Selling Satisfaction

A Qualitative Analysis of Cybersecurity Awareness Vendors' Promises

Hielscher, Jonas; Schöps, Markus; Opdenbusch, Jens; Reichmann, Felix; Gutfleisch, Marco; Marky, Karola; Parkin, Simon

DOI
10.1145/3658644.3690196

Publication date
2024

Document Version
Final published version

Published in
CCS '24

Citation (APA)
Hielscher, J., Schöps, M., Opdenbusch, J., Reichmann, F., Gutfleisch, M., Marky, K., & Parkin, S. (2024). Selling Satisfaction: A Qualitative Analysis of Cybersecurity Awareness Vendors' Promises. In *CCS '24: Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security* (pp. 2666-2680). ACM. https://doi.org/10.1145/3658644.3690196

Selling Satisfaction: A Qualitative Analysis of Cybersecurity Awareness Vendors' Promises

Jonas Hielscher*
Chair for Human-Centred Security
Ruhr University Bochum
Bochum, Germany

Markus Schöps
Chair for Human-Centred Security
Ruhr University Bochum
Bochum, Germany

Jens Opdenbusch
Chair for Human-Centred Security
Ruhr University Bochum
Bochum, Germany

Felix Reichmann
Developer Centered Security
Ruhr University Bochum
Bochum, Germany

Marco Gutfleisch
Chair for Human-Centred Security
Ruhr University Bochum
Bochum, Germany

Karola Marky
Digital Sovereignty Lab
Ruhr University Bochum
Bochum, Germany

Simon Parkin
TPM Cybersecurity Group
Delft University of Technology
Delft, Netherlands

Abstract

Security awareness and training (SAT) vendors operate in a growing multi-billion dollar market. They publish various marketing promises on their websites to their customers – organizations of all sizes. This paper investigates how these promises align with customers' needs, how they relate to human-centered security challenges highlighted in prior research, and what narrative is presented regarding the role of employees (as SAT recipients). We also investigate the level of transparency in vendor promises, as to whether it constitutes an information asymmetry. We gathered search terms from $n = 30$ awareness professionals to perform an automated Google search and scraping of SAT vendors' websites. We then performed a thematic analysis of 2,476 statements on 156 websites from 59 vendors. We found that the messaging from SAT vendors precisely targets customers' need for easy-to-implement and compliance-fulfilling SAT products; how SAT products are offered also means that some of the impacts of SAT go unmentioned and are transferred to the customer, such as user support. In this vendor-customer relationship, employees are portrayed as a source of weaknesses, needing an indefinite amount of training to be incorporated into the organization's protection. We conclude with suggestions for SAT vendors and regulators, notably toward an SAT ecosystem that directly links SAT solutions to usable security technologies within the organization environment.

CCS Concepts

• **Security and privacy** → *Usability in security and privacy.*

*Corresponding Author. Contact: jonas.hielscher@ruhr-uni-bochum.de

CCS '24, October 14–18, 2024, Salt Lake City, UT, USA

ACM ISBN 979-8-4007-0636-3/24/10
https://doi.org/10.1145/3658644.3690196

Keywords

Security Awareness, Security Market, Human-Centered Security

ACM Reference Format:
Jonas Hielscher, Markus Schöps, Jens Opdenbusch, Felix Reichmann, Marco Gutfleisch, Karola Marky, and Simon Parkin. 2024. Selling Satisfaction: A Qualitative Analysis of Cybersecurity Awareness Vendors' Promises. In *Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS '24), October 14–18, 2024, Salt Lake City, UT, USA.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3658644.3690196

1 Introduction

Organizations worldwide invest billions of dollars annually into cybersecurity awareness and training (SAT), and the market is growing [76]. SAT vendors deliver training platforms, campaign material, and simulated phishing attacks to their customers: organizations of all sizes. Numerous studies have investigated how employee-facing SAT products are experienced and how they could be improved (e.g., [12, 47, 49, 54, 61]). Complementing this, there have been studies of how security managers manage the security-related behaviors of the users they serve (e.g., [9, 57, 64]). These prior studies (further detailed in Section 2) have identified a range of misalignments regularly noted from practice over time. These misalignments include users perpetually regarded as needing to do more for their organization's security. Yet, in parallel, users are treated as being the "weakest link" [70] in security. As SAT becomes a regular fixture in organizations, once users can be made to engage entirely with SAT content, they will variously behave securely. They will no longer be a source of security concerns for the organization.

