"To Do This Properly, You Need More Resources": The Hidden Costs of Introducing Simulated Phishing Campaigns

Lina Brunken, Annalina Buckmann, Jonas Hielscher,
and M. Angela Sasse, *Ruhr University Bochum*

https://www.usenix.org/conference/usenixsecurity23/presentation/brunken

This paper is included in the Proceedings of the
32nd USENIX Security Symposium.

August 9–11, 2023 • Anaheim, CA, USA

978-1-939133-37-3

Open access to the Proceedings of the
32nd USENIX Security Symposium
is sponsored by USENIX.

"*To Do This Properly, You Need More Resources*": The Hidden Costs of Introducing Simulated Phishing Campaigns

Lina Brunken, Annalina Buckmann, Jonas Hielscher, M. Angela Sasse
Human-Centred Security – Ruhr University Bochum

Abstract

Many organizations use phishing simulation campaigns to raise and measure their employees' security awareness. They can create their own campaigns, or buy phishing-as-a-service from commercial providers; however, the evaluations of the effectiveness in reducing the vulnerability to such attacks have produced mixed results. Recently, researchers have pointed out "hidden costs" – such as reduced productivity and employee trust. What has not been investigated is the cost involved in preparing an organization for a simulated phishing campaign.

We present the first case study of an organization going through the process of selecting and purchasing a phishing simulation. We document and analyze the effort of different stakeholders involved, and present reflection from semi-structured interviews with 6 key actors at the end of the procurement process. Our data analysis shows that procuring such simulations can require significant effort from different stakeholders – in our case, at least 50,000€ in person hours – and many hidden intangible costs. Evaluating if a product or service meets training requirements, is acceptable to employees, and preparing the technical infrastructure and operational processes for running such a product all require significant time and effort. The prevailing perception that phishing simulation campaigns are a quick and low-cost solution to providing security training to employees thus needs to be challenged.

1 Introduction

Currently, organizations around the world spend billions of dollars every year on IT security awareness campaigns (**SAC**) and phishing simulation campaigns (**PSC**) [25]. The aim – stated by the standards and regulations that recommend or require these [23, 45] – is to raise employee awareness of security threats, and to generate metrics for secure behavior [30, 34]. PSC have had great success in the market, and a number of studies found them effective in lowering clickrates, at least in the short term [42, 54, 56, 62]. But more recently, a long-term study has cast serious doubt on the effectiveness of the approach [43]; other researchers have suggested potential negative side effects for the security and productivity of organizations [60].

This paper adds another piece to the puzzle of understanding costs and benefits of PSCs: it presents a case study that documents and analyzes the organizational cost and effort required in procuring a PSC and SAC product, and preparing for deployment. We studied a European organization with over 30,000 employees selecting and procuring a PSC and associated SAC product. Our aim was to identify (I) the types and number of tasks involved in selecting and deploying the product, (II) the type and number of organizational stakeholders involved in those tasks, and (III) the factors that drove the decision-making process at different stages. We analyzed a log of activities associated with the process over a 5 month period leading up to the selection and purchase of a particular product, plus interviews with 6 key actors, which enabled us to identify a wide range of tangible and intangible costs that the process created for individuals and the organization. The results of our case study will enable other organizations to understand what the cost of purchasing a PSC beyond the "sticker price" is likely to be, and avoid some of the *effort sinks* we identified.

We formulated the following research questions:

Q1: How does the process of selecting and procuring a security awareness training with a phishing simulation campaign look like in detail?

Q2: What organizational stakeholders are involved in the procurement and implementation phase of phishing simulations?

Q3: What hidden costs occur during the procurement and implementation phase of phishing simulations?

We found that (I) the process of identifying and procuring a suitable service provider (**SP**) for a PSC took well over a year, and required participation from a wide range of – often

senior – organizational stakeholders, (II) the expected benefits of PSC are vague – customers mainly hope to derive KPIs, (III) to actually use all of the features provided by the SP, it is necessary to have a well maintained master data system, (IV) SP are not fulfilling the requirements of custom learning content, all required languages fully translated and dubbed, offering an automated categorization of all the reported e-mails, and providing an API interface, and (V) SP are trying to pass on costs, efforts, and responsibilities to their customers.

2 Background & Related Work

There has been a small but important strand of research investigating security in the context of organizations [1, 5, 6, 10, 49, 59], e. g., on the usability of security mechanisms [17, 22, 61], the effects of security policies [18, 32, 33], the perception of security by employees [4, 27], and the effects of security on productivity [7–9, 28, 37, 38]. Here, we specifically review studies that investigated the friction, workload, and organizational cost associated with security in 2.1, before focusing on research on SAC and PSC in 2.2.

2.1 Organizational IT Security

Starting with [9], there has been a number of studies on the friction between security and productivity, and the direct and hidden costs for organizations [7, 8, 28, 37, 38]. Building on micro-economic and human factors literature, they argue that non-compliance with security policies largely arises because of goal conflicts and/or that the effort required for compliance is perceived as excessive. Thus, the *compliance budget* [9] of employees needs to be determined and managed carefully: Parkin et al. [47] outlined a dashboard-based approach which organizations could employ. Building on this, Herley [28] argued for a more critical assessment of whether the effort required by a security behavior is actually worth it. He singled out advice given to users on phishing for particular criticism, arguing "if users spent even a minute a day reading URLs to avoid phishing, the cost (in terms of user time) would be two orders of magnitude greater than all phishing losses". Whilst the threat landscape has arguably changed since then, the argument that performing such checks on every email is cumbersome for employees, and not entirely effective in protecting organizations, remains valid. Herley also argues that the high-cost/low benefit that employees experience with many security mechanisms and advice leads to them being ignored – resulting in unknown hidden costs for the companies [28]. Kirlappos et al. [37] analyzed the reasons for non-compliance with organizational security policies using a mixed-methods approach, conducting 126 semi-structured interviews, followed by a scenario-based survey with n=1256 in two organizations. They found that the primary cause for non-compliance with security policies was a "perceived conflict of security with productive activities", and conclude that "employees are the principal agents who must decide how to implement security in specific contexts", for which they need the necessary skills to become "security-aware principal agents". In a follow-up study, Kirlappos et al. [38] found that the friction between security and primary work tasks "led to the development of activities that can be characterized as *shadow security*" – employees manage the risks they understand with available, low-friction security solutions. Such solutions – for instance protecting a sensitive document with a password before emailing it – may not meet organizational security requirements. Nevertheless, these practices can present starting points for developing effective and acceptable *and* productive security practices, in collaboration with employees. Including employees' needs in a participatory manner is key to reduce friction, thereby reducing costs of security, and making security endeavors sustainable. A recent development in research on organizational IT security is its conceptualization as care work and emotional labor, another factor of hidden cost [31, 44]. Kocksch et al. [40] proposed to specifically analyze care practices within IT security, to account for the "continuous, often invisible work" that it relies upon, and, only recently, Kaur et al. [36] investigated emotional labor among system administrators, finding that it adds an extra layer of effort on them, that, left unaccounted for, can lead to dissatisfaction and employee turnover. Similar hidden costs have been found among security operations staff [59], and, recently, among CISOs, who feel worn down by battling with employees and business leaders alike [30]. We build on this work, by using the theoretical lenses of friction [9, 28, 37, 38], emotional labor [31, 36], and care [40, 44] for analysis of our data and presentation of our results.

2.2 Security Awareness and Phishing Simulation Campaigns

SAC are the primary intervention most organizations use to influence employees' security behavior [15, 16], and most now use them in conjunction with PSCs, not least because ISO27004, for example, explicitly recommends them as a way of verifying the success of security training [34]. PSCs are also required for many other security certifications – e. g., national ones – and are heavily advertised at security conferences and in professional magazines, often referred to as "best practice". SPs that offer PSCs argue that they work by creating "teachable moments" [24]: having just "fallen" for a phishing email is a prompt to engage with the teaching material presented. An early large-scale study by Caputo et al. [14] however, found that most employees quickly close the window, rather than engage with it. Volkamer et al. [60] pointed out that the BMAP model by B. J. Fogg [11], on which the "teachable moment" concept is based, clearly states that such prompts only work if a person is sufficiently motivated and able to perform the target behavior – so inducing an experience of failure is counterproductive. Recent large-scale

empirical studies produced mixed or negative results. Gordon et al. [26] tested a PSC and training with 5.416 employees and report that while some clickrates were slightly reduced, the associated training had no positive effect. A long-term study with 14,000 employees [43] found that embedded training in PSC did not reduce the click rates of the employees who had been subjected to it.

The effectiveness of the widely used SAC packages has also been questioned: Pattinson et al. [48] found that formal security training does not necessarily translate to higher security awareness, but can lead to overconfidence and complacency. Reeves et al. [52] concluded, not only that such security awareness and training attempts are largely ineffective, but that they may contribute to "cybersecurity fatigue": overexposure to cybersecurity-related advice causes weariness. They found that SACs were generally rated poorly by employees. Interviews with 20 employees revealed that they disengage because (I) the program contradicts their perception of threats, (II) is poorly designed, and (III) the content is seen as irrelevant to their work context. Various other studies found that trainings and warning indicators do not prevent phishing to an acceptable degree [2, 19, 53, 57]. Jampen et al. [35] reviewed a wide range of anti-phishing training evaluation studies, and concluded that "most studies have attempted to answer the question of whether training makes trainees less susceptible to phishing attempts, little information is available concerning how such training changes their behavior regarding benign e-mails."

Sasse et al. [29, 55] introduced the *security learning curve*, which proposes 9 steps that organizations need to support to enable lasting behavior change. The knowledge imparted by SACs covers only a small part of this. Organizations first need to ensure *security hygiene* [39] – ensure that employees can perform secure behaviors in the context of their other duties. Also essential to successful adoption is *security self-efficacy* [12, 13, 21], which can be, e. g., heavily damaged through phishing simulations that set traps for employees and induce experiences of failure.[1] Based on available literature and their own observations of deployments in a number of organizations, Volkamer et al. [60] compiled the security, legal, and trust issues associated with PSCs. They conclude that running a PSC that meets security and legal requirements is likely to be costly, and that the negative impact on trust and self-efficacy of employees is such that, overall, "the cost and negative side-effects clearly outweigh the low external validity of a such a campaign, and the limited reduction in vulnerability that results". We build on Volkamer et al. [60] by providing detailed empirical evidence on the preparatory work that an organization should expect when acquiring and setting up a PSC – in addition to paying for the tolls or service.

