose not to participate in providing feedback or criticised their employer.

⁵A works council is an internal body of a company elected by employees to represent their interests towards the management which is legally required in many German companies.

6.6 Results

In this section, we first provide demographic information about the employees, which we collected feedback from. After that, we explain the used methodology for the qualitative analysis, followed by the results of collected feedback.

6.6.1 Participants. Feedback was collected eight weeks after the information text was emailed to the employees by the CISO. Of the 75 employees who opened the questionnaire, 24 completed it. 16 were male, five were female, one was non-binary, and two did not answer the question. Five employees were younger than 30 years of age, and 13 were between 30 and 50 years of age. six employees were between 50 and 65 years of age. Almost half of the employees had an academic degree or a high-school diploma. Furthermore, seven stated that middle school was their highest level of education.

6.6.2 Feedback. A majority of the 24 respondents gave examples of incidents [Q1], which are related to emails such as phishing, spam or malicious attachments (10) or incidents which are caused by attackers (6). Four employees mentioned missing access protection (i.e. unlocked screen or no authentication) or entry protection (i.e. unlooked doors or lockers) as examples of incidents, whereat eight employees draw the connection to the loss of personal data. Asked about when an obligation to report exists [Q2], nine employees stated, information security incidents always have to be reported. Contrary to that, 15 respondents said that an obligation to report only exists if a certain threshold is exceeded, whereas two employees mentioned the involvement of attackers from outside the company. The majority of the employees answered that they would report a recognized incident [Q3] to the IT department (15), the data protection officer (7), the CISO (4), as well as their line manager (3). It can be determined that everyone has at least a sensible idea of whom to report an incident, given that in practice i.e. the DPO or the IT department would forward a report to the CISO certainly. 21 of the 24 respondents said that they had received the information text from the CISO [Q4]. However, three employees did not receive the text or did not remember receiving it. Of those who said that they received the information text, the majority stated [Q5] that they read through it very carefully (16). However, five respondents stated that they quickly skimmed the information text. There was no employee, who had not looked at the received information text [Q8]. Asked about their opinion of the text [Q6], eight of the respondents gave positive feedback. Here, for example, the length of the text was rated as appropriate and the incident examples increased the value of the information text to the employee. In addition, it was mentioned, that informing employees about their legal obligations to report incidents at work is particularly important. Five employees gave neutral feedback (i.e. 'the material is ok') and three made suggestions for improvements. So, for example, it was stated that the given information should also be presented as a web-based training course, as well as during other events and meetings inside the company. There was no negative feedback. Asked about how suitable the chosen way was to distribute information about incident reporting to all employees [Q7], only one respondent rated this as 'bad', whereby the option 'neutral' was selected by six employees. More than half of the employees who received the information text considered the distribution to be 'somewhat good' (3), 'good' (8) or 'very good' (3). Of those who said that they did not receive (3) the information text, one explained it [Q9] with an overload of emails at this time, whereas two respondents gave no answer. After the actual information text was shown again to all participants, more than half gave positive (10) feedback [Q10] or suggestions for improvement (5). For example, it was mentioned again multiple times, that the information should be distributed inside the company in various ways and should also be easily accessible during everyday work. Four respondents gave feedback, which was considered negative. For example, it was stated, that email is in general not the right way to communicate such information and training in person should be preferred.

6.7 CISO Feedback

After the employee feedback was collected, we asked the CISO about the feedback he received after the information text was sent as well as his personal feedback. Since the CISO is the central point of contact for all IT security-related issues in the company, this was to find out whether there were any questions, comments or complaints from the employees that were addressed personally to him but were not mentioned in a questionnaire and therefore would not have been recorded in this way alone. It was also intended to determine whether, in the time after the information text was sent, employees may have contacted the CISO with certain, possibly even repeated, incidents that may have already been forgotten by the time the questionnaire was sent. Related to the information text, he did not receive feedback, neither positive nor negative. As a result, different interpretations are possible. On the one hand, it can be concluded that the text did not raise any questions, since otherwise, employees would have asked the CISO. On the other hand, it is also possible that the importance of the information was misjudged and therefore no contact was made, even though there were questions. Although the text was approved by the CEO and works' council, the CISO was asked by the head of central administration to consult before distributing something similar in the future. This shows the importance of communication and coordination between different departments when it comes to company-wide IT security. Therefore the CISO will take up the topic in the next internal communication round with the department heads. According to the CISO, the poster was printed and displayed in offices or in meeting rooms by the employees several times. He also pointed out that, in his opinion, it is particularly important and necessary to regularly remind employees of incident reporting. His plan is to inform them again within the next year.

7 DISCUSSION & FUTURE WORK

Based on our experiences, the results and collected feedback, the following recommendations can be made for the application of such information texts in the corporate context: (1) It is very important to specifically address reasons for under-reporting of incidents, as outlined in Section 2. The organisation ought to clearly identify a person with demonstrable response capabilities (usually as CISO) and establish a culture of benevolence so that victims do not feel negative emotions if they fall victim to a cybercrime. These prerequisites must always be ensured for each organisation in which informative texts are to be deployed to improve reporting.

(2) To prevent problems and misunderstanding, the process should be clearly communicated, not only to the decision-makers inside the organisation (i.e. CEO), but also to all other stakeholders, such as the human resources and legal departments, the data protection officer and the works council.

(3) General knowledge about information security incidents should be enhanced because, for example, some participants incorrectly assume reportable incidents have to involve external attackers. Given that the presented information text examples cannot cover all possible eventualities, it is important to address this potential misunderstanding in the organisation's awareness-raising materials.

(4) The primary goal, for an organisation, is for incidents to be reported so that countermeasures can be taken as soon as possible. Therefore, it is not important for employees to distinguish between incidents related to data protection and those related to information security, as long as they understand that they have to report all incidents. Hence, it makes sense to combine multiple ways of reporting various kinds of incidents using a unified procedure across the organisation. This offers the advantage that employees no longer have to think about how and to whom they report a particular incident, and removes the need for them to classify the incident correctly.