Where these are typical concerns for security managers, the lack of resources to create SAT in-house on the customer side might be a major driver to rely on external SAT vendors [33, 38]. All the while, there are increasing compliance requirements to have SAT in place.[1] With greater compliance expectations comes greater

[1]The SAT vendor KnowBe4 claims that over 8,500 U.S. standards require SAT: https://www.knowbe4.com/resources/security-awareness-compliance-requirements/, accessed April 29, 2024.

involvement from stakeholders in adopting SAT products. This includes an organization's security manager as an SAT customer, their employees as recipients, and, of course, SAT vendors and SAT regulators, to name a few. Research has found that a new SAT product, such as anti-phishing training [14], can impact a range of functions in an organization. Previous studies have focused not only on employees as users but also SAT managers and Chief Information Security Officers (CISOs) as SAT product customers [33, 37, 38].

For the SAT market, prior research implies that SAT customers – whether a CISO or SAT manager – cannot verify the quality of SAT products by themselves [37, 38], and do not know how to effectively manage the human factor (e. g., [64]). This would then imply that they are in a precarious position of needing to trust the vendor. Where the SAT vendor has an understanding that the prospective customer does not, this constitutes an information asymmetry. The customer also has limited (if any) capacity or appropriate measures to check the product *claims* that the vendors make.

More broadly, within the cybersecurity and related product markets, prior examples of information asymmetries have been found between vendors and customers, such as with the security claims software vendors provide to potential customers [6, 7] – a *Market for Lemons* [3], where customers lack information about the quality of the product and are hence in a disadvantage. This highlights a concern that the SAT market may be its own Market for Lemons, which would require investigation.

In this paper, we examine the claims made by SAT vendors to understand what information asymmetries a potential customer of SAT products has to parse. One recent case study already pointed to SAT vendors' inability to keep their promises regarding easy implementation of their phishing simulation products into the customer systems [14]. We formulate the following research questions:

RQ1: What do SAT vendors promise their customers? Particularly, which problems do they claim their products solve?
RQ2: What products and services do SAT vendors offer?
RQ3: What image of users (employees) do SAT vendors communicate?

To explore the above RQs, we combine web-crawling techniques with qualitative coding methods to take the customers' perspective when studying SAT vendors (as detailed in Section 3): (I) Firstly, we gather search terms in an online questionnaire from $n = 30$ SAT professionals (Section 4). Those professionals sit on the customer side and need to buy and implement SAT in their organizations [34, 38, 41, 42]; (II) We then use the 112 provided search terms to perform automated searches with the Google API, where we crawled 843 unique websites; (III) We filter the websites based on strict vendor criteria; (IV) Finally, we qualitatively code and analyze 2476 statements on 156 websites from 59 vendors. Every code in the codebook is closely tied to one of the research questions to focus on the relevant statements out of the more than 50,000 statements within our dataset.

From our analysis of vendor websites (Section 5 to 7), we find that SAT products are adapted to the sparse time and resources of SAT managers, which leaves the improvement of security as a secondary goal for SAT. Fulfilling compliance standards and implementing new learning techniques like Microlearning and Gamification are essential selling points. We then find that the offered success metrics are inappropriate for tracking employees' behavior change. Employees are portrayed as weaknesses but also necessary parts of an organization's defense with no consideration for their limits (in terms of time and capabilities) or the requirement for usable security mechanisms that enable them to behave securely.

Our main contributions are: (I) We are the first to study the vendor side of the SAT ecosystem (that consists of CISOs and SAT managers buying SAT [37, 38], employees using it [26], and vendors marketing it). Without any understanding of SAT vendors, academic SAT interventions can only have a limited impact in practice, as the incentives of all SAT stakeholders decide how SATs are implemented; (II) We identify externalities created by the vendor-customer relationship that ensure that neither the vendor nor their customers are at fault if something goes wrong. (III) We identify *user archetypes* among the vendor claims that frame the user as a liability that implies that they are untrainable, even though this is exactly what vendors offer and what customers demand. (IV) We characterize the information asymmetries that exist in the SAT vendor-customer relationship, where the customer would struggle to independently measure the products they use. (V) We make suggestions as to how SAT products can be improved to serve the goal of better (usable) security.

2 Background & Related Work

Here we look at the definition of SAT and previous work studying SATs in organizations (Section 2.1), the customers of SAT vendors (2.2), and the information asymmetry present in the security market (Section 2.3). Hence, here we look at prior work in the *SAT ecosystem* with CISOs and SAT managers as SAT vendors' customers, employees as the SAT end-users, and SAT vendors as a special form of security vendor.