[1] For example: How a Phishing Awareness Test Went Very Wrong: https://www.bankinfosecurity.com/blogs/how-phishing-readiness-test-goes-very-wrong-p-2948, accessed June 2, 2023

3 Research Method

In 2022, we conducted a case study during the procurement phase of a PSC in a large European corporation, over a period of 5 months.[2] We were able to document the process in detail, including the workload associated in selecting and procuring a new PSC for the various stakeholders involved. After the SP for the PSC was selected, we collected the experiences and reflections of 6 key actors involved in the process in 5 semi-structured interviews (4 individual, 1 with 2 interviewees present). Our research method is visualized in detail in Figure 1.

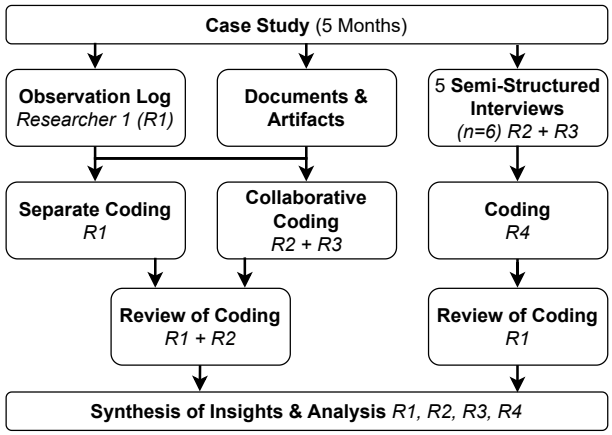

Figure 1: Our Research Method.

3.1 Partner Organization & Setting

Our partner organization is an international company headquartered in Europe, with more than 30,000 employees globally: ***TruckCorp***. The company is typical for large global companies that have grown by acquisition, and rely heavily on IT for their core business. It has a number of requirements for SAC and PSC, e. g., caring for employees working in different types of jobs (from blue collar workers to IT experts), in different countries, with different languages and organizational cultures.

The company had attempted a PSC once before, but had to abandon it during the first testing (Proof of Concept/ **PoC**) because an extreme number of tickets were reported by employees and queries overwhelmed the service desk. This initial experience led to a better understanding of the needed PSC requirements, as well as a determination to find a solution that would be practical and resilient in the long term. TruckCorp also had an existing SAC that delivered a mandatory IT security training. In a certified part of TruckCorp (ISO27001, etc.), new employees were additionally trained.

[2] The study lasted a little more than 5 months, which is reflected in Figure 2.

Our study accompanied the process of finding and deciding on a new PSC SP. After a closer consideration of possible SP, this request evolved to additionally wanting a new SAC, because obtaining both services from the same SP would lead to better integration and lower cost. 2 internationally well established SPs were identified for a PoC, which we identify as SP1 and SP2. We documented the procurement process for 5 months during a case study.

3.2 Case Study

Case studies are less common than laboratory and survey studies in usability and usable security research, since they can require significant investment in planning and negotiation to obtain access. In other disciplines, case studies are appreciated for the in-depth contextual knowledge they provide. In security research case studies can provide real-life, contextual insights into how different stakeholders manage "everyday, practical problems" [20]. Further, as case studies are longitudinal, they allow to study how the phenomenon under scrutiny develops and unfolds over time [51], in a specific context, as well as the application of different methods for qualitative and quantitative data gathering. There have been a number studies investigating the effectiveness of PSCs in organizations, with mixed results. Whilst early investigations [42] reported a case study where PSC were effective in reducing clickrates, other studies [14, 43] found no positive effect.

Our case study is the first to document and analyze the selecting and procurement of a PSC in an organization. One researcher (**R1**) was embedded in our partner organization, closely observing and documenting the procurement process. In the following, we describe the process of structured participant observation, taking field notes and writing observation logs (**OL**), followed by the complementary interviews in the final stage of the process of procurement.

3.2.1 Documentation Process & Observation Log

R1 was embedded in TruckCorp as part of the information security division (**IS division**) and able to closely observe the different steps involved in the procurement process over a period of 5 months. R1 participated in everyday work settings, as well as online and offline meetings with different internal and external stakeholders.

The structured observation focused on documenting how different stakeholders managed the process, the workload, as well as the arising friction and the associated hidden costs. Through conversations with colleagues, R1 also got deeper insights into the events, reasons, and motivations for implementing the SAC and PSC that occurred before the documentation started. During this process, R1 was closely guided by R2 and R3 in bi-weekly meetings, in which events were reflected upon and further proceedings were discussed.

The procurement process was documented by taking daily notes, recording everyday as well as single important events, recording the workload, and summarizing important conversations regarding the research questions. These notes were sometimes taken "on the fly" during the work day, or afterwards, to be as accurate as possible and to avoid forgetting important observations and details. The notes were then tidied up, consolidated, and formulated into the OL for analysis. To better understand the procurement process, R1 further collected various artifacts for later analysis. Among these were: the company's requirement catalog, a stakeholder matrix, a survey gathering feedback, and checklists comparing the pros and cons of different providers.

3.2.2 Concluding Interviews

After the decision for a provider was made, R2 and R3 conducted 5 semi-structured interviews on-site with 6 interviewees (P1-6). The interviews were conducted by R2 and R3 to capture P1-6's reflections on how the process – from procurement-start to decision-making – had gone from an outsider perspective, i.e., someone who was not involved in the process. The 6 interviewees were approached because they had been key actors who were endowed with (P1-4), or very strongly involved in (P5-6) the procurement, as well as the final decision-making process. P1-4 were part of the internal IT department while P5-6 belonged to another business unit that had high stakes towards the PSC due to certifications, which is why they were specifically involved. The interviews lasted for about an hour each, centering questions on their experiences with the procurement process, how it affected their work, and their expectations towards the SAC and PSC. P5 and P6 were interviewed at the same time, so it became a lively conversation between 2 stakeholders and 2 researchers. The underlying interview guide was developed by R1, R2, and R3, based on their discussions, and the overarching research questions. The full interview guide can be found in our replication package.

3.3 Data Analysis

The data set captured was extensive and contained very different kinds of data: 73 entries in the OL, 20 documents, 26 artifacts, a survey, and 5 interview transcripts with 620 paragraphs. To make sense of the data set, we decided on qualitative content analysis, primarily engaging in structured deductive coding [41] that fitted our structured documentation process. Deductive codes were derived from the research questions that guided the structured observation and documenting processes to identify, evaluate, and analyze involved stakeholders, workload, friction, and hidden costs. A few inductive codes were created, to account for emerging themes that were important for analysis, yet not included before.

The applied code book consisted of codes accounting for the *hidden costs*, with subcodes for workload, time, emotional

labor/care work, and hassle factor. Another primary code was *stakeholders*, with subcodes for involved, and affected stakeholders. A further primary code accounts for *security*, with subcodes for data protection, technical aspects, security behavior, and security awareness. A primary code was used for *expectation*, with subcodes for requirements, behavior change, and evaluation. Finally, a primary code was used to analyze the *overall process*, including a subcode for the PoCs. All primary codes had subcodes for "friction/conflict", to better understand the arising friction in the different areas.

The same codebook was applied to analyze the OL and the interview transcripts. The OL was first coded by R1, then by R2 and R3 in collaborative coding sessions, including writing memos with first analytical formulations. To bridge insider- and outsider perspectives, arising questions were discussed with R1 in-between the sessions, and answers added in memos for further information. The interview transcripts were coded separately by R4, using the same deductive codes as for the OL, and accounting for new, emerging themes with inductive codes. In the end, we synthesized our insights and analysis in several focused discussions, which benefited highly from the interdisciplinary backgrounds of the researchers (computer science, information security, psychology, human-computer interaction, and social sciences).

3.4 Ethics & Data Privacy

We provide a full ethics protocol in Appendix A.

3.5 Limitations

We present a case study in a single organization, TruckCorp. From parallel research with security practitioners, we know that a significant number of internationally distributed companies of a similar size, who rely heavily on IT (which has evolved over the past 2 decades) to support their business operations, face similar issues. Our results are not generalizable to smaller organizations, more centralized ones, or larger international organizations that were "born digital" since they are likely to have other requirements and resources available. The observational data recorded in the OL was collected by a single researcher embedded in the PSC procurement project. Therefore, they had insights to all communications and attended most meetings, but may have missed or misinterpreted some individual interactions. To counter this, and to clarify ambiguities, R2 and R3 had several review sessions with R1 during data analysis.

Due to organizational constraints, it was not possible to conduct interviews with representatives of all involved departments, which would have provided a more complete picture of arising friction and hidden costs. We therefore identified and approached 6 key actors who had an overview over the whole process and how it affected their respective work and department. All quotes have been translated to English from its original language.[3]

4 Results

We present the results of our analysis in six parts: (I) A conservative cost calculation of the procurement process (based on estimated person-hours). (II) The reasons for procuring a SAC including PSC, and what individual stakeholders and the organization expected to achieve by implementing it (Section 4.2). (III) The steps that were undertaken over the course of more than one year in the selection and procurement process (Section 4.3). (IV) The stakeholders (including those that were not explicitly considered at the start) and processes involved at various stages of the decision (Section 4.4). (V) Conflicts and sources of friction with other goals and processes, and the hidden costs for the organization that resulted from these (Section 4.5). (VI) Workload and costs that occurred from the multitude of tasks for the stakeholders across the organization (Section 4.6).

Table 1: The conservative cost calculations for the stakeholders. *h*: the hours spend on the project per stakeholder group. *€/h* the estimated salary of the stakeholders. *Sum (€)* the total costs per stakeholder group.