In future work, it would be desirable to apply the evaluated information text and the recommendations in other organisations. For example, applying the text in a longitudinal study could provide an opportunity to gather more information about improvements in incident reporting incidence over a longer period of time. In addition, the recommendations should be refined in the context of other legal and cultural backgrounds (e.g., in the UK or the USA). Future work could also address the question of how often employees should be reminded of their reporting obligations. Furthermore, it would be worthwhile to see more research in the field of information security incidents in general. For example, it would be useful to investigate to what extent there are different understandings of incidents and their severity and whether a universal definition can be derived and agreed on.

7.1 Limitations

Even though the waiver of legal consequences was contained in every information text, this can still be interpreted by a recipient as an indirect threat of sanctions, which could impair the intended effect.

While our user study in 5 was conducted using the Clickworker platform, we recruited German-speaking participants from all areas and disciplines, who do not work for the organisation where we would be evaluating the final version. Some might have been unemployed and may not have had much work experience. Others might have been able to benefit from the experience of a long professional career. Furthermore, the participants, in contrast to employees, did not have to dread potential consequences in the employment context. This would feed into their reactions to the information texts or the correctness of their scenario rating.

Although the mail asking for feedback in 6 was sent to all of the about 240 employees, only a small number actually gave feedback. The resulting sample therefore might be biased because it could have included respondents who often participate in online surveys and therefore possibly act differently.

Given that the occurrence of information security incidents is neither predictable nor evenly distributed over time, the effect of the information text on the reporting could generally only be addressed with a longitudinal study. This also applies in particular to smaller companies, where the number of information security cases may be lower compared to very large companies.

This paper describes the application of an information text in a medium-sized energy company in Germany. Although there are various factors which could influence the applicability in other organisations. For instance, the social background or the age distribution of employees might have an impact on the effectiveness of the information texts. Furthermore, there are companies, which are multinational and therefore influenced by different cultures of communication and management.

8 CONCLUSION

There has been little research on the communication of reporting obligations within organisations. Although reporting is a prerequisite for effective security awareness in the organisational context because employees must know how to recognize as well as how and to whom to report information security incidents. Otherwise, for an organisation, it becomes much more difficult to apply effective countermeasures and to fulfil its own legal obligations. We developed a process for deriving texts to inform employees about their legal obligation to report information security incidents and to explain how they should carry out this obligation. We presented a study with 257 participants in which we evaluated different information texts for a German medium-sized company using the described process. Thereafter, the best-performing information text was then deployed in the company and disseminated to all employees. We reviewed

the feedback we collected from 24 employees afterwards and conclude with recommendations for its application in other corporate contexts.

ACKNOWLEDGMENTS

This research was supported by funding from the topic Engineering Secure Systems, subtopic 46.23.01 Methods for Engineering Secure Systems, from the Helmholtz Association (HGF) through the Competence Center for Applied Security Technology (KASTEL) and from KASTEL Security Research Labs. We would also like to thank for the cooperation with the Stadtwerke Ettlingen and in particular the chief information security officer, as without this cooperation and willingness to help, this study would not have been possible.

REFERENCES

- [1] Austrian Government. 2004. Employees' Liability Act (Dienstnehmerhaftpflichtgesetz). <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10008209>.
- [2] M. Bidgoli, B.P. Knijnenburg, J. Grossklags, and B. Wardman. 2019. Report Now. Report Effectively. Conceptualizing the Industry Practice for Cybercrime Reporting. In *2019 APWG Symposium on Electronic Crime Research (eCrime)*, Vol. 2019-November. IEEE, 1–10. <https://doi.org/10.1109/eCrime47957.2019.9037577>.
- [3] Bianka Breyer and Matthias Bluemke. 2016. *Deutsche Version der Positive and Negative Affect Schedule PANAS (GESIS Panel)*. GESIS - Leibniz-Institut für Sozialwissenschaften, Mannheim. 20 pages. <https://doi.org/10.6102/zis242>
- [4] M Button, Lisa Sugiura, Dean Blackburn, Richard Kapend, David Shepherd, and Victoria Wang. 2020. VICTIMS OF COMPUTER MISUSE EXECUTIVE SUMMARY. https://researchportal.port.ac.uk/portal/files/20818541/Victims_of_Computer_Misuse_Executive_Summary.pdf.
- [5] James Carr. 2005. *Rowe v. Guardian Auto. Products, Inc.*, Case No. 3:04CV7145 (N.D. Ohio). <https://www.casemine.com/judgement/us/59147324add7b0493438a826>.
- [6] Cassandra Cross. 2018. Expectations vs reality: Responding to online fraud across the fraud justice network. *International Journal of Law, Crime and Justice* 55 (2018), 1–12. <https://doi.org/10.1016/j.ijlcrj.2018.08.001>.
- [7] Cassandra Cross, Criminology Research Advisory Council (Australia), Kelly M Richards, and Russell G Smith. 2016. *Improving responses to online fraud victims: An examination of reporting and support*. Criminology Research Advisory Council. <https://eprints.qut.edu.au/98346/>.
- [8] DynaSis. [n. d.]. Unreported Cyber Crime. <https://dynasis.com/article-unreported-cyber-crimes>.
- [9] European Parliament. 2020. Directive on security of network and information systems (NIS Directive). [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2020\)654198](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2020)654198).
- [10] Federal Ministry of Justice. 2019. Act on the Federal Office for Information Security (BSI Act - BSIG). https://www.gesetze-im-internet.de/englisch_bsig/index.html.
- [11] Andy Field, Jeremy Miles, and Zoë Field. 2012. *Discovering statistics using R*. Sage Publications.
- [12] Vaibhav Garg, L Jean Camp, Katherine Connelly, and Lesa Lorenzen-Huber. 2012. Risk communication design: Video vs. text. In *Privacy Enhancing Technologies: 12th International Symposium, PETS 2012, Vigo, Spain, July 11-13, 2012. Proceedings 12*. Springer, 279–298.
- [13] Vaibhav Garg, Lesa Lorenzen-Huber, L Jean Camp, and Kay Connelly. 2012. Risk communication design for older adults. In *ISARC. Proceedings of the International Symposium on Automation and Robotics in Construction*, Vol. 29. IAARC Publications, 1.
- [14] George Grispos, William Bradley Glisson, David Bourrie, Tim Storer, and Stacy Miller. 2017. Security incident recognition and reporting (SIRR): an industrial perspective. In *2017 Americas Conference on Information Systems (AMCIS 2017), Boston, Massachusetts, United States*. <https://doi.org/10.48550/arXiv.1706.06818>.
- [15] Wolfgang [VerfasserIn] Hau. 2020. Becksche Online-Kommentare BGB.
- [16] Nathan House. 2022. The real reasons why cyber crime goes unreported – and why things are about to change.... <https://www.stationx.net/real-reasons-cyber-crime-goes-unreported-things-change/>.
- [17] ISACA. 2019. New Study Reveals Cybercrime May Be Widely Underreported—Even When Laws Mandate Disclosure. <https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2019/new-study-reveals-cybercrime-may-be-widely-underreported-even-when-laws-mandate-disclosure>.
- [18] U Ismail. 2020. The Nigeria Police Force and Cybercrime Policing: An Appraisal. *Dutse Journal of Criminology and Security Studies (DUJSCC)* 1 (2020), 78–88.
- [19] Nivedita James. 2023. Cyber Crime Statistics 2023: Cost, Industries, and Trends. <https://www.getastra.com/blog/security-audit/cyber-crime-statistics/>.
- [20] Manpreet Kaur and Munish Saini. 2022. Indian government initiatives on cyberbullying: A case study on cyberbullying in Indian higher education institutions. *Education and Information Technologies* (2022), 1–35. <https://doi.org/10.1007/s10639-022-11168-4>.