2.1 SAT in Organizations

Security Awareness & Training (SAT) is an underdefined term, yet used widely [38]. The terms *security awareness, training, and education* [32] are often used similarly in security research and are hard to distinguish [5]. While NIST 800-50 [79] defines awareness as a process to focus attention, training to generate necessary skills, and education to integrate all skills, we do not distinguish between employees' security training and awareness-raising measures. We consider any intervention, online or in-person, to increase employees' security knowledge and/or to change their behavior as SAT.

Hundreds of studies have investigated SAT "effectiveness" and how to improve them regarding user engagement or received knowledge [26, 49, 54]. Phishing simulations [16, 28, 40, 47, 53, 62], or trends like Gamification [22] got the attention of the HCS and usable security research community. However, only a small portion of those studies was carried out in real-world organizational contexts, e. g., [14, 40, 53], instead in (artificial) lab environments or with online surveys for a general population.

How To Measure Security Awareness. Measuring the awareness of employees is a critical step to analyze the effectiveness of security awareness campaigns [17] and to identify the weak spots of employees to allow for targeted training [71]. Measuring the

effect of awareness campaigns also facilitates their continuous improvement and shows the achieved return of investment (ROI) [17]. There are different ways to measure the awareness of employees: questionnaires and surveys, interviews, observations, monitoring, benchmarks, behavior tests, etc. [26]. In practice, questionnaires are the primary way of measuring awareness [26], even though the often used "knowledge query" is criticized as being not significant compared to real behavior measurements [68]. Still, to achieve "real" behavior measurement, the definition of metrics and the quantification of human behavior is necessary, which is often a problem for the industry [26].

2.2 SAT Customers

On the customer side of SAT, organizations of all sizes, public and private, buy SAT from external vendors. Those organizations can not or want to develop SAT by themselves. While in the biggest organizations, dedicated SAT managers might be responsible for buying and selecting SAT [14, 38], the vast majority of responsible SAT managers only have little of their time available to handle the procurement, implementation, or even improvement of SAT [33, 41, 42]. This lack of time and still little prioritization of HCS in organizations compared with technical security [37] might be another reason why SAT vendors thrive, as they promise to take away workload from their customers – while a previous case study [14] found that the SAT vendor promises, of easy and fast implementation, do not materialize in practice. When considering the costs of SAT, organizations need to consider the costs of procurement [14], the operational costs [14], but also the indirect costs in terms of employees' time [36] and harmful side-effects on employees motivation [12, 81]. In summary, incentives to sell, buy, implement, and measure SAT might exist from vendors' and customers' sides that are not built around the goal of increasing organizational security.

Compliance. One reason for increased interest in SAT capabilities will be regulatory expectations, which are becoming more explicit over time (e. g., NIS2 [24]), or nonetheless implied in more long-standing community guidelines (e. g., ISO27001 [45]). These materials define the role of SATs for more organizations. At least for US government agencies, compliance with certain standards is the most important indicator for successful SAT [46]. However, a study from Tsen et al. [74] indicates that implementing security frameworks by compliance rules does not correlate with fewer security incidents. Comprehensive figures on the number of organizations that deploy SATs are missing. In the UK, the government estimated that only 10% [58] of organizations implement SAT. That would leave great potential for further market growth. Available *market analysis* [29] shows that the market is not a monopoly but that multiple vendors are present, including traditional technology vendors.

CISOs. SAT comprises many activities, which include, but is not limited to advising on the creation of secure passwords [23] and the successful detection of phishing-emails [14, 16], the establishment of a "security culture" [21, 66], and the deployment of posters and other informational material [1, 10]. These activities are often seen by CISOs – the head of security in larger organizations – as a *fire and forget* approach [37], meaning there is a lack of clear measurements of success. Interestingly, CISOs sometimes see SAT as a mitigation strategy to solve friction caused by security, explaining to employees the need for these security measures [37]. However, CISOs are often doubtful about the positive effect of SATs [37].

Phishing Simulations hold a special place in the SAT toolkit: CISOs see them as the main tool for measuring employees' security behaviour [37], positively emphasizing the possibility of showing clear "reports" to superiors. Still, CISOs also report negative aspects of these simulations, citing that the relationship with employees may be burdened, which is also discussed in research [77]. Implementations are also not always as easy as thought [14].