Nr.	Stakeholder	h	€/h	Sum (€)
1	Team leads	25	35	875
2	Project Team	1,566	30	46,980
3	PoC User	37.5	30	1,125
4	Data Protection	13	30	390
5	Work Council	5	25	125
6	Infosec Board	27	55	1,485
7	CIO	3	85	255
8	Int. Communication	16	25	400
9	Mail Admins	11	25	275
10	Network Admins	8	25	200
11	Service Desk	9	15	135
12	Legal	4	35	140
13	Infosec team	20	30	600
14	Int. Colleagues	16	30	480
15	Compliance	9	30	270
16	Software Dev.	1	30	30
17	Procurement	24	20	489
		1,794.5		**54,245**

4.1 Cost Calculation

Based on the tasks carried out by the involved stakeholders, we calculated the approximate costs of the procurement

[3] We do not reveal the original language here to keep the country of our study anonymous.

process by summing up the estimated working hours of all stakeholder groups, and multiplying it with the average income of the stakeholder position[4] (see Table 1). The 1,794.5 working hours lead to total costs of **54,245€**. Since we did not document the exact amount of time effort of every individual involved in the process, this is an extremely conservative estimate, and also does not include the opportunity costs (such as profits these stakeholders normally generate on their main tasks). Note that these costs only present the working hours of the stakeholder during the procurement, leaving out the costs of the product, surrounding infrastructure and operational costs. In the following sections we dive deeper into the reasons for these tangible costs, as well as the intangible costs that – while hard to calculate – organizations should be aware of.

4.2 Drivers For And Expectation Towards a Phishing Simulation Campaign

In 2019, TruckCorp suffered an attack over the Christmas holidays. The initial attack included a phishing e-mail with malware, which TruckCorp's technical defenses did not recognize. An employee clicked and enabled the malware, which caused some damage. As a result, the organization's leadership mandated that all employees should undergo regular phishing simulations and SACs.

Further drivers were TruckCorp's customer requirements and the decision to obtain security certifications: *"customers have the requirements that we move in the direction of basic protection, [...]. And one requirement is that you complete target group-specific training."* – [P5]. *"The decision to use security awareness and measures has actually been around for years. [...] We have an area that is 27001 certified, and there has always been a requirement to train employees on a regular basis, which we have gradually expanded."* – [P3].

The fact that PSCs are widely advertised as "best practice" and go-to KPIs when aiming for "the human factor" e. g., by NIST [58], was also mentioned. So ultimately, we can identify the need to meet external IT security standards or certifications as major incentive to implement a SAC and PSC – rather than enabling employees to learn secure behaviors. Still, SPs often advertise PSC as a learning metric, enabling them to better protect the company against attacks.[5] However, no standardized methods exist to record these KPIs. Often it is about click- and reporting rates, which on their own have little significance. The interviewees were aware of this, but assumed that the data obtained through the PSC could provide information about "general behavior patterns", and to

[4] We used public databases such as glassdoor and stepstone to assess the average income, e. g., for "information security specialists" for the country of our study. We then rounded the results to keep the exact European country of our study hidden.

[5] For instance, one of the SP's marketing material states: *"Get a first-hand look at our product and find out how our phishing simulations can help your employees learn to actively protect your organization from attacks."* – [SP1].

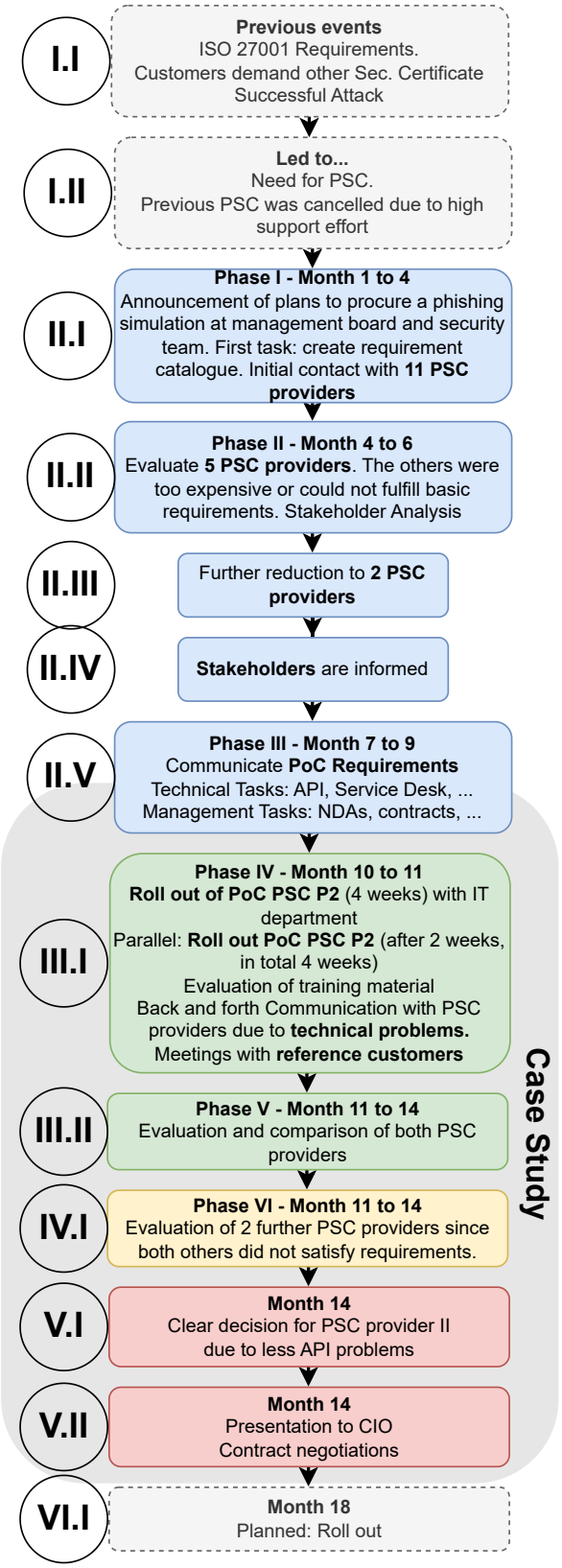

Figure 2: The different steps of the PSC evaluation process took 14 months, and longer until roll out.

answer questions like: *"Are there any sub-areas where a lot of people click on them? Are there certain characteristics in these sub-areas that we can connect? So the characteristics that we have to connect them, that is mostly location."* – [P3]. The expectation was to be able to identify hotspots of risky behaviors, and target them for further interventions, and, further, to use these KPIs to highlight the importance of security awareness and training to senior management, hoping for more understanding and budget in the future.

4.3 Overall Process Development

In total, the process of identifying a suitable SP and issuing a contract for a new PSC took over one year (see Figure 2). The phases that TruckCorp went through were as follows:

Project start: identifying possible SPs. In 2021, the Truckcorp CIO and division manager IS set up the project to identify and commission an SP. Initial requirements were reused and adapted from the first PSC in 2019 **(II.I)**. The main criteria were (I) high-quality phishing e-mail templates in all required languages, (II) automated categorization of e-mails reported by employees (usually via an integrated report button that had subsequent categorization options), and (III) an API interface. Plus, fit within a given budget. Since the market had moved on, the current SPs and their offerings were reviewed, and a pre-selection was made based on official market analysts articles, online research, and recommendations. During this time, the Information Security Board (**ISB**), with all the Information Security Officers from different areas, was informed about the idea of conducting a PSC. All ISB members were responsible for Information Security in specific areas or business units. In regular meetings the division manager IS presented the current status.

SP shortlist. 11 SPs were considered in the initial evaluation. The procurement team contacted them for for further information on their offers. 2 SPs did not respond. In this first iteration, the main criteria were pricing and the ability to simulate phishing e-mails. Only 5 SPs met the expectation of the requirements list. With these remaining SPs, detailed discussions about their product were arranged that each took about an hour and required the presence of at least one technical professional, and one organizational manager out of the project team. **(II.II)**. Additionally, the division manager IS attended these meetings as well. After this round, only 2 potential SPs remained in the contention for the PoC **(II.III)**:

- **SP1** was chosen because – based on the answers given at the meeting – they seemed to meet the requirements. For a newcomer, SP1 had a good reputation and larger reference customers.
- **SP2** was more established in the industry, and was one of the top picks of an international market research organization. Furthermore this SP was recommended by one of the ISB members.

During the consultations, the project team held with ISB and the CIO, it emerged that buying SAC and PSC from the same SP would be significantly cheaper than buying them individually. Thus, the project team requested new quotes for a combined PSC and SAC from both shortlisted SPs. During this time additional stakeholders were informed about the plan to test 2 products **(II.IV)**.

Pre-PoC-Phase. To further test the products, the project team conducted meetings to plan the PoCs. Within parts of the Corporate IT (approx. 150 IT professionals) both phishing solutions were to be tested **(II.V)**. At this time, SP2 quickly became the project team's clear favorite. SP1 had looked promising during the early stages, but was found to have a number of shortcomings in direct comparison with SP2, in particular, no measures to reduce ticket volume, and no API for import/export. Members of the project team started saying: "It's going to be SP2 anyway." However, since the procurement department required comparative price and service evaluation, the PoC had to be completed with both SPs.

All initial stakeholders were invited to a meeting to inform them about the procurement of a new PSC tool and the upcoming PoC. In the pre-PoC phase, all the technical requirements had to be implemented. The OL recorded a significant increase in numbers of e-mail and meetings – with other organizational stakeholders, but in particular with SP1. The most important implementation tasks were (I) phishing-button roll out for both SPs, (II) drafting an announcement e-mail for all PoC participants, (III) consulting TruckCorp's legal department on possible trademark infringement in phishing e-mails sent by SPs, (IV) liaising with TruckCorp's IT Service Desk, that would field queries by PoC participants, especially about the expected ticket volume, (V) contracts and documents gathering.

The PoC preparation phase took about 3 weeks longer than expected, due to slow or incomplete e-mail responses form SP1, missing documents on both sides, and vacation days.