- [21] Erka Koivunen. 2012. "Why Wasn't I Notified?": Information Security Incident Reporting Demystified. In *Information Security Technology for Applications: 15th Nordic Conference on Secure IT Systems, NordSec 2010, Espoo, Finland, October 27-29, 2010, Revised Selected Papers 15*. Springer, 55–70. https://doi.org/10.1007/978-3-642-27937-9_5.
- [22] T. L. Kuo. 2022. *Criminal Victimization in Taiwan: an opportunity perspective*. Ph. D. Dissertation. UCL Department of Security and Crime Science, University College London.
- [23] Law Case Summaries. 2012. Hodgson v Amcor [2012] VSC 94. <https://lawcasesummaries.com/knowledge-base/hodgson-v-amco-2012-vsc-94/>.
- [24] Guillaume Lovet. 2009. Fighting Cybercrime: Technical, juridical and ethical challenges. , 63–76 pages.
- [25] Laure Lydon. 2021. *Corporate under reporting of cybercrime: Why does reporting to authorities matter?* Master's thesis. Royal Holloway University London.
- [26] Kenny MacDonald. 2019. *Action Fraud*. Technical Report V3-A0718. Scottish Police Authority.
- [27] Mike McGuire and Samantha Dowling. 2013. Cyber crime: A review of the evidence Chapter 4: Improving the cyber crime evidence base. Home Office Research Report 75 <https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence>.
- [28] Alexis Michail. 2020. *Tackling the Challenges of Information Security Incident Reporting: A Decentralized Approach*. Ph. D. Dissertation. University of East London.
- [29] Roderick Mooi and Reinhardt A Botha. 2015. Prerequisites for building a computer security incident response capability. In *2015 Information Security for South Africa (ISSA)*. IEEE, 1–8. <https://doi.org/10.1109/ISSA.2015.7335057>.
- [30] Dirk Müllmann and Melanie Volkamer. 2021. Meldepflicht von IT-Sicherheits- und Datenschutzvorfällen durch Mitarbeitende-Betrachtung möglicher arbeitsrechtlicher Konsequenzen. In *Informatik*. Gesellschaft für Informatik, Bonn. https://doi.org/10.18420/inf2020_74.
- [31] Rudi [VerfasserIn] Müller-Glöge. 2020. *Erfurter Kommentar zum Arbeitsrecht* (20., neu bearbeitete auflage ed.). C.H. Beck, München.
- [32] PSI Media. 2020. HOW CAN WE ADDRESS THE UNDER-REPORTING OF CYBER-CRIME? *Counter Terror Business* 43 (2020). <https://counterterrorbusiness.com/features/how-can-we-address-under-reporting-cyber-crime>.
- [33] Karen Renaud, Rosalind Searle, and Marc Dupuis. 2021. Shame in cyber security: effective behavior modification tool or counterproductive foil?. In *New Security Paradigms Workshop*. Online, 70–87. <https://doi.org/10.1145/3498891.3498896>.
- [34] Christian [VerfasserIn] Rolfs. 2019. BeckOK Arbeitsrecht. C.H. Beck, München.
- [35] Alex Scroxtton. 2021. Fraud and cyber crime still vastly under-reported. *Computer Weekly* <https://www.computerweekly.com/news/252495844/Fraud-and-cyber-crime-still-vastly-under-reported>.
- [36] Frederick Antione Smith. 2020. *The Influence of Anonymity Factors on IT Security Incident Reporting*. Ph. D. Dissertation. Capella University.
- [37] Martin Sparrius, Mofida Sadok, and Peter Bednar. 2021. What Can We Learn from the Analysis of Information Security Policies? The Case of UK's Schools. In *Human Aspects of Information Security and Assurance: 15th IFIP WG 11.12 International Symposium, HAISA 2021, Virtual Event, July 7–9, 2021, Proceedings 15*. Springer, 81–90. https://doi.org/10.1007/978-3-030-81111-2_7.
- [38] Statista. 2022. Largest fines issued for General Data Protection Regulation (GDPR) violations as of July 2022. <https://www.statista.com/statistics/1133337/largest-fines-issued-gdpr/>.
- [39] Finn Olav Sveen, Jose Maria Sarriegi, and Jose J Gonzalez. 2009. The role of incident reporting in reducing information security risk. In *Twenty Seventh International Conference of the System Dynamics Society*.
- [40] Franz Jürgen [HerausgeberIn] Säcker, Roland [HerausgeberIn] Rixecker, Hartmut [HerausgeberIn] Oetker, and Bettina [HerausgeberIn] Limperg (Eds.). 2020. *Münchener Kommentar zum Bürgerlichen Gesetzbuch* (8 ed.). Number 666 in Beck-online. Verlag C.H. Beck, München.
- [41] David R. Thomas. 2006. A General Inductive Approach for Analyzing Qualitative Evaluation Data. *American Journal of Evaluation* 27, 2 (2006), 237–246. <https://doi.org/10.1177/1098214005283748> <https://doi.org/10.1177/1098214005283748>.
- [42] S. van de Weijer, R. Leukfeldt, and S. Van der Zee. 2020. Reporting cybercrime victimization: determinants, motives, and previous experiences. *Policing, A International Journal* 43, 1 (2020), 17–34. <https://doi.org/10.1108/PIJPSM-07-2019-0122>.
- [43] Steve G.A. van de Weijer, Rutger Leukfeldt, and Sophie van der Zee. 2021. Cybercrime reporting behaviors among small-and medium-sized enterprises in the Netherlands. In *Cybercrime in Context*. Springer, 303–325. https://doi.org/10.1007/978-3-030-60527-8_17.
- [44] David Watson, Lee Anna Clark, and Auke Tellegen. 1988. Development and validation of brief measures of positive and negative affect: the PANAS scales. *Journal of personality and social psychology* 54, 6 (1988), 1063.
- [45] D. Wilson, A. Patterson, G. Powell, and R. Hembury. 2006. Fraud and technology crimes. Findings from the 2003/04 British crime survey. The 2004 offending, crime and justice survey and administrative sources. London: Home Office, <https://www.gov.uk/government/publications/the-offending-crime-and-justice-survey-longitudinal-analysis-2003-to-06>.
- [46] Josephine Wolff. 2018. The Real Reasons Why Cybercrimes May Be Vastly Undercounted. <https://slate.com/technology/2018/02/the-real-reasons-why-cybercrimes-are-vastly-underreported.html>.