2.3 A Lemons Market in SAT Journeys

Security managers may understand the needs of users, moreso if framed against e. g., support costs [11, 57]. However, a gulf exists between many (typically technical) security managers and the very human needs of non-expert users of security-related technologies in organizations [8, 9, 37, 64]. Some security managers are more able to determine the quality of SAT offerings than others.

Looking at other studies with and around vendors of security products, as already as in 2001, Anderson explained that an information asymmetry between security vendors and their customers created a *market-for-lemons* [6]: a situation where vendors can sell anything without the customers being able to verify whether the products deliver what is promised. Other scholars have confirmed this problem over the years [56, 67, 72]. Such asymmetry is possible where customers do not have the right tools or metrics to assess the security products they have bought, and measurements and creating reliable figures in security is notoriously hard [48, 59]. In regards to information asymmetry between vendors and users, a few studies have been carried out that investigate false claims by vendors, e. g., for VPNs [4, 25, 63], and false GDPR promises [30]. However, we are not aware of any such study in the realm of SAT.

3 Method

Here, we describe our multi-stage data collection and analysis method. This includes a targeted engagement with SAT professionals for search terms they use to find SAT products; using their search terms, we then appraised vendor website content for how it currently frames engagement with users. We performed an automated large-scale SAT vendor website crawling based on Google search results that we got through the gathered search terms. We then applied the same qualitative thematic analysis techniques that were previously used to study SAT managers and CISOs [20, 33, 37, 38]. We developed our research questions based on years of observations made while engaging with the SAT professionals community: we participated in dozens of SAT practitioner conferences and community events in Europe, where we participated in discussions with them. There, we got the impression that there may be a significant gap between what vendors promise and what organizations actually receive. To verify those assumptions, we gathered large sets of publicly available product information about security vendor claims, as it has been done previously, e. g., in the realm of VPNs [4]. Figure 1 summarizes our methodology.

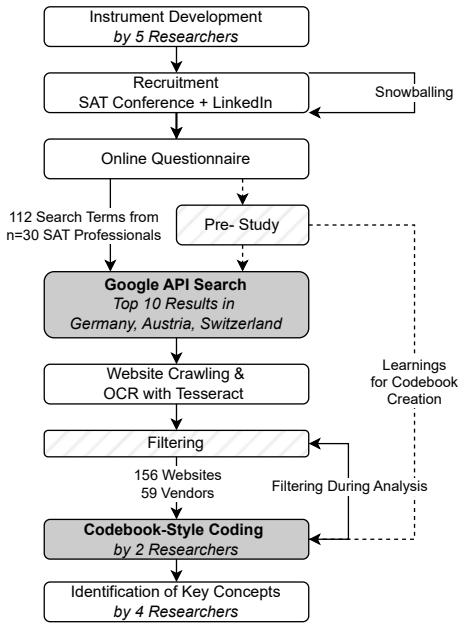

Figure 1: Our method: We gathered search terms from SAT professionals to find and analyze SAT vendors' promises.

3.1 User Survey

To study SAT vendors, we first need to identify them. We considered a few approaches, e. g., using publicly available lists of vendors, like the Gartner report [29]. The problem with such lists is that the selection criteria for vendors are unclear; it is unlikely that they are exhaustive, and they focus on *market leaders*.

We chose a different approach: we took the perspective of SAT professionals and created an online questionnaire (see Appendix A), where we asked the participants for search terms they would use to search for appropriate vendors – with the idea to collect search terms from security professionals already been used [50]. We recruited those professionals through our network, via LinkedIn, Snowballing, and from a group of SAT managers we had already recruited for a previous interview study [38]. The complete list of all search terms can be found in our online Appendix [39]. Since we wanted to keep the perspective of SAT professionals, we made no changes to the terms, meaning that we also kept not very promising terms, e. g., "awareness".

3.2 Website Crawling and Scraping

We deduplicated the search terms from the questionnaire. We inserted them in a script – where we forced the exact term through quotation marks, e. g., `"usable security"` – that gathered the URIs of the top ten Google search results, utilizing Google's Programmable Search Engine.[2] The API responses did not contain advertisements, so there was no bias toward vendors that paid Google to place their ads. We used the top ten results as they traditionally represent the first search results page that most users will click and begin to form opinions from – where we also followed guidelines from previous work [50]. We used every search term three times: once by selecting the regional identifier *Germany*, *Austria*, and *Switzerland* (commonly known as the *DACH* region). We chose these three countries since our survey participants were based there. We aimed to focus our research so that we could get more realistic localized results. The searches resulted in JSON-formatted results that a Google search would yield. These JSONs were then aggregated into one list containing the top ten URIs of each search. The list of URIs was then used to scrape all websites found by the Google search. To scrape these websites, we utilized Selenium[3] to not only download the source code of the website but to load the websites' frontend and screenshot them. We used the optical character recognition tool Tesseract[4] to convert the screenshots into PDFs and make the PDFs' text searchable and markable.