PoC. The actual PoC phase lasted 6 weeks in total **(III.I)**. Due to the PoC phases for the 2 SPs now overlapping, employees enrolled received twice the number of phishing e-mails in those 2 weeks. During this time, every member of the project team blocked at least half of their work day, to further test and evaluate the 2 products. The most important tasks in this phase were: (I) Picking e-mail templates for the PoC from a selection provided by SP, (II) evaluating the content and language of the SAC modules provided by SP, (III) identifying KPIs, (IV) looking for a solution for reducing the workload of an expected increase in ticket volumes, while maintaining the ability to collect target group-oriented feedback, and (V) reporting technical issues, like wrong reporting settings, users

not being integrated correctly, and waiting for the SP's fixes – of which some could not be fixed by SP1 in the short term. Since these only caused minor issues during the PoC, the project team decided to just run with it – because at this stage, they already had decided SP1 would not be selected.

SP2 offered more technical add-ons (e. g., a quick phishing-template generator) so there was more for the project team to test. Again, the scheduled time of 2 weeks was not enough, so the PoC was extended, to allow for checking of the SAC content. That check revealed several shortcomings, e. g., that many SAC modules were not available in all necessary languages, a lot of content was only available with subtitles, cultural incompatibility of the material with European employees, and security advice that was not applicable to TruckCorp. Additionally, there was not enough target group-specific training material, e. g., employees with data protection roles. Much of the SAC turned out to be a collection of poster-type pages, rather than integrated e-learning materials.

Post-PoC & Decision-Making. The results of the PoC had to be compiled and prepared for presentations to the division manager IS, ISB and CIO **(III.II)**. Additionally, there were 5 internal discussion meetings for the project team and with the division manager about the missing education modules of SP2. Reluctantly, the division manager IS instructed a project team member to look for other SPs within 2 weeks **(IV.I)**. Together with a member of the IS division, they reached out to 2 further SPs. SP3 looked promising, so a 1 hour demo was arranged with total of 3 attendees from the project team and IS division. Afterwards the open questions from the project team could not be clearly answered within 2 weeks by the SP3. Since it was unknown if – and when – functions and translations could be added, the project team decided to decline SP3.

A final survey was conducted with all PoC participants that had access to the SAC modules. Their responses were tied between SP1 and SP2. The close majority of the ISB members preferred SP1, because they preferred their user interface and learning content. But the project team members decided to disregard the vote because SP1 had too many technical issues **(V.I)**. At a subsequent meeting with the ISB and the CIO, their choice was accepted **(V.II)**.

4.4 Involved Stakeholders

During preparation of the PSC, a stakeholder matrix was built, showing all departments & teams that needed to be involved – 16 in total, based on the prior matrix of the previous PSC.

The stakeholder table in Appendix 2 shows all involved stakeholders, highlighting whether they have been accounted for initially, as well as indicating the estimated time and work they facilitated. Our analysis shows that 4 stakeholders had been missed out, and that several stakeholders received more tasks than intended. Since the set up from vendors differ significantly, it was hard for the project team to estimate all the relevant stakeholders beforehand. Subsequently, several stakeholders could not find the time to complete their tasks.

Thus, many of the decision-makers outside of the project team did not review the SAC content that TruckCorp subsequently spent a six-figure sum on buying.

P5 and P6 said that they could not complete the SP assessment tasks on top of their regular work load within the short timeframe. Fig. 2 shows that they had 4 weeks in total for testing both SP. This turned out to be especially problematic for stakeholders or tasks that were not accounted for in the first place. For example, during the process the question arose, whether to use the selected SPs also for the data protection and compliance SACs, which already had a tool. But the compliance and data protection team did not have the resources to fully evaluate the relevant SACs – the data protection team did not look at the DP content at all.

4.5 Friction

The procurement & implementation of a SAC with PSC that fitted TruckCorp's requirements demanded a large amount of interaction and consultation with many of stakeholders within different TruckCorp departments, as well as external actors – and many of those interactions caused friction [9, 28, 37, 38]. Friction can sometimes be constructive, more often it reduces employees' productivity, causes stress and dissatisfaction, and clouds the work atmosphere. Analyzing our data through the lens of friction [9, 28, 37, 38] revealed the following key sources of friction: (I) between the requirements and SPs' offers, (II) between the different stakeholders, as well as in the (III) general procurement process.

TruckCorp requirements vs. SP offerings: *"Jam tomorrow".* The project team formulated multiple, specific requirements regarding the SAC and PSC. These were communicated beforehand through the procurement team and within multiple meetings. Although the SPs were convinced they could meet the expectations, there were multiple issues and requirements that turned out to not be manageable, e. g., language packages did not exist for all modules, missing content for promised target groups, missing measures to reduce the ticket volume, etc. SP representatives promised that they were aware of these issues, and that these would be fixed in the future. Problems experienced and reported by the project team during the PoCs were mostly deflected: *"these would not occur during a real implementation"* – [OL]. The promises that it would all be fine if the service was bought – which we coded as "jam tomorrow" – caused significant frustration and friction among TruckCorp staff involved, because they could not be certain that the service would meet their requirements when rolled out. A source of friction between the project team and other TruckCorp stakeholders was the decision to move to a new SAC platform – they wanted a PSC, but SPs' pricing for PSC plus SAC was perceived as "too good to refuse". This

ultimately led to TruckCorp now having 4 different training platforms that cover different topics – and that have to be paid for and maintained. On top of that, staff in some departments now to work through 4 different platforms to receive training.

P2 as part of the IT expressed the wish to *"... have a platform to cover all the topics. [...] A central tool, where all training courses are to be run, because we have too many tools for different training courses in use"*. Furthermore, other stakeholders anticipated friction and change costs associated with changing from a training platform that they and their employees were used to. Several departments that tested the SAC modules found the content quality was below that of existing materials: in parts it did not align with the organizations' security guidelines, which was confusing for employees (OL). According to the OL, as well as P5 and P6, this was particularly noticeable in situations where there were company-internal peculiarities, e. g., endpoint protection measures, or the handling of mobile phones for work.

The IS division wanted to be able to track which employees' clicked on the PSC's e-mails, to localize potential vulnerabilities (P3), and target them with specific training. Additionally, they wanted to identify technical problems, e. g., employees not receiving simulated phishing e-mails, or too many. This caused friction with data protection guidelines, especially GDPR. SP1 specifically advertises compliance with GDPR, and does not identify individual employees to their customer companies. As a multinational organization, TruckCorp requires the e-mail templates, as well as learning materials in many different languages, which presented a problem to both SPs: *"Other providers have then said, we have 2-3 core topics, which are available in all languages. Everything else beyond them you can no longer set up and handle on campaigns [because it is only available in English]"* – [P2]. In other cases, different languages were available but the (auto-translated) content did not fulfill basic quality criteria.

One SP quoted a significant additional sum for delivering their SAC in different languages, effectively outsourcing the translation cost to the customer (see Section 5.3). Target group-specific training for employees with different levels of IT and IS knowledge was a requirement for TruckCorp. Initially, both SPs indicated they would provide those, but then did not. Again: "jam tomorrow".

One SP sales manager even asked for a specific listing of desired topics and content, because they would then think about creating new suiting e-learnings – afterwards. Both SPs promised that the PSC would create "teachable moments" and render employees amenable to learning via the SACs offered. However, the PoC revealed a huge deviation between the click rates on simulated phishing e-mails, and subsequent click rates on the SACs, meaning that effect did not manifest.

Another major source of friction was the organization's technical requirements as opposed to the SPs' deployability. For example, to reduce the workload with handling incoming tickets, they needed a presorting mechanism. This caused friction with a lot of the SPs' offers. However, as this was the main reason for the last PSC to fail, this point was not open to discussion. Another issue was missing Application Programming Interfaces (API) – SPs used excel sheets for importing user data. For a larger company with several business units, this would be extraordinary tedious.

Ultimately, the result of the PoCs was that neither SP could meet all of TruckCorps' requirements, but it was still decided to proceed with purchasing the one that was the least bad fit.

Friction between Stakeholders: Different Needs and Values. In several stages of the process, friction occurred between different stakeholders who had diverging needs and values regarding the SAC and PSC.

The friction bewetween TruckCorp's requirements and the SPs' deployability has already been discussed. Yet friction also occurred within the organization, between the requirements of the IS and the mail and network team. The requested domain-names for the PSC e-mails would have never ended up in the users' mailboxes, due to the filters TruckCorp uses. Therefore the sender domains had to be adjusted.

Another important stakeholder was the service desk team, which was concerned about the increased workload associated with handling tickets. Additional meetings took place to address this concern. While some test users enjoyed the PSC, others were annoyed and complained to the IS division. Some employees thought the IS division was able to read their calendar and target emails accordingly. Many IT professionals, on the other hand, complained the e-mails were too easy.

Friction also arose between the procurement department's requirements, and the IS division. While it was clear quite early that the technical requirements could not be met by SP1, the procurement department insisted on a price proof and comparative evaluation – which significantly increased the workload for all stakeholders. A major source of friction was the different assessment of the the SAC content and effect of the PSC. Some business units valued the content of SAC higher than the PSC, because their units had specific requirements in terms of data protection. They had even developed their very own, organization-specific course material. During the process, they did not feel included enough, and, ultimately, their specific requirements not met.

Secondly, there were diverging views on which PSC templates could be used. Some TruckCorp stakeholders did not like the idea of "attacking" fellow employees, and were against PSC imitating internal e-mails. The SPs countered that "real attackers would not act like that", and this view was shared by all of the reference customers the project team spoke to. Most project team members also subscribed to the view that "closeness to reality" was more important than employees feeling tricked. But, ultimately, they bowed to the pressure from business units and refrained from using content such as e. g., imitating new data protection policies, or promising bonuses. A severe source of friction that affected

several stakeholders was a mismatch between the generic SAC content offered by SPs, and TruckCorp's requirements. Some SAC material contradicted TruckCorp's policies and practices, e. g., for endpoint-configurations. The content was also judged as culturally inappropriate: *"very American, very loud, very colorful – not fitting to our company."* – [OL].

Since every stakeholder was involved in many other projects, it was difficult to find suitable time slots for meetings, and get stakeholders to respond within deadlines.