APPENDIX

ABC

Reportable information security incidents

Protect ABC's IT infrastructure together!

-  **Malware on devices** (e.g. on PCs, laptops, smartphones) if a possible virus infection is detected.
-  **Loss of mobile devices** (e.g. laptops, smartphones) through which you can access ABC services or data.
-  **Loss of removable storage devices** (e.g. USB sticks, CDs) on which confidential or personal data is stored.
-  **Discover devices** (e.g. WLAN routers, small boxes) that are suddenly there but were not announced.
-  **Blackmail or coercion** to not behave in accordance with the rules, e.g. if someone unknown is desperate to have access to your devices or your rooms.
-  **Identity theft**, for example after accidentally giving out a password on a phishing website or over the phone.

Please report information security incidents immediately to the chief information security officer or the IT department.

The author of the images and parts of the text is XXX

Fig. 6. Translated version of the German poster with examples of reportable information security incidents. Every in 5 evaluated information text contains the examples in part 5. The company name has been changed to ABC for anonymity.

motivation	<p>Part 1 Introduction</p> <p>Option_1A Dear colleagues,</p> <p>In order to increase the security level at ABC, we need your help. We really need you to report information security incidents.</p> <p>With this e-mail I would like to explain the reporting of information security incidents in more detail.</p>	<p>Option_1B Dear colleagues,</p> <p>In order to increase the security level at ABC, we need your help. It is therefore imperative that you comply with your obligation to report information security incidents.</p> <p>With this e-mail I would like to explain the reporting of information security incidents in more detail.</p>	<p>Option_1C Dear colleagues,</p> <p>In order to increase the security level at ABC, we need your help. It is therefore imperative that you comply with your obligation to report information security incidents. Please note that proven non-reporting of an information security incident can have (severe) sanctions for you.</p> <p>With this e-mail I would like to explain the reporting of information security incidents in more detail.</p>
	<p>Part 2 Offer to employees</p> <p>Option_2 In order to relieve you of personal consequences due to possible misconduct in terms of reporting and to show you how important it is for ABC that you report information security incidents immediately, ABC has decided the following: ABC will refrain from sanctioning employees who report their own slightly negligent or negligent behaviors.</p>		
	<p>Part 3 Examples of behaviour</p> <p>Option_3A [none]</p>	<p>Option_3B For a better classification of what is (slightly) negligent, you will find practical examples here.</p> <p>An example of (slightly) negligent behavior would be if you interact with a fraudulent email where the sender email address is legitimate and the content seems plausible.</p> <p>Another example would be if you are in a private office and you leave your computer unattended and unlocked for a short period of time with the door locked, but someone still gains access to your computer, gets your password, and sends e-mails and places orders using your user account.</p> <p>If you have any questions about the obligation to report information security incidents, you are welcome to contact the information security officer at any time.</p>	<p>Option_3C For a better classification of what is (slightly) negligent, you will find practical examples here.</p> <p>An example of (slightly) negligent behavior would be if you interact with a fraudulent email where the sender email address is legitimate and the content seems plausible.</p> <p>Another example would be if you are in a private office and you leave your computer unattended and unlocked for a short period of time with the door locked, but someone still gains access to your computer, gets your password, and sends e-mails and places orders using your user account.</p> <p>Overall, you can use the content of the security training as a guide. In the case of behavior that is not in the sense of this content and leads to a information security incident, there is a risk that the violation will be classified as grossly negligent.</p> <p>In the following, for your classification, we also give examples from current case law regarding other organizations where the judges classified the behavior as grossly negligent, which made sanctions by the employer permissible.</p> <ul style="list-style-type: none"> An example of grossly negligent behavior would be interacting with an email in which the prince of a far away country offers you money or an unbelievable deal. Security training, in particular, should make it clear to everyone that such e-mails should not be interacted with. Another grossly negligent behavior would be the use of an obviously insecure password (e.g. Password! or ABC-123). The corresponding incident would be that you realize that someone has access to one or more of your ABC Services. A third example of grossly negligent behavior would be when an information security incident (e.g. malware on your computer) occurs because you left your computer unattended and unlocked - even for a short time - in a place where other people are also present or can easily gain access. Another example of grossly negligent behavior would be reusing a (secure) password, which you also use outside of ABC for private online services. The corresponding incident would be that you realize that someone has access to one or more of your ABC Services. <p>If you have any questions about the obligation to report information security incidents, you are welcome to contact the information security officer at any time.</p>
awareness	<p>Part 4 How to report</p> <p>Option_4 Report information security incidents immediately to the information security officer or the IT department. The situation will then be analyzed together with you and we will discuss what can be done to keep the probability and severity of damage to ABC as low as possible.</p>		
	<p>Part 5 What to report</p> <p>Option_5 You can find examples of reportable information security incidents here. This overview is in poster format so that you can post it in your office and key locations similar to fire guidance. If you are unsure whether what you are observing is an information security incident or whether it just seems unusual to you, contact the information security officer or the IT department as a precaution.</p> <p>I will be glad to answer any questions you might have. Kind regards</p>	<p>Poster [separate file]</p>	

Fig. 7. Translated versions of the different options of the in 5 evaluated information texts. The same colours represent identical text. The Poster of part 5 could be found in Figure 6. A schematic representation of the different options could be found in Figure 3.