Filtering. We applied multiple rounds of filtering to reduce the initial dataset. (I) Firstly, we automatically filtered out all websites that did not include the term "security". (II) Then, we used a strict definition of an SAT vendor in our research: *a company with commercial SAT offers for all types of employees in different organizations.* With this definition, we excluded those vendors that only provided their products for a certain type of industry, e. g., healthcare, and those public agencies that offered free publicly available SAT content, like the British National Cyber Security Centre (NCSC). This strict filtering was introduced following our pre-study (Section 3.3), where we found that SAT products focused on specialized groups of employees (like software developers) were out of the scope of our third research question. We manually visited all domains where we searched for product information to validate whether a vendor met those criteria. All crawled websites were included in the qualitative analysis for all vendors who met the strict definition. (III) During the qualitative coding (Section 3.4), further filtering was applied: when we did not apply a single code on a website (e. g., because it was a technical FAQ), we removed the website from our set.

3.3 Pre-Study

We conducted a pre-study to familiarize ourselves with the method and research scope. In this pre-study, we utilized the gathered research terms and conducted a search and crawling of vendors' websites from the US and Germany. Four researchers then also created the first codebook for the crawled websites. Here, we learned valuable lessons that informed the main study, e. g., focusing on participants' perspectives, focusing our research on the DACH region, and screening vendors, e. g., excluding universities hosting SAT. We kept the questionnaire answers from the pre-study, but neither the crawled data nor the codebook were used in the main study. The coding of the pre-study provided lessons for the codebook of the main study. For example, we used a code "Security Myths", with which we coded SAT content that was, in our opinion, not appropriate. However, we then realized we were not able to make such judgments. We wanted to inform ways for the SAT ecosystem to improve, but our pre-study codes were pitched toward critique.

[2]Programmable Search Engine by Google: https://developers.google.com/custom-search, accessed April 29, 2024.

[3]Selenium: https://www.selenium.dev, accessed April 29, 2024.

[4]tesseract-ocr: https://github.com/tesseract-ocr, accessed April 29, 2024.

3.4 Qualitative Analysis

We used Kuckartz's [51] process scheme of content-structuring analysis, based on Braun & Clarke's [13, 18] theory of thematic analysis, where we used the *codebook style* coding – combining deductive and inductive coding strategies and a category-based evaluation along main codes. We used MaxQDA 2022 for the coding process. The coding process took four months and dozens of joint sessions between the coders. Deductive codes were created based on our research questions and the answers of our participants to the question *What would you look for when choosing a security awareness & training provider?* Codes that appeared to be judgmental were then changed based on lessons learned from the pre-study (Section 3.3). All those codes were reduced and combined into one final codebook in discussions between two experienced coders.

We decided to explicitly subordinate every code under one of the three research questions (see online Appendix [39] for the complete codebook). Through this explicit link to a research question, we could remove multiple initial codes containing information unrelated to our research questions, e. g., about the explicit costs of SAT products. This was necessary as our dataset included more than 50,000 statements, whereas only a subset of statements were within the realm of our research questions. All documents were then coded in joint sessions between the two coders, during which full agreement on the coding was reached. Four coders wrote up the results based on the coding and memos.

3.5 Ethics & Data Privacy

The institution where the study was set up did not have an institutional review board (IRB) nor an ethics review board (ERB) for security research. The PI followed institutional guidelines and best practices for ethical security research [75]. Regarding the questionnaire, we followed the strict European GDPR. All survey participants gave explicit consent to report their demographic data in an aggregated, anonymized form. The data protection officer approved the consent form. As compensation, we offered to share our study's results before publication. We decided against explicitly publishing the names of the vendors in this paper. It may be possible to deanonymize the vendors through a reversed search of the cited statements (where those are used). Still, we wanted to limit the impression that we would either support specific vendors whose advertised statements aligned with HCS research or blame those contradicting this research. As such, we also analyzed in a balanced manner – through regular team discussions, we aimed to monitor and manage any biases emerging from the analysis.