4.6 Workload & Hidden Costs

Multiple costs (with regards to time, workload, newly involved stakeholders) that were not taken into account initially, occurred during the evaluation and procurement phase. We differentiated between the following categories: (I) General Workload & Time, (II) Hassle Factor, (III) Emotional Labor & Care Work, (IV) other work tasks.

I. General Workload & Time. In total, according to the OL, the project manager spent 83 working days on the facilitation of the implementation process (sick and vacation days not included). During this time period, they had at least 29 scheduled meetings with colleagues, SPs, and other stakeholders, 56 talks and discussions with colleagues, and worked on 77 e-mails that they sent or that were sent to them. While the project manager was specifically assigned the primary task of the procurement, the work often came on top of their general work tasks for the other stakeholders. Among these tasks, that were necessary for procurement, were (I) deducing the requirements, of which some were only identified during the process, compare them with SPs' offers, and communicate them to the SPs, (II) deducing different target groups, as this was not offered by the SPs, (III) reading through SPs' documents and instructions, e. g., for installment of technical specifities, (IV) going through and evaluating learning content, (V) going through, evaluating, and sorting out (un-)fitting e-mail templates, (VI) checking technical issues within own and with other departments, and finding solutions for them, (VII) checking in with the legal department on whether it was allowed to use brands in the e-mail templates, (VIII) paperwork, from contracts to checklists, (IX) checking black- and whitelisting, (X) asking for, obtaining, evaluating other stakeholders' feedback and trying to integrate it, (XI) going back and forth with the SPs, trying to find solutions to occurring issues before and during the PoC, (XII) evaluating tools and platforms, (XIII) preparing and conducting meetings with the SPs, other stakeholders, the reference clients, and within the team, (XIV) preparing and conducting presentations to IT and Management Board, (XV) preparing pro- and contra-Lists to assist decision-making, (XVI) researching other SPs, as the evaluated ones did not fully meet all criteria, and (XVII) dealing with procurement department's requirements.

II. The Hassle Factor. The "Hassle Factor" refers to work tasks that were particularly cumbersome, causing frustration and annoyance, literally getting on employees' nerves [9], and contributing to stress in the workplace. While some employees respond to security hassle with circumventions that undermine security [1], others may fall ill, and yet others see no other option than quitting their jobs to try and find better conditions elsewhere [50].

An indication of the amount of hassle the process caused is that, at one point, everyone involved in the process seemed to be so annoyed, that someone suggested: *"Let's just stop doing this."* – [OL].

Major contributors to the hassle factor were: (I) Technical issues that occurred during PoC that could not be adjusted; e. g., Whitelisting, missing working report button; incomplete roll out, (II) realizing early that a product (SP1) does not meet the requirements, but having to continue testing it to meet due procurement guidelines, (III) things taking a lot of time, having to deal with lots of different stakeholders, and explaining issues several times because of vacation times, (IV) being annoyed by inappropriate content in the education material, (V) being frustrated by bad communication within and with other teams which caused further delays, (VI) being annoyed by incongruities in the SPs' self-presentations and their actual offers (content wise and technically), (VII) being annoyed with workload of going through all the courses – but once you saw the low quality, there was a need to check, (VIII) being so frustrated to neither have the energy nor time anymore to keep quality high, (IX) being annoyed of feeling like a "broken record" that keeps on repeating the same issue, while nobody seems to listen, e. g., in regards to treating your coworkers with respect by not sending unfair e-mail templates, (X) being stressed by time running out due to procurement requirements, and (XI) being frustrated by lack of time to deliver a quality SAC and PSC due to lack of time, as well as lack of fitting offers.

III. Emotional Labor & Care Work. One aspect of work that is rarely accounted for is the emotional aspects, as well as care work, that people engage in, and that is fundamental for productive security, as well as a productive corporate culture. Analyzing our data through the lenses of emotional labor [31,36] and care [40,44] uncovered these, quite literally, hidden costs – which represented a decent amount of work that was necessary for procuring a quality SAC and PSC.

The OL reveals that several stakeholders engaged in care work when keeping in mind the effects of the PSC on other affected, yet not involved, stakeholders, and overall organizational culture, by: (I) checking the education material thoroughly, on whether the content was fitting and appropriate to the employees and organizational context, (II) trying to take on the employees' perspective and empathizing with them while doing so, e. g., to avoid them becoming bored or overwhelmed by the courses, and taking into consideration

employees' available resources, such as time and attention, to reduce friction and maintain productivity, (III) thinking about whether employees would actually profit, i.e., learning secure behaviors, from these materials, and whether it was understandable from their perspective and fitting to their contexts, (IV) checking for suitable – and unsuitable – e-mail templates, e. g., to prevent simulation of internal e-mails, which could negatively affect the organizational culture, (V) standing up for other employees and representing their needs in several meetings and discussions with internal and external stakeholders, (VI) checking in with, and taking into account the needs of other involved stakeholders, asking for and trying to integrate their feedback into the process, (VII) developing ones' own, department-specific learning material, and (VIII) caring for the SPs, in not wanting to give a "too negative" feedback.

While caring for others, compensating the aforementioned "hassle factor", as well as the friction during the process expanded upon in Section 4.5, in itself constitutes emotional labor, we identified other incidents that are worth mentioning in their own right: (I) having to deal with inappropriate and offensive content within the phishing templates and education material during evaluation, (II) dealing with negative, sometimes outright annoyed feedback from other involved or affected stakeholders, be it towards the education material or the PSC, (III) feeling unwell with specific statements in presentations, and having to present content that does not align with your and the organization's values in regards to the PSC, (IV) dealing with frequent unempathetic statements by other stakeholders, internal and external, who consider it necessary to "attack" work colleagues as realistically as possible, and (V) being ridiculed by other stakeholders for caring for stakeholders affected by the PSC.

IV. Other Work Tasks. We identified other work tasks and hidden costs that have to be taken into account, which we briefly summarize here.

Support effort & Employees Master Record Maintenance. During the previous PSC, the volume of tickets overwhelmed the support: *"We did a test roll-out [...] with about 500 users and received about the same number of tickets per month with false positives, which we have to process manually, and now we want to roll out the campaign for these 22,500 people. That means, [...] we would expect a ticket rate of 22,500 tickets, maybe half, let's say only 10,000. That would keep my team busy for a few days/months/weeks."* – [P3]. Also, this will cost additional effort from the security team itself: *"It will also have a direct impact on my team, because the support effort will increase, especially in the first months/weeks, and will be higher until we have parameterized it appropriately, and otherwise it will go into regular operation at some point."* – [P3].

A topic mentioned by all interview participants that caused a huge amount of work was the maintenance of the employee records (data sets that hold information about employees' names, positions, and contact details). Up-to-date records are key to automatically roll out a PSC to thousands of employees. However, it turned out, in a multinational organization the records bear some problems: *"It all starts with the fact that we have the names, the supervisors, the e-mail addresses of the end users. That everything is prepared sensibly and maintained properly. Since we are relatively decentralized, there are many people who maintain it. Wherever a lot of people maintain things, a lot of mistakes happen. That is the first challenge. That there are people in there who no longer exist, where the e-mail address is perhaps no longer correct, or who have since moved on, or are doing something else."* – [P1].

That led to the involvement of the security and IT teams in the maintenance of the records: *"[...] that's our main workload at the moment, and we're trying to absorb it through other processes, so we've added a first level, so that not everything ends up directly with us, but that our colleagues who deal specifically with identity management absorb it. So it's not just up to us."* – [P3].

5 Discussion

"To do this properly, you need more resources." – [OL].

Our results show that the process of procuring a PSC is not necessarily straightforward. Large organizations often have heterogeneous technical infrastructures and training requirements – so selecting the right product or service for an organization needs to involve i.e. time and effort from many different stakeholders. The process of balancing their – often contradictory – requirements is not straightforward. In our case study, contradictory requirements had not been anticipated, and the result was a drawn-out process rife with conflicts, unexpected extra work, a final decision that left half of the stakeholders unhappy, and the organization with a multitude of training platforms. Current PSC and SAC offerings seem to be geared towards large organizations with thousands of employees, but SPs are not able to tailor their offerings to complex technical infrastructures or specific content requirements. No SP could fulfill all technical and content aspects of TruckCorp. Even getting to the point of testing and deciding between 2 SPs involved considerable effort and hidden costs that organizations may not be aware of: (I) the procurement process for PSC and SACs creates significant additional tasks for most stakeholders involved, (II) SPs expect their customers to adapt their technical infrastructure to the product, and outsource quality control to the client, and (III) offer little support for target group-specific customization. The organization in our case study had an up-to-date technology infrastructure, well-resourced central IT and a dedicated IT security team,

plus experience in running consultations with stakeholders when planning and making changes to processes and technology. Organizations that do *not* have these resources are likely to encounter more issues and workload than TruckCorp did. Like TruckCorp, many organizations see PSCs as a quick and effective solution to employees clicking on potentially dangerous links. TruckCorp paid a high five-figure amount on the combined PSC and SAC; our very conservative estimate of the person-hours from different stakeholders in the procurement process is more than 50,000€. As [60] point out, there will be additional cost (lost productivity, dealing with reports and tickets) when the PSC is actually implemented.

No SP met all of TruckCorps requirements. This was obvious to all involved, and some frustrated stakeholders suggested "Let's just stop doing this". But as the organization had decided to purchase a PSC before investigating the market, key stakeholders felt they had to see it through. This is akin to the *sunk cost fallacy* by [3]: not wanting to "write off" the time and effort already spent, and not wanting to fail the organization's desire to comply with certification standards and security "best practices" [30] drove the organization to purchase the solution that offered "the least bad fit".

5.1 Security Awareness Is A Task On Top

The PSC was planned as a project with 3 main project members from the IS division – though they all had other tasks or project responsibilities. The time and effort of the other organizational stakeholders had not been budgeted for – they were expected to assess the SAC materials, and report observations during the PoC "on top" of their usual duties. Security specialists tend to assume that non-specialists can just absorb such extra effort for security – what Herley described as "valuing their time as zero" [28]. Unsurprisingly, many stakeholders did – and could – not complete their assigned tasks.