Scenarios Used During the User Study

<p>grossly negligent scenario a</p>	<p>Your colleague receives an email with the corporate logo of a well-known logistics company. The e-mail text contains - in broken German and spelling mistakes - a note that an order can only be delivered if a customs declaration has been completed. To do this, your colleague should click on the link contained in the e-mail. Although he/she is not expecting a delivery, he/she follows the link anyway. Clicking on the link downloads malware onto the computer.</p>
<p>grossly negligent scenario b</p>	<p>Your colleague is traveling on the train and is working on a work laptop. Although he/she has different passwords for the different accounts, he/she cannot remember them. Since he/she does not trust a password manager, he/she wrote down the access data on a separate piece of paper, which he/she keeps in his/her wallet. When he/she cannot find the note just before getting off the train, he/she does not worry at first and expects that he/she will find it later. When your colleague arrives home, all their passwords have been changed and he/she no longer has access to them.</p>
<p>grossly negligent scenario c</p>	<p>Your colleague receives an email from an account provider that his/her profile is currently being used on a new device. In fact, he/she is only using the service on one device and hasn't logged in there recently. Nevertheless, he/she does not change the access credentials, does not report the incident and ignores the notification.</p>
<p>grossly negligent scenario d</p>	<p>In the ABC inbox, your colleague finds an e-mail in which he/she is informed that a three-digit sum of money will be paid out by a bank. In order to be able to carry out the transfer, he/she will be asked to provide personal information about himself and his colleagues and various ABC information. Delighted with the unexpected windfall, he/she replies to the message and discloses the requested information.</p>
<p>grossly negligent scenario e</p>	<p>To log in to his/her workstation computer, your colleague uses the name of his/her dog as a password, followed by year of birth. As he/she talks about the dog incessantly, both pieces of information are well known within the department and beyond. After a lunch break, he/she comes back to the office and realizes that his/her machine is unlocked and various sensitive documents have been accessed.</p>
<p>grossly negligent scenario f</p>	<p>While attending a conference, your colleague leaves the seat to get a cup of coffee. When he/she returns a few minutes later, he/she realizes that he/she forgot to close the laptop they were using. After he/she returns to the office the following day, he/she wants to access the laptop again. To his/her surprise, instead of the usual login, a message appears notifying him/her that the device has been encrypted by malware.</p>
<p>grossly negligent scenario g</p>	<p>Since it is not easy for your colleague to remember all their passwords, he/she uses the same password for different websites and online services in his/her private life. For the sake of simplicity, he/she also uses the same password to log in within the ABC systems. Now he/she is astonished to find that individual e-mails have disappeared from the business mailbox, although he/she is sure that they were not deleted by him/her. He/she also receives a series of messages asking him/her not to send the recipient any more promotional emails.</p>

slightly negligent scenario a	While your colleague is working on his computer, an operating system pop-up window appears, prompting him/her to install an update to remove security vulnerabilities. However, he/she is busy with another task which he/she doesn't want to interrupt by restarting the computer at that time. He/She therefore clicks on the "remind me later" button. About an hour later, a hacker gains access to the computer by exploiting a vulnerability that would have been removed by the update. The existence of the vulnerability had only just become known, so it had not yet been widely reported in the media.
slightly negligent scenario b	During a public presentation, your colleague wants to download information from an online account on the ABC laptop. When entering the access data, he/she takes care to shield the keyboard as much as possible, but overlooks a person who is standing to the side behind him/her who can record the login data with the smartphone. A little later he / she notices that someone has gained access to his / her account.
attention check	While your colleague is working on their computer, an operating system pop-up window appears, prompting him/her to install an update to remove security vulnerabilities. However, he/she is busy with another task which he/she doesn't want to interrupt by restarting the computer. He/She therefore clicks on the "remind me later" button. For the question, please indicate that this is not an information security incident. About an hour later, a hacker gains access to the computer by exploiting a vulnerability that would have been fixed with the update. The existence of the vulnerability had only just become known, so it had not yet been widely reported in the media.

User Study (1st evaluation)

PANAS.

Items of the Positive and Negative Affect Schedule Score in the used German and the corresponding English version.

#	German	English	Dimension
1	aktiv	active	positive affect
2	bekümmert	distressed	negative affect
3	interessiert	interested	positive affect
4	freudig erregt	excited	positive affect
5	verärgert	upset	negative affect
6	stark	strong	positive affect
7	schuldig	guilty	negative affect
8	erschrocken	scared	negative affect
9	feindselig	hostile	negative affect
10	angeregt	inspired	positive affect
11	stolz	proud	positive affect
12	gereizt	irritable	negative affect
13	begeistert	enthusiastic	positive affect
14	beschämt	ashamed	negative affect
15	wach	alert	positive affect
16	nervös	nervous	negative affect
17	entschlossen	determined	positive affect
18	aufmerksam	attentive	positive affect
19	durcheinander	jittery	negative affect
20	ängstlich	afraid	negative affect

Original Question in German

Nun möchten wir gerne von Ihnen wissen, wie Sie sich fühlen. Hierbei beziehen wir uns speziell auf den Text, den sie gerade gelesen haben. Die folgenden Wörter beschreiben unterschiedliche Gefühle und Empfindungen. Lesen Sie jedes Wort und tragen Sie dann in die Skala neben jedem Wort die Intensität ein. Sie haben die Möglichkeit, zwischen fünf Abstufungen zu wählen.