3.6 Limitations

Our methodology has multiple limitations. Firstly, not all vendors were presented equally in the dataset. While some vendors had multiple websites around different topics, some had only one website, maybe related to a specific topic like "Gamification". However, our dataset presents various vendors of different sizes and origins and allows deep insights into the various claims they make. We did not utilize all possible search terms but instead, realistic queries gathered from SAT practitioners. We analyzed publicly available data based on vendors' claims – their promotional material. We cannot validate whether the vendors can deliver what they promise. Details about the vendor products might also be hidden to protect vendors' intellectual property. As prospective customers, SAT managers could contact a vendor for more information, and more information is likely available beyond the website content we analyzed here. However, our analysis in later sections shows that the customer would be burdened with the responsibility to articulate the right questions to ensure that the SAT product functions smoothly, which can require understanding user needs. Hence, analyzing public claims is a suitable tool for addressing our research questions and gaining insights into information asymmetries between vendors and customers. Since Google search results are inconsistent, our results might not be fully reproducible, as future searches might deliver different websites. Our search was also not exhaustive: more vendors exist, as a look into the Gartner list shows [29]. Another limitation is that we did not talk directly to vendors. An approach of getting the vendor's viewpoint is useful in e. g., studies of VPN client applications [63]. It would, however, have somewhat defeated the purpose of examining website messaging to rely too heavily on explanations outside of that limited information that potential customers need to parse. Organizations will not base their decision to buy an SAT product solely on the results of a Google search, and hence, our method focuses on a specific approach to exploring options for an SAT product; prospective customers with large budgets might otherwise, for instance, go straight to a leader consultancy such as Gartner (and their reports), and in essence pay a premium to remove the guesswork and shortcut the exploration of identifying a suitable product. Hence, in-situ studies (like Brunken et al. [14]) are also required to understand procurement decisions in detail, as an understanding of human and organizational processes is still necessary to fit security to the business.

4 Results: Dataset

Here, we explain the key properties of our dataset. Since our codebook with the key themes was structured around our research questions, the presentation of our results is as well (RQ1: Section 5, RQ2: Section 6, RQ3: Section 7). Where appropriate, we link our results to previous work.

4.1 Search Terms

42 participants fully answered our questionnaire, out of which **n=30 participants** fulfilled our screening criteria. 9 participants were female, 15 male, and 6 did not want to answer. 23 participants worked with SAT on a weekly basis, 6 on a monthly basis, and 1 on an annual basis. 2 participants were 18-24 years old, 18 were 25-34, 7 were 35-44, and 1 was 45-54.

Participants provided us with 134 search terms, of which 112 were unique. With the automated Google Search of Top 10 results, we found 843 unique websites. We removed all websites that did not contain the keyword "security". We then reviewed the website previews to remove all that had no relation with SAT, e. g., domains with sexual health awareness or firewall security. We also removed all websites we knew might hold matching content but belong to no vendor, e. g., *acm.org* as a publisher for SAT papers. We coded and analyzed 189 websites. We removed 23 websites during coding, ending up with 156 websites from 59 vendors, where we coded 2.476 statements (from 56,211 total statements in the

data set, where we excluded statements unrelated to our research questions, such as pricing and subscription models). A statement was any complete sentence or phrase (e. g., "Entertaining, relevant learning experiences") containing information about the vendor or their products. Table 1 shows the accumulated key properties of the vendors. 31/59 vendors were not part of the Gartner list [29]. Despite our search from the DACH region, the largest number of vendors was US-based.

Table 1: Accumulated key properties of the vendors.

Primary Products	n = 59 #	%
Security Awareness	27	*46%*
Cybersecurity (e. g., Anti-Virus)	24	*41%*
E-Learning	4	*7%*
Technology (e. g., Software)	3	*6%*
Country		
United States	26	*45%*
United Kingdom	10	*17%*
Germany	7	*12%*
Australia	2	*3%*
Ireland	2	*3%*
Japan	2	*3%*
Netherlands	2	*3%*
Switzerland	2	*3%*
Denmark, Finland, France, Iceland, Israel, Russia	6x1	*11%*
Number of websites in our dataset		
>10	4	*7%*
5-9	6	*9%*
2-4	10	*17%*
1	39	*67%*

4.2 Choosing a Vendor

Our n = 30 participants made 111 statements on how they would choose a vendor (which informed the creation of our codebook). The most common statements were about (I) the type of training (18 participants, e. g., "short learning modules"), (II) the customizability of the SAT product (16 participants, e. g., "Customisability of the form 'can I adapt the look and feel that it feels like my organization?'"), (III) the easy implementation of the SAT product into the own systems (14 participants, e. g., "Can I embed the training in another LMS or other contents into the LMS of the provider?"), (IV) positive customer references (15 participants, e. g., "'N Training Programs Sold': The number of training programs sold."), and (V) that the SAT concept would be backed by science (9 participants, e. g., "Show me that they are doing it based on research").