There were different and partly conflicting requirements for the PSC and SAC, e. g., the awareness manager wanted to focus on the content, while security team focused on API requirements. Without a process to determine what is best for the organization overall, stakeholders as principal agents [46] seek to minimize the cost for themselves. Here e. g., the help desk did not want anything that increased the number of tickets they have to deal with, IT procurement wanted to buy training and PSC from the same SP because it was cheaper and easier to implement, never mind the content. Such behavior patterns are common in organizations, and can lead to accumulation of hidden costs [46].

Insufficiently specific task assignments and/or communication made hidden costs worse. If every ISB member had actually reviewed the content of the SACs offered by SP1 and SP2, it would have been a huge time expenditure. Given these are senior staff, some – very sensibly – delegated the tasks of reviewing and checking translations to other employees in their business units, but some of their peers just gave up. P5 and P6 wanted to review the content, but report that too short deadlines caused stress for the ISB members who actually wanted to do the task. Volkamer et al. [60] pointed out the running PSCs created significant extraneous effort for non-security stakeholders; our results show that this was the case even during procurement. And since security specialists tend to disregard the effort involved in security tasks [28], the allocation of tasks and timelines for completion should be done by a stakeholder representative, not the security team.

5.2 Security Awareness Beyond Security

The tasks and decisions involved in procuring a quality PSC and SAC exceeded the capabilities and capacity of an average IS division. The core competence is on the technical aspects of security and preparing for a smooth running of the PSC. Arguably, detailed checking of SACs for compliance with organizational security polices, and organizing the checking of the quality of translations, is not a good use of their time. In the end, none of the SPs was able meet all the organizations' requirements. But the IS division had to pick a SP, or abandon the procurement process and tell organizational leadership that they were not able to roll out a PSC as requested, and considered necessary for compliance reasons. They chose to maximize their own utility [46] by opting for a combined PSC and SAC that (I) had the lowest "sticker price" (pleasing the procurement people), and (II) that met their own technical specifications, and thus created least work for them to implement. They had no incentive to consider the workload and cost that their decision caused for other departments, who had of course "been consulted". They also ignored that during the PoCs, only a small proportion of the clicks generated by the PSC translated into engagement with the SAC content – meaning that the combined product may be cheap, but not effective. Given the mounting evidence that being phished in the course of everyday work does *not* increase employee engagement with SAC content or improved performance in security tasks [14, 43, 60], organizations should re-consider using PSCs as the driver for their security awareness and training efforts.

Sasse et al. [55] argue that an approach that actually supports employees in recognizing phishing attacks, encourages learning and the development of secure behaviors requires a different type of organizational strategy and commitment. The content of learning materials should be evaluated and developed by professionals with the necessary skill set. Targeting of content, choice of delivery channels and timelines should be coordinated with department leaders. This points to having a dedicated position to manage and balance the negotiation process between the different stakeholder interests – as well as a dedicated security awareness team covering the required skills.

5.3 Offloading Work To Clients

The content of the SAC often did not fit organizational policies and cultural sensitivities – issues pointed out by the few stakeholders who managed to work through the material. Customer organizations who do not review materials in detail and request or make adaptions are likely to end up with content that does not fit. We identified several occasions in which the workload – and therefore the costs – to ensure a quality SAC and PSC was shifted from the SP to the client: (I) identifying necessary specific target groups by themselves, while this should be in the SPs' portfolio, and target group specific material did not even exist, (II) quality checking the education material and e-mail templates, (III) finding fitting e-mail templates and learning material fitting to the organization, (IV) proofreading – and finding mistakes – in the available translations, (V) having to pay for further, necessary translations, that could then be used by the SPs for other clients, and (VI) figuring out themselves how to handle the increasing workload due to raising ticket amounts.

This transfer of workload from the SPs to the client increases the person-hours, and thus the hidden cost, associated with procuring and implementing a PSC and SAC.

5.4 Recommendations For Organizations

Other researchers have cast doubt on the effectiveness of PSCs [43] and identified cost associated with running them [60]. Our results add costs the organization is likely to incur before even getting to the point of running it. If organizations use PSCs primarily to gather "some data" about employees' state of secure behavior [30] they should consider alternative metrics, like a reporting mechanism, surveys and technical logs. There is a lack of meaningful metrics for measuring employees' security awareness, which makes the apparently objective numbers PSCs so appealing – but that does not make them meaningful indicators of how vulnerable an organization is [60]. For organizations who want to implement a PSC – e. g., for compliance reasons – we can give the following recommendations: (I) *Identify clear goals* you want to achieve with a SAC and PSC and *how you will measure if they have been met*. Different SPs collect different data, besides click-rates and reported PSC e-mails – make use of that. (II) To implement a PSC and SAC a *correct master data* is crucial. Ensure this requirement *beforehand*. This will be also necessary to benefit from extra features some SPs offer. (III) There should be a *dedicated project manager* that has the resources to primarily manage the project team & other stakeholders, ideally nothing beyond. (IV) Consider establishing a dedicated *security awareness team*, that includes professionals in *education & human behavior* to ensure the facilitation of secure behaviors. (V) Make sure the educational content fits to *your organizations needs*. (VI) *Involve all the necessary stakeholders* in your organization right from the start, only assigning tasks that are mandatory, as well as needed resources. (VII) *Budget sufficient resources* in terms of costs, specialists, and time, beforehand – a quality SAC & PSC is not a short-term project to "tick a box".

6 Conclusion

We observed and documented the process of procuring a security awareness campaign (SAC) and phishing simulation campaign (PSC) in a large European company over a period of 5 months. The analysis of the data we collected during the case study, and subsequent interviews with key actors, revealed that – even though this was not the first time they had bought such a product – the process required a significant amount of time and effort by various organizational stakeholders. These are significant intangible costs that organizations do not account for, e. g., time for the API administration, quality checking and fixing of the content, and keeping management informed. Those costs amounted to more than 50,000€ in person hours, not including the opportunity cost of these stakeholders not attending to their main tasks. Further, it was just too much for some stakeholders, who more or less dropped out of the process – for instance, not all assigned stakeholders actually checked whether the SAC content matched policies relevant to their business units or translations. Thus, it is likely that issues will emerge later on. Further intangible costs were brought about by the friction the process caused between different organizational stakeholders – who did not agree on which service provider's (SP) offering to select – and the friction in interaction with the SPs, when trying to make their offerings fit with the organizations' needs. A majority of the customizing work had to be done by the organization. It is still unclear if the chosen SACs and PSCs will improve employees' security knowledge and behavior – since some stakeholders already identified mismatches between the content and their business units' needs.

Our study sheds light on these hidden costs, to enable organizations to understand that purchasing such a service, even if they do it mostly to "tick the box" of having a security awareness program to meet regulatory or certification requirements, requires resources beyond the tangible costs of paying the SP. We encourage further research on the actual costs of operating security measures – including the hidden ones – and actual effectiveness of security measures in organizational settings. The organization in this case study was large and had considerable security knowledge and staff, yet still ended up buying a service that did not meet several of its requirements. Also, more knowledge is needed especially in the area of small and medium enterprises, who have other requirements, fewer resources, and specialists to procure quality SACs and PSCs. Future work should also engage and include employees, to find out how they – and their productivity – are affected. Additionally, we encourage the development of metrics to measure and quantify these effects.

Acknowledgments

We thank TruckCorp and all involved employees for their trust and openness towards our research. We thank the 5 anonymous reviewers for their feedback and our shepherd for guiding us to acceptance. We thank Markus Schöps for his proof-reading. Our work was supported by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy – EXC 2092 CASA – 390781972 and (partly) also by the PhD School "SecHuman – Security for Humans in Cyberspace" by the federal state of NRW, Germany.

References

[1] ADAMS, A., AND SASSE, M. A. Users are not the enemy. *Communications of the ACM 42*, 12 (1999), 40–46.

[2] ALSHARNOUBY, M., ALACA, F., AND CHIASSON, S. Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies 82* (2015), 69–82.

[3] ARKES, H. R., AND BLUMER, C. The psychology of sunk cost. *Organizational Behavior and Human Decision Processes 35*, 1 (1985), 124–140.

[4] ASHENDEN, D. In their own words: employee attitudes towards information security. *Information & Computer Security* (2018).

[5] ASHENDEN, D., AND LAWRENCE, D. Security Dialogues: Building Better Relationships between Security and Business. *IEEE Security & Privacy 14*, 3 (2016), 82–87.

[6] ASHENDEN, D., AND SASSE, A. Cisos and organisational culture: Their own worst enemy? *Computers & Security 39* (2013), 396–405.

[7] BEAUTEMENT, A., COLES, R., GRIFFIN, J., IOANNIDIS, C., MONAHAN, B., PYM, D., SASSE, A., AND WONHAM, M. Modelling the human and technological costs and benefits of usb memory stick security. *Managing information risk and the economics of security* (2009), 141–163.

[8] BEAUTEMENT, A., AND SASSE, A. The economics of user effort in information security. *Computer Fraud & Security 2009*, 10 (2009), 8–12.

[9] BEAUTEMENT, A., SASSE, M. A., AND WONHAM, M. The compliance budget: managing security behaviour in organisations. In *Proceedings of the 2008 new security paradigms workshop* (2008), pp. 47–58.

[10] BECKER, I., PARKIN, S., AND SASSE, M. A. Finding security champions in blends of organisational culture. *Proc. USEC 11* (2017).

[11] BJ FOGG. *Tiny Habits: The Small Changes that Change Everything*. Houghton Mifflin Harcourt, 2019.

[12] BORGERT, N., JANSEN, L., BÖSE, I., FRIEDAUER, J., SASSE, M. A., AND ELSON, M. A Decade of Dividedness: A Preregistered Systematic Review of the Cybersecurity Self-Efficacy Methods, 2023.

[13] BORGERT, N., REITHMAIER, O. D., JANSEN, L., HILLEMANN, L., HUSSEY, I., AND ELSON, M. Home Is Where the Smart Is: Development and Validation of the Cybersecurity Self-Efficacy in Smart Homes (CySESH) Scale, 2023.