Translation

Now we would like to know how you feel. Here we refer specifically to the text that you have just read. The following words describe different kinds of feelings and perception. Read every word and mark the intensity on the scale. You have the choice between five gradations. Please indicate how you generally feel.

Answer scale

For each of the 20 items, the answer scale contains five single-choice categories, which are marked as follows (German/English): 1 = "Not at all", 2 = "a little", 3 = "moderately", 4 = "quite a bit", 5 = "extremely"/"extremely".

Rating of scenarios.

The following question is about the rating of scenarios in the used German and the corresponding English version.

Original Question in German

Wie stufen Sie das Verhalten in dem beschriebenen Szenario ein?

Translation

How do you rate the behavior in the scenario described?

Answer scale

The answer scale contains four single-choice categories, which are marked as follows: 1 = "slightly negligent", 2 = "grossly negligent", 3 = "intentional", 4 = "non of the three options applies".

Demographics.

The following questions are questions about the demographics of the participant in the used German and the corresponding English version.

Original Question in German

Welches Geschlecht haben Sie?

Translation

What is your gender?

Answer scale

The answer scale contains four single-choice categories, which are marked as follows: 1 = "male", 2 = "female", 3 = "non-binary", 4 = "Prefer not to say".

Original Question in German

Wie alt sind Sie?

Translation

How old are you?

Answer scale

The answer scale contains 12 single-choice categories, which are marked as follows: 1 = "younger than 18", 2 = "18 to 19", 3 = "20 to 25", 4 = "25 to 39", 5 = "30 to 34", 6 = "35 to 39", 7 = "40 to 44", 8 = "45 to 49", 9 = "50 to 54", 10 = "55 to 59", 11 = "60 to 64", 12 = "65 or older".

Original Question in German

Welchen beruflichen Bildungsabschluss haben Sie?

Translation

What professional education do you have?

Answer scale

The answer scale contains nine single-choice categories, which are marked as follows:

- 1 = "Still a pupil"
- 2 = "School finished without graduation"
- 3 = "elementary or lower secondary school leaving certificate, or equivalent qualification"
- 4, 5 = "Intermediate of secondary school leaving certificate or equivalent qualification" the qualification in 5 is an equivalent qualification but is received in the former DDR

6 = “vocational baccalaureate, entrance qualification for a university of applied science”

7 = “final secondary-school examinations, university entrance qualification”

8 = “University of Applied Science school diploma / university degree”

9 = “other degree”, followed by a textbox

Pre-knowledge.

Original Question in German

Haben Sie in der Vergangenheit in einem Unternehmen oder einer Organisation gearbeitet, in dem oder der Sie über das Thema "IT-Sicherheitsvorfälle" bzw. allgemeine Meldepflichten informiert worden sind?

Translation

Have you worked in a company or organization in the past where you were informed about the topic of "information security incidents" or general reporting obligations?

Answer scale

The answer scale contains two single-choice categories, which are marked as follows: 1 = “Yes. In fact, I received the following types of information there:” followed by a text field, 2 = “No”.