5 Results: RQ1 – Promises

Here, we present the different reasonings the vendors used to justify why someone should buy their products.

5.1 1-Click Campaigns: Easy Implementation for Security Managers

The most common reasonings were built around the SAT products' easy setup, implementation, and administration. Here, 28 vendors made 141 statements. The vendors seemed to be aware that their customers deploying the SATs have limited resources [38, 41, 42] and need every help in implementing SATs they can get: *"Free up IT time to focus on big projects."* — [V14], or *"No security team has the time and resources to replicate the kind of sophistication and variety of a genuine phishing attack."* — [V52]. 16 vendors stated that their SATs could be launched within minutes, or *"in just a few steps"* — [V23]. The vendors undercut each other about the time until launch. While one vendor said it would take 20 days and another 14 days till their SAT products could go live, the majority wrote about 15, 5, or even 1 minute between the SAT setup and the start of the campaign, e. g., *"Go from zero to implemented in less than five minutes. Save time and money with our Click and Launch program."* — [V14].

Reflecting on the only peer-reviewed study investigating the effort it takes customers to implement SAT, it seems unlikely that the short periods the vendors promise can hold in practice [14]: the integration of SATs in the systems of larger organizations, in particular, can take months. Nevertheless, 17 vendors promised exactly such easy integration. 12 vendors offered the automation of SATs, like the automatic reassignment of training after some time. 8 offered easy administration, and 6 a usable administration experience. Four vendors directly addressed the SAT managers and explained that the SAT would free up the managers' valuable time: *"reduce their remediation workload by up to 90%. It saves them time and effort by automating and streamlining the following."* — [V54].

5.2 Easy Learning for Employees

Regarding the core concept of training and learning, vendors reported various product advantages. For one, many vendors mentioned user engagement as a necessary component for effective learning: 25 vendors explained this in 75 statements, always using the term "engaging" or a variation of it, e.g., *"All our e-learning courses and challenge games provide interactivity and engagement to impart knowledge effectively."* — [V20]. Fun was another concept that vendors liked to report, citing it as helpful to increase user engagement and, in turn, successful learning: 12 vendors mentioned this in 27 statements, characterizing their training components as fun, humorous, or lighthearted, e.g., *"[...] your training content must be fun, informative, and, above all else, consistently engaging."* — [V14]. 15 vendors stated that boring or non-engaging training was a problem: *"old-school e-learning (a.k.a. death by PowerPoint) is putting your employees to sleep."* — [V17]. 4 vendors explained that security awareness itself would not do the job: *"Security Awareness Is Dead."* — [V11].

Some vendors also mentioned the flexibility that users had with their training in learning when and how they liked: 12 vendors mentioned this in 17 statements, citing flexibility regarding time (because of voluntary short training units as described in Section 6.2.3) or flexibility regarding the device the training could be completed on (laptops, smartphones or tablets). Other advantages of easy learning mentioned were its relevance to users' daily lives and direct feedback.

5.3 The Non-Quantifiable Human Error

26 vendors made 58 statements about how dangerous humans would be for any organization's security. They presented a number – sometimes based on reports from their own white papers or large

tech companies like Verizon – to underline the danger, which was then followed with the natural solution for the problem: their SAT products, e. g., *"one in every five end users click on suspicious phishing message links [...] three-quarters compromised their data. By implementing dynamic security awareness training options, organizations can avoid extended downtime [...]"* — [V14]. The vendors presented different and often contradicting numbers to make their case for the danger through humans: Humans are responsible for 95% (2 vendors), 92% (1), 90% (5), 88% (1), 85% (3), 82% (4), 80% (1), 74% (5), 70% (1), 25% (1) data breaches. Phishing is involved in 90% (1), 75% (1), 36% (1), 33% (2) of data breaches. Four vendors stated that phishing would be the number one threat, and two, that human error would be the number one vulnerability.

Other presented numbers were that 95% of phishing emails would require human interaction to work (1), 1 in 5 users would click on (presumably simulated) phishing links (1), 1 in 10 would do this (2), 29% attacks would use stolen passwords (1), 22% of organizations were breached by an insider (1) and 20% by a remote worker (1). The most extreme statement was that *"ALL [100%] cyber attacks are rooted in human behavior manipulation, security awareness training is the most effective tool to safeguard sensitive information from hackers."* — [V14]. The numbers were not only contradicting between vendors, but sometimes one vendor would even use different numbers, e. g., one stated that *"phishing attacks account for 90% of data breaches"* — [V44], only one paragraph before they wrote *"a whopping 88% of data breaches being caused by human error"* — [V44].