[14] CAPUTO, D. D., PFLEEGER, S. L., FREEMAN, J. D., AND JOHNSON, M. E. Going spear phishing: Exploring embedded training and awareness. *IEEE Security & Privacy 12*, 1 (2014), 28–38.

[15] CARELLA, A., KOTSOEV, M., AND TRUTA, T. M. Impact of security awareness training on phishing click-through rates. In *2017 IEEE International Conference on Big Data (Big Data)* (2017), IEEE, pp. 4458–4466.

[16] CHAUDHARY, S., GKIOULOS, V., AND KATSIKAS, S. Developing metrics to assess the effectiveness of cybersecurity awareness program. *Journal of Cybersecurity 8*, 1 (2022).

[17] COLNAGO, J., DEVLIN, S., OATES, M., SWOOPES, C., BAUER, L., CRANOR, L., AND CHRISTIN, N. "it's not actually that horrible": Exploring adoption of two-factor authentication at a university. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (2018), CHI '18, p. 1–11.

[18] DEMJAHA, A., CAULFIELD, T., ANGELA SASSE, M., AND PYM, D. 2 fast 2 secure: A case study of post-breach security changes. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (New York, 2019), IEEE, pp. 192–201.

[19] DHAMIJA, R., TYGAR, J. D., AND HEARST, M. Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems* (2006), pp. 581–590.

[20] DOURISH, P., GRINTER, R. E., LA DELGADO DE FLOR, J., AND JOSEPH, M. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing 8*, 6 (2004), 391–401.

[21] ENISA- EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY. Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity, 2019.

[22] FARKE, F. M., LORENZ, L., SCHNITZLER, T., MARKERT, P., AND DÜRMUTH, M. "you still use the password after all"—exploring fido2 security keys in a small company. In *Proceedings of the Sixteenth USENIX Conference on Usable Privacy and Security* (2020), pp. 19–35.

[23] FOR INFORMATION SECURITY, G. F. O. It-grundschutz-compendium: Orp.3 awareness and training in information security, 2021.

[24] FRANZ, A., ZIMMERMANN, V., ALBRECHT, G., HARTWIG, K., REUTER, C., BENLIAN, A., VOGT, J., ET AL. Sok: Still plenty of phish in the sea-a taxonomy of user-oriented phishing interventions and avenues for future research. In *SOUPS@ USENIX Security Symposium* (2021), pp. 339–358.

[25] GLOBENEWSWIRE. Global cybersecurity awareness training market size & trends, 2022.

[26] GORDON, W. J., WRIGHT, A., GLYNN, R. J., KADAKIA, J., MAZZONE, C., LEINBACH, E., AND LANDMAN, A. Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system. *Journal of the American Medical Informatics Association : JAMIA 26*, 6 (2019), 547–552.

[27] HANEY, J. M., AND LUTTERS, W. G. " it's scary... it's confusing... it's dull": How cybersecurity advocates overcome negative perceptions of security. In *SOUPS@ USENIX Security Symposium* (2018), pp. 411–425.

[28] HERLEY, C. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 workshop on New security paradigms workshop* (2009), pp. 133–144.

[29] HIELSCHER, J., KLUGE, A., MENGES, U., AND SASSE, M. A. "Taking out the Trash": Why Security Behavior Change requires Intentional Forgetting. In *New Security Paradigms Workshop* (New York, NY, USA, 2021), ACM, pp. 108–122.

[30] HIELSCHER, J., MENGES, U., PARKIN, S., KLUGE, A., AND SASSE, M. A. "Employees Who Don't Accept the Time Security Takes Are Not Aware Enough": The CISO View of Human-Centred Security. In *Proceedings of the 32nd USENIX Security Symposium* (2023), USENIX Security '23, USENIX Association. https://www.usenix.org/conference/usenixsecurity23/presentation/hielscher.

[31] HOCHSCHILD, A. R. The managed heart. In *Working In America*. Routledge, 2015, pp. 47–54.

[32] INGLESANT, P., AND SASSE, M. A. Studying password use in the wild: practical problems and possible solutions. In *Symposium On Usable Privacy and Security (SOUPS) 2010* (2010).

[33] INGLESANT, P., AND SASSE, M. A. Information security as organizational power: a framework for re-thinking security policies. In *2011 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST)* (2011), IEEE, pp. 9–16.

[34] ISO CENTRAL SECRETARY. Information Technology – Security techniques – Information Security Management – Measurement. Standard ISO/IEC TR 29110-1:2016, International Organization for Standardization, Geneva, CH, 2016.

[35] JAMPEN, D., GÜR, G., SUTTER, T., AND TELLENBACH, B. Don't click: Towards an effective anti-phishing training. a comparative literature review. *Hum.-Centric Comput. Inf. Sci. 10*, 1 (aug 2020).

[36] KAUR, M., RAMULU, H. S., ACAR, Y., AND FIEBIG, T. " oh yes! over-preparing for meetings is my jam:)": The gendered experiences of system administrators. *Proceedings of the ACM Human-Computer Interaction* (2022).

[37] KIRLAPPOS, I., BEAUTEMENT, A., AND SASSE, M. A. "comply or die" is dead: Long live security-aware principal agents. In *Financial Cryptography and Data Security: FC 2013 Workshops, USEC and WAHC 2013, Okinawa, Japan, April 1, 2013, Revised Selected Papers 17* (2013), Springer, pp. 70–82.

[38] KIRLAPPOS, I., PARKIN, S., AND SASSE, M. A. Learning from "shadow security": Why understanding non-compliance provides the basis for effective security. In *(Proceedings) Workshop on Usable Security* (2014).

[39] KIRLAPPOS, I., AND SASSE, M. A. What usable security really means: Trusting and engaging users. In *Human Aspects of Information Security, Privacy, and Trust: Second International Conference, HAS 2014, Held as Part of HCI International 2014, Heraklion, Crete, Greece, June 22-27, 2014. Proceedings 2* (2014), Springer, pp. 69–78.

[40] KOCKSCH, L., KORN, M., POLLER, A., AND WAGENKNECHT, S. Caring for it security: Accountabilities, moralities, and oscillations in it security practices. *Proceedings of the ACM on Human-Computer Interaction 2*, CSCW (2018), 1–20.

[41] KUCKARTZ, U. *Qualitative Inhaltsanalyse (German)*. Beltz Juventa, 2012.

[42] KUMARAGURU, P., CRANSHAW, J., ACQUISTI, A., CRANOR, L., HONG, J., BLAIR, M. A., AND PHAM, T. School of phish: A real-world evaluation of anti-phishing training. In *Proceedings of the 5th Symposium on Usable Privacy and Security* (New York, NY, USA, 2009), SOUPS '09, Association for Computing Machinery.

[43] LAIN, D., KOSTIAINEN, K., AND ČAPKUN, S. Phishing in organizations: Findings from a large-scale and long-term study. In *2022 IEEE Symposium on Security and Privacy (SP)* (2022), pp. 842–859.

[44] MOL, A., MOSER, I., AND POLS, J. *Care in practice: On tinkering in clinics, homes and farms*, vol. 8. transcript Verlag, 2015.

[45] OF STANDARDS, N. I., AND TECHNOLOGY. Pre-draft call for comments: Building a cybersecurity and privacy awareness and training program, 2021.

[46] PALLAS, F. Information Security Inside Organizations - A Positive Model and Some Normative Arguments Based on New Institutional Economics. *SSRN Electronic Journal* (2009).

[47] PARKIN, S., VAN MOORSEL, A., INGLESANT, P., AND SASSE, M. A. A stealth approach to usable security: Helping it security managers to identify workable security solutions. In *Proceedings of the 2010 New Security Paradigms Workshop* (New York, NY, USA, 2010), NSPW '10, Association for Computing Machinery, p. 33–50.

[48] PATTINSON, M. R., BUTAVICIUS, M. A., PARSONS, K., MCCORMAC, A., CALIC, D., AND JERRAM, C. The information security awareness of bank employees. In *HAISA* (2016), pp. 189–198.

[49] PFLEEGER, S. L., SASSE, M. A., AND FURNHAM, A. From weakest link to security hero: Transforming staff security behavior. *Journal of Homeland Security and Emergency Management 11*, 4 (2014), 489–510.

[50] PHAM, H. C., BRENNAN, L., AND FURNELL, S. Information security burnout: Identification of sources and mitigating factors from security demands and resources. *Journal of Information Security and Applications 46* (2019), 96–107.

[51] POLLER, A., KOCKSCH, L., TÜRPE, S., EPP, F. A., AND KINDER-KURLANDA, K. Can security become a routine? a study of organizational change in an agile software development group. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (New York, NY, USA, 2017), CSCW '17, Association for Computing Machinery, p. 2489–2503.

[52] REEVES, A., DELFABBRO, P., AND CALIC, D. Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue. *SAGE open 11*, 1 (2021), 21582440211000049.

[53] REINHEIMER, B., ALDAG, L., MAYER, P., MOSSANO, M., DUEZGUEN, R., LOFTHOUSE, B., VON LANDESBERGER, T., AND VOLKAMER, M. An investigation of phishing awareness and education over time: When and how to best remind users. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)* (2020), pp. 259–284.

[54] RIZZONI, F., MAGALINI, S., CASAROLI, A., MARI, P., DIXON, M., AND COVENTRY, L. Phishing simulation exercise in a large hospital: A case study. *Digital health 8* (2022), 20552076221081716.

[55] SASSE, A., HIELSCHER, J., FRIEDAUER, J., AND BUCKMANN, A. Rebooting it security awareness – how organisations can encourage and sustain secure behaviours. In *European Symposium on Research in Computer Security* (Berlin, 09 2022), Springer, Springer, pp. 1–18.

[56] SHENG, S., HOLBROOK, M., KUMARAGURU, P., CRANOR, L. F., AND DOWNS, J. Who falls for phish? a demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2010), CHI '10, Association for Computing Machinery, p. 373–382.

[57] SIADATI, H., PALKA, S., SIEGEL, A., AND MCCOY, D. Measuring the effectiveness of embedded phishing exercises. In *10th USENIX Workshop on Cyber Security Experimentation and Test (CSET 17)* (2017).