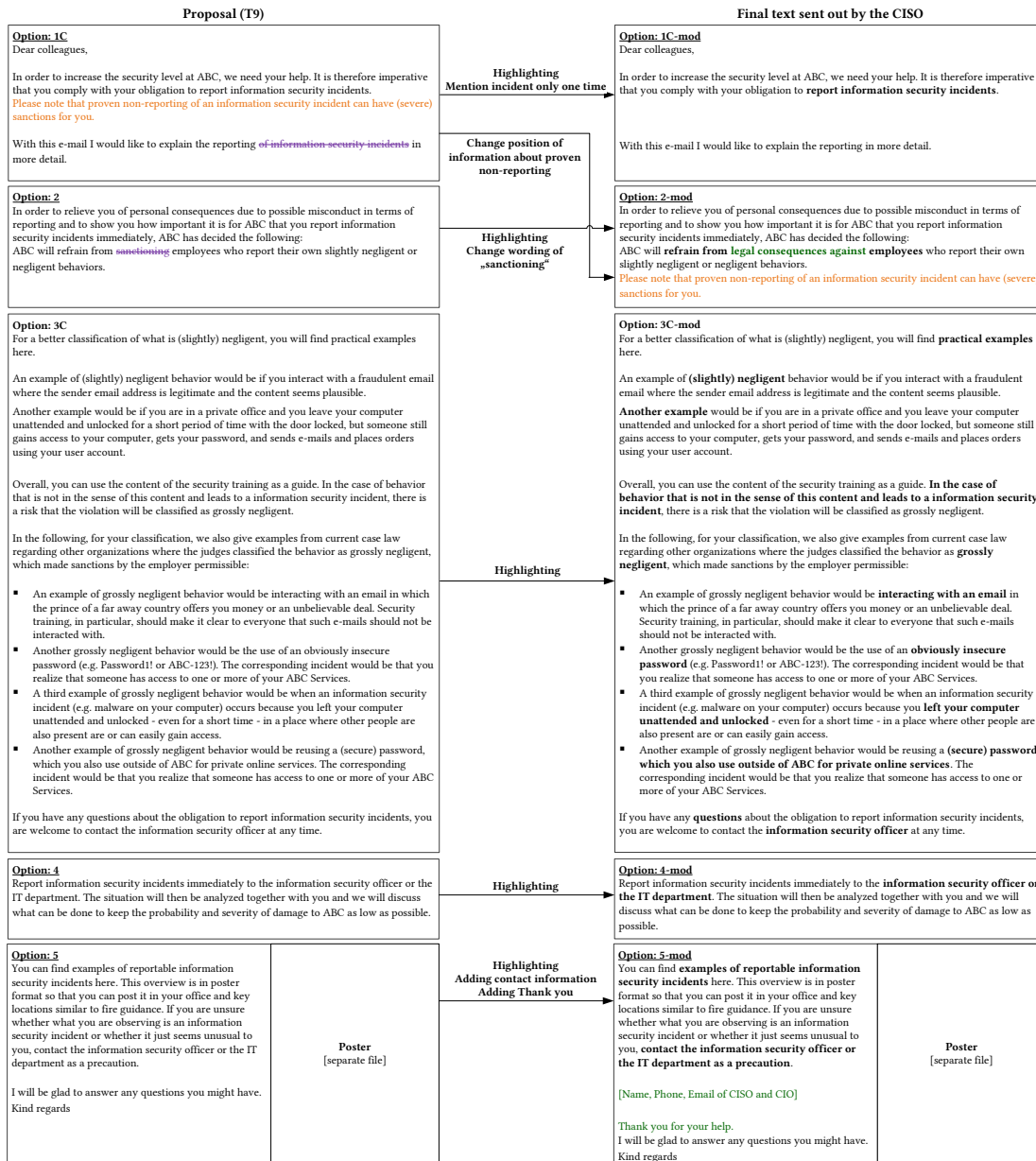


Fig. 8. Changes between the proposal after the user study (5.4) and the final text sent to the employees of the company by the CISO. Yellow means moved positions in the text, green means newly added, and purple means removed. The differences are described in the centre. **For the final version of this paper, this figure will be published online as an interactive graphic due to the limited readability here.**

Collection of Feedback (2nd evaluation)

Q1: Give Example for Incident.

Original Question in German

Bitte nennen Sie ein Beispiel für einen Informationssicherheitsvorfall im Umfeld der ABC.

Translation

Please name one example for an information security incident in the environment of ABC.

Answer scale

The answer scale contains a text field.

Q2: When Obligation to Report Exists?

Original Question in German

In welchen Fällen besteht die Pflicht zur Meldung eines Informationssicherheitsvorfalls?

Translation

In which cases is there an obligation to report an information security incident?

Answer scale

The answer scale contains a text field.

Q3: To Whom Report?

Original Question in German

An welche Stelle bei den ABC würden Sie einen meldepflichtigen Informationssicherheitsvorfall melden?

Translation

To which office at ABC would you report a reportable information security incident?

Answer scale

The answer scale contains a text field.

Q4: Received the Information?

Original Question in German

Haben Sie in den vergangenen Wochen Informationen zur Meldepflicht von Informationssicherheitsvorfällen bei den ABC erhalten?

Translation

Have you received any information about ABC's information security incident reporting obligations in the past few weeks?

Answer scale

The answer scale contains three single-choice categories, which are marked as follows: 1 = "Yes", 2 = "No", 3 = "No idea".

Q5: Looked at Information?

Original Question in German

Haben Sie sich die Informationen bereits angeschaut?

Translation

Have you already looked at the information?

Answer scale

The answer scale contains four single-choice categories, which are marked as follows: 1 = “Yes, I looked at it very closely”, 2 = “Yes, I have looked at it closely”, 3 = “Yes, but I only skimmed it”, 4 = “No”.

Q6: Feedback on Received Information.

Original Question in German

Sie haben angegeben, dass Sie sich die Informationen zur Meldepflicht von Informationssicherheitsvorfällen bereits angeschaut haben. Wie ist Ihr Feedback zu den Informationen?

Translation

You indicated that you have already viewed the information about the reporting obligation of information security incidents. What is your feedback on the information?

Answer scale

The answer scale contains a text field.

Q7: How Appropriate Was the Distribution?

Original Question in German

Wie geeignet war die Art der Verteilung der Informationen, um alle Beschäftigten der ABC über die Pflicht zur Meldung von Informationssicherheitsvorfällen zu informieren?

Translation

How appropriate was the method of distributing information to inform all ABC employees of the obligation to report information security incidents?

Answer scale

The answer scale contains seven single-choice categories, which are marked as follows: 1 = “very bad”, 2 = “bad”, 3 = “a little bad”, 4 = “neutral”, 5 = “a little good”, 6 = “good”, 7 = “very good”.

Q8: Why Not?

Original Question in German

Sie haben angegeben, dass Sie sich die Informationen zur Meldepflicht von Informationssicherheitsvorfällen noch nicht angeschaut haben.

Wieso haben Sie sich die Informationen noch nicht angeschaut?

Translation

You have indicated that you have not yet looked at the information on the obligation to report of information security incidents.

Why haven't you looked at the information yet?

Answer scale

The answer scale contains a text field.

Q9: Why Not Noticed?

Original Question in German

Am 26.09.2022 wurde eine E-Mail mit dem Betreff "Meldepflicht von Informationssicherheitsvorfällen" an alle E-Mail Konten der ABC verschickt. In dieser E-Mail wurde die Pflicht zur Meldung von Informationssicherheitsvorfällen erläutert. Haben Sie eine Idee, woran es liegen könnte, dass Sie die E-Mail nicht wahrgenommen haben bzw. Sie sich nicht erinnern konnten, dass Ihnen die E-Mail zugeschickt wurde?

Translation

On 09/26/2022, an email with the subject "Obligation to report information security incidents" was sent to all ABC email accounts. This email explained the obligation to report information security incidents. Do you have any idea what might have caused you not to notice the email or you could not remember that the email was sent to you?

Answer scale

The answer scale contains a text field.

Q10: Feedback on Final Information Text.

Original Question in German

Welches Feedback haben Sie zur E-Mail vom 26.09.2022 inkl. der Anhänge?

Translation

What feedback do you have on the email dated 09/26/2022 including the attachments?

Answer scale

The answer scale contains a text field.

Q11: Demographics (optional).

Original Question in German

Welches Geschlecht haben Sie?

Translation

What is your gender?

Answer scale

The answer scale contains four single-choice categories, which are marked as follows: 1 = "male", 2 = "female", 3 = "non-binary", 4 = "Prefer not to say".

Q12: Demographics (optional).

Original Question in German

Wie alt sind Sie?

Translation

How old are you?

Answer scale

The answer scale contains 12 single-choice categories, which are marked as follows: 1 = "younger than 18", 2 = "18 to 19", 3 = "20 to 25", 4 = "25 to 39", 5 = "30 to 34", 6 = "35 to 39", 7 = "40 to 44", 8 = "45 to 49", 9 = "50 to 54", 10 = "55 to 59", 11 = "60 to 64", 12 = "65 or older".

Q13: Demographics (optional).

Original Question in German

Welchen beruflichen Bildungsabschluss haben Sie?

Translation

What professional education do you have?