5.4 Stakeholder Satisfaction

Vendors marketed their products to make two primary stakeholders happy that would judge the customers (the SAT manager): compliance auditors (Section 5.4.1) and management (Section 5.4.2).

5.4.1 For Compliance. 25 vendors explained in 86 statements that their SATs would help comply with various regulations and help the customer be prepared for any audit. In contrast, 7 vendors in 11 statements challenged the idea of using SATs (solely) to reach compliance: *"Paying lip service to basic compliance gets you nowhere."* — [V11]. 3 vendors warned their customers that non-compliance could lead to financial penalties, and 5 that they should always be prepared for audits: *"Track progress and run reports on completion for auditing purposes."* — [V20]. 4 vendors described SATs that would help to be compliant as something distinct to "normal" SATs, as an add-on: *"Not ready to set up a comprehensive phishing training and defense program? You can still get started right away and satisfy check-a-box compliance needs with our free Computer Based Training (CBT)."* — [V43]. The other 21 described it as intrinsic within their SATs. 15 vendors listed the specific regulations that their SAT would help to comply with: *"Many compliance regulations such as HIPAA, PCI, SOX, GDPR, and CCPA, and even some insurance requirements, require cybersecurity training for all employees."* — [V48]. The online Appendix [39] lists all regulations that were mentioned.

5.4.2 To Satisfy Management. 11 vendors claimed that their product would help to satisfy management that security awareness is taken care of. Besides reporting features of SAT products (Section 6.4.2), 4 vendors offered help getting more budget for security awareness. For example, the phishing susceptibility of employees was named to be *"great ammo to get budget"* — [V24]. V54 advertised the possibility of generating reports or dashboards to *"[...] get CISOs to prioritize behavior change program"* — [V54], indicating that these pages do not target CISOs but rather larger companies that have additional positions regarding security awareness, such as SAT managers [38, 41, 42].

5.5 Success Claims Through Case Studies

Only 11 vendors made 22 explicit statements on how the success of their SAT had been proven before – in numbers and through customer case studies. On all other websites and for all other vendors the reasoning for buying their product stayed generic and did not include any number that could be used to claim success. Six vendors stated that at their customers' organizations, the click rates in phishing simulations went down following their training, e. g.: *"Fortunately, the data showed that this 33.2% can be brought down to just 18.5% within 90 days of deploying new-school security awareness training. The one-year results show that by following these best practices, the final [Phishing] Percentage can be minimized to 5.4% on average."* — [V24]. Only one vendor claimed that their customers would experience fewer real-world malware infections following their SAT implementation: *"Our customers [...] reduce successful phishing attacks and malware infections by up to 90%."* — [V54]. Two vendors simply showed numbers for increased employee knowledge, one number for increased engagement through their Gamification solution, and another for increased employee satisfaction.

Summary – Section 5: Vendors claim that SAT is low-effort and achieved rapidly (which SAT managers with limited time resources are looking for [38, 43]) and often "user engagement" – grabbing user attention – will achieve success. This, in turn, should help to satisfy management and auditors [37, 38, 43]. Other vendors use confusing numbers to imply that security problems are mainly based on human error or wilful non-compliance with security and that this will be where to look if the situation needs to improve.

6 Results: RQ2 – Products

Here, we present our findings regarding the vendors' SAT products, services, and features.

6.1 Passwords & Co: SAT Topics

As SAT managers [38] and the vendors themselves (Section 6.3.2) describe the customizability of SATs as key, it is essential to know what topics the SATs can cover. For 27 vendors, we could identify topics: Social Engineering (22 vendors), Password and login security (18), Malware (15), Secure web browsing (10), Security when working remotely (10), Compliance related topics (8), Privacy (8), Endpoint Security (7), Physical Security (6), Threat Landscape (4), and Threats Through Artificial Intelligence (3). 3 vendors explicitly stated that some topics would also be relevant to the employees' personal lives. All those topics comprised of a mix of attacks, technologies, defenses, and behaviors. In no case did we see an example of how those topics would be taught, e. g., what exemplary scenarios would be used. Sometimes, the vendors would also use

rather technical terms, like "smishing" (phishing