[58] STEVES, M., GREENE, K., AND THEOFANOS, M. Categorizing human phishing difficulty: a Phish Scale. *Journal of Cybersecurity 6*, 1 (09 2020). tyaa009.

[59] SUNDARAMURTHY, S. C., MCHUGH, J., OU, X., WESCH, M., BARDAS, A. G., AND RAJAGOPALAN, S. R. Turning contradictions into innovations or: How we learned to stop whining and improve security operations. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)* (2016), USENIX Association Denver, CO, pp. 237–251.

[60] VOLKAMER, M., SASSE, M. A., AND BOEHM, F. Analysing simulated phishing campaigns for staff. In *European Symposium on Research in Computer Security* (2020), Springer, pp. 312–328.

[61] WEIDMAN, J., AND GROSSKLAGS, J. I like it, but i hate it: Employee perceptions towards an institutional transition to byod second-factor authentication. In *Proceedings of the 33rd Annual Computer Security Applications Conference* (New York, NY, USA, 2017), ACSAC '17, Association for Computing Machinery, p. 212–224.

[62] YANG, W., XIONG, A., CHEN, J., PROCTOR, R. W., AND LI, N. Use of phishing training to improve security warning compliance: Evidence from a field experiment. In *Proceedings of the Hot Topics in Science of Security: Symposium and Bootcamp* (New York, NY, USA, 2017), HoTSoS, Association for Computing Machinery, p. 52–61.

A Ethics Protocol

A.1 Access to the field

Access to the field was granted by the TruckCorp CIO. Our principal researcher, R1, was well known within the IS division, as well as other departments, as they had carried out studies on the impact of security measures within the organization before under the supervision of R2 and R3 that colleagues and superiors in the IS division deemed helpful. After consultation with those, the Truckcorp CIO approved R1's proposal of a study in cooperation with university-based researchers. From then on, the study was also announced to the ISB and several times within the IS division. Further, all TruckCorp parties and stakeholders were informed about the study and agreed to participate. The SPs involved were informed that R1 was documenting and analyzing the process, and that they were working in collaboration with academic supervisors. As such, they were granted access to all relevant communication, meetings, documents, and so on. To protect anonymity of the organization we cannot reveal further information on the negotiation of access

A.2 Data Management and Analysis

The observations that were captured in field notes were highly standardized and structured by our research questions, i.e., capturing the stakeholders, their tasks, general workload, as well as occurrences of friction, care work, and emotional labor. All data (field notes, documents, observation log, interview recordings & transcripts) adhered to the strict European GDPR, and exclusively stored and encrypted at local machines and servers of TruckCorp and the research institution. The field notes were taken by R1 daily and digitally. These notes were then tidied up, consolidated, and formulated into the OL by R1, and shared with R2 and R2 for joint analysis. The 6 interviewees signed written consent forms, which were approved by a data protection officer, prior to being interviewed.

A.3 Safety Considerations (Risks)

To protect the anonymity of the organization and our participants we omit more detailed information about the our access to the organization, and more detailed descriptions of the position of R1, described the roles and position of our interviewees in vague rather than precise terms, give only vague descriptions of the SPs and their offers.

Due to the longitudinal nature of our research, and it occurring within everyday contexts, it is possible that persons involved "forgot" that an OL was written. To counter that, R1 tried to remind other stakeholders on several occasions on what was being captured. As a result, friendly jokes were frequently made on R1's role, indicating — and further spreading — awareness of the study. The willingness of 6 main stakeholders to engage in concluding interviews further highlights their positive attitude towards the study, which was also explicitly stated in personal conversations.

One critical point to navigate were the interactions with the SPs, as they were less frequent, involved changing stakeholders, and constrained by time, e. g., in meetings with a set agenda and time limit. These constraints, and the aim to prevent Hawthorne effects, made it impossible to remind them of the research at every occasion, as done with employees inside the organization. While they were generally informed about R1 being a researcher, due to the time passing between the interactions, they may have forgotten about the study. However, the high degree of standardization of the structured documentation process -– mainly focusing on the workload and costs for the organization — prevented capturing details that did not pertain to our research questions. We very carefully decided which data to include and to exclude from our analysis, and how we present it, to protect anonymity and maintain respect to all involved actors, while producing knowledge of societal value. Longterm documentation processes of this kind can be highly strength-draining for the researcher and involve ongoing self-reflexivity, the intricate management of an insider-outsider role, as well as emotions in the field. To accomplish this, R1 was supported by the supervision of experienced researchers in set bi-weekly meetings for reflection and discussion, as well as in-between-meetings if need be. During these meetings, upcoming ethical questions were further discussed, and R1 given the time to reflect on their experiences and emotions during their research.

A.4 Expected outcomes of the study (Benefits)

Due to past experiences and stories through the grapevine, we expect the costs (time, workload) for procuring a PSC to be way higher than advertised by SPs. By shedding light on these hidden costs, we hope to (I) increase awareness of decision-makers, who may then assign resources accordingly, (II) increase awareness on SPs, who may then improve their products, (III) by doing so, benefit employees who are the least accounted for stakeholders in PSCs.

A.5 Ethics

Our institution is a university in central Europe where the system regarding IRB approvals works differently from the USA. Usually, IRBs are only responsible for their specific disciplines, and approval is needed only for specific studies, which do not pertain to our research. On the other side we adhere to strict data privacy law — the GDPR. Further, our interdisciplinary team thoroughly and continually discussed ethical questions at each stage of the research (before and during data collection, analysis, and writing up).

B Stakeholder List

Table 2: An overview of all involved stakeholder, their tasks and involvement (1/2).

Nr	Stakeholder	Init	Task	Involvement
1	Project Team	Yes	Project Management; requirements catalog; stakeholder analysis and communication; provider selection and communication; reporting and feedback; maintenance and implementation of the PoC; evaluation of products and materials	During the procurement phase the three project team members invested multiple days per week. Ideally this workload decreases over time, when the SAC and PSC are implemented fully.
2	IT Procurement	Yes	Initial stakeholder meeting; first vendor contact; communication driver for requirements catalogue, legal documents; negotiation; purchasing	Depending on the procurement stage the IT procurement contact was heavily involved and spent several hours per week on the project. Due to fluctuation the main IT procurement contact changed, so a new employee had to familiarize with the project, and the team lead became backup contact for the project team.
3	Data Protection	Yes	Initial stakeholder meeting; Responsible contact for order processing contract, NDA, Processing activity; evaluation of the data protection related material and e-learnings from the vendors	One person had to check all the dedicated contracts and evaluate the data protection trainings from the both PoC vendors. This would have taken several hours, but the dedicated contact never had the time for content evaluation.
4	Work Council	Yes	Understanding and releasing the concept	This took a few hours for the council members
5	Information Security Board	Yes	Ongoing feedback loop; PoC vendor materials review: especially different languages and quality of the content; as part of the phishing simulation: interact with phishing mails (report or click) and evaluate, endsurvey on which vendor to choose	All board members took part in monthly meetings with short updates on the project development. Additionally every Member was supposed to take a a closer look into the materials, which would have taken multiple hours especially for two vendors. More than half of the participants did not give feedback before the endsurvey.
6	General Management / CIO	Yes	Budget-planning; ongoing feedback loop during the procurement phase; presentation of decisions; Offer acceptance	In total this cost a couple of hours during the procurement phase
7	Internal Communication/Marketing	Yes	Initial stakeholder meeting; Develop internal awareness advertisement materials; Internal announcement and communication on test users of phishing simulation	Depending on the procurement stage a couple of hours of workload for one employee. Due to frequent delays, the Internal Communication contact was asked to operate fast.
8	IT Department	Yes	Testing of the PoC Phishing Simulation, feedback through ticket system and in person	Hundreds of employees for a few minutes. No one gave feedback through the ticket system. Many opened a ticket because they did not know how to report the mail otherwise and thought it was real phishing.

Table 3: An overview of all involved stakeholder, their tasks and involvement (2/2).

Nr	Stakeholder	Init	Task	Involvement
9	Directory and Mail Team	Yes	Initial stakeholder meeting; setup mail rules: Mail bounces, report message button	This team communicated from the beginning that due to the high workload, the requests had to be announced early enough. Both PoCs may have taken a couple of hours to set up.
10	Network Team	Yes	Initial stakeholder meeting; firewall rules setup (enable provider templates, domains/dedicated IPs)	Similar to Directory and Mail Team.
11	Service desk	Yes	Initial stakeholder meeting; Processing or forwarding of the incoming tickets regarding the PoC	During the PoC the ticket volume increased an therefore more workload occurred. Orienting to the last campaign in the actual go-live this will take several hours per week
12	Legal Department	No	Review of contracts and documents; clarification on trademark related issues	A couple of hours for the complete PoC.
13	Parts of the remaining Information Security Division	Partly	Processing user-tickets; Evaluation of the e-learning and phishing mails from both PoC vendors; Reporting and technical support and monitoring	All team members were asked for feedback, only one colleague besides the project team had a closer look on the one of the two platforms, for approximately one or two hours including the written feedback. Furthermore, the dedicated ticket volume that the service desk could not handle increased the workload for other team members. A part-time employee was assigned to the further evaluation of the trainings at short notice, as the project team had to attend to other business tasks. This took several hours/week.
14	Sister-company / Affiliated company	Yes	Information loop, configuration setup PoC	The company themselves had to test their PoC setup with the vendors themselves. For TruckCorp only communication loop and a bit of technical recommendations. All in all approximately a few hours per month on keeping the contact up to date.
15	International colleagues	No	Proofreading and impressions of the trainings and their language quality	Several international colleagues were asked to review the PoC trainings regarding language and content. One person even sent a 12 page long correction of the translation of one of the vendors. This must have taken several hours.
16	Compliance department	No	Evaluation of the compliance related material and e-learnings from both vendors	This took approximately a couple of hours for both vendors.
17	Software Development Department	Yes	Initial stakeholder meeting; (optional) development of additional functions for the message report button	This department was not needed during the PoC phase, further involvement and effort unclear.