Answer scale

The answer scale contains nine single-choice categories, which are marked as follows:

1 = "Still a pupil"

- 2 = "School finished without graduation"
- 3 = "elementary or lower secondary school leaving certificate, or equivalent qualification"
- 4, 5 = "Intermediate of secondary school leaving certificate or equivalent qualification" the qualification in 5 is an equivalent qualification but is received in the former DDR
- 6 = "vocational baccalaureate, entrance qualification for a university of applied science"
- 7 = "final secondary-school examinations, university entrance qualification"
- 8 = "University of Applied Science school diploma / university degree"
- 9 = "other degree", followed by a textbox

Codes Feedback Employees

Q1: Give Example for incident.

#	Code DE	Code EN	Description	Example
1	Schadsoftware	Malware	Malicious software, malware, etc. is mentioned.	"Malware on device"
2	Verlorenes Endgerät	Lost terminal device	Loss of a terminal device like a laptop or a cell phone is mentioned.	"Laptop stolen"
3	Verlorene Datenträger	Lost data medium	Loss of a data medium like an USB stick is mentioned.	"Loss of an USB stick"
4	Personenbezogene Daten/Bezug zu Datenschutz	Personal data/connection to data protection	A connection to personal data or personally identifiable information is established. (Is actually a data protection incident).	"Email to wrong receiver"
5	E-Mail-Kontext	Email context	A connection to email is established.	"Mail traffic" "Malicious attachment of an email"
6	Unbekannt/keine Angabe	Unknown/no answer specified	No answer can be given.	"I am not aware of any"
7	Spam	Spam	Spam is mentioned specifically.	"Spam mail"
8	Phishing/ Identitätsdiebstahl	Phishing/identity theft	Phishing is mentioned specifically. The person mentions identity theft through e.g. a phishing mail as an information security incident.	"Link in a phishing mail clicked"
9	Link klicken	Link clicked	It is specified that the incident is caused by the click on a link.	"Dubious link in a mail clicked"
10	Telefon	Telephone	It is specified that the incident occurs in connection with a phone call.	"Share data on phone"
11	Daten weitergeben	Share data	It is generally stated that the incident is caused by passing on data to third parties.	"Email with wrong address to wrong receiver"
12	Unberechtigte	Unauthorized	It is stated that unauthorized third parties receive information.	"Personal data reach the public"
13	Anhang	Attachment	It is specifically mentioned an attachment.	"Malicious attachment of an email"
14	Hackerangriff	Hacker attack	It is generally mentioned a hacker attack.	"Hacking"
15	Zulieferer	Supplier	It is stated that an attack on a supplier can also lead to an incident at the company.	"Attack on a company who is working for ABC in the field of network management"

16	Nicht melden	No report	It is stated that the non-reporting of a situation can cause an incident.	"If you do not report it"
17	Kein Zugriffsschutz	No access protection	The missing access protection leads to an incident.	Openly accessible documents, no password
18	Kein Zutrittsschutz	No entry protection	The missing entry protection leads to an incident.	Door not locked

Q2: When Obligation to Report Exists?

#	Code DE	Code EN	Description	Example
1	ISV immer melden	Always report	Incidents must always be reported.	"information security incidents must always be reported"
2	Selektion	Selection	Conditions or limitations are specified from which a reporting obligation applies.	"If nobody has reported the incident yet"
3	Nennt Beispiele	Names examples	Specific examples for incidents are named.	"Clicked on an unauthorized link"
4	Angreifer	Attacker	The involvement of an attacker is being addressed.	"In case of a hacker attack"
5	Datenschutzbeauftragter	Data protection officer	The data protection officer is specifically named. (Word must occur)	"In case of doubt, always in consultation with the data security officer"

Q3: To Whom Report?

#	Code DE	Code EN	Description	Example
1	IT-Abteilung	IT department	The IT department is referred to in a broader sense.	"IT"
2	Informationssicherheitsbeauftragter	Chief information security officer	The Chief Information Security Officer is mentioned. (The term Chief Information Security Officer or Information Security Officer must be named)	"Chief information security officer" "Information security officer"
3	Datenschutzbeauftragter	Data security officer	The data security officer is named.	"Data security officer"
4	Konkrete Personen	Concrete person	A concrete person is mentioned.	e.g., <Name>
5	Vorgesetzte	Supervisor	Report to supervisor.	"To the department head"

6	Andere	Another	Report to another department of the company.	e.g., executive department technology
---	--------	---------	--	---------------------------------------

Q6: Feedback on Received Information.

#	Code DE	Code EN	Description	Example
1	Positiv	Positive	The information is generally evaluated positively.	“clear, understandably”
2	keine Angabe	No answer	No feedback is specified or there are no memories about the text.	“nvm”, “xxx”, “have just scanned the information”
3	Verbesserungsvorschlag	Suggestions for improvement	Suggestions for improvement are made.	“Possibly usefully to inform more broadly through presentation, notices, etc.”
4	Neutral	Neutral	The information is evaluated neutrally.	“were ok”

Q8: Why Not? No answers.

Q9: Why Not Noticed?

#	Code DE	Code EN	Description	Example
1	Verklickt im Fragebogen	Clicked wrong in questionnaire	The person clicked wrong in questionnaire.	“Have noticed it, just clicked wrong”
2	Keine Angabe	No answer	No reason is given.	“-”
3	Mailüberfluss	Email overload	The person states receiving a lot of mails every day so they cannot remember each one.	“You receive every day different mails from different sources and unfortunately not few. Therefore, you cannot remember every email you received. The fact that one has received it is understandable to a certain extent.”

Q10: Feedback on Final Information Text.

#	Code DE	Code EN	Description	Example
1	Positiv	Positive	The email is evaluated positively.	“good info”
2	Verbesserungsvorschlag	Suggestions for improvement	Suggestions for improvements of the email are given	“Should be deposited in several places to be able to find them quickly”

3	keine Angabe	No answer	No feedback is specified or there are no memories about the text.	“no answer” “xxx”
4	Anhang	Attachment	A statement regarding the attachment of the email is made.	“illustrative examples in the attachment”
5	Negativ	Negative	The email is evaluated negatively.	“Many information all at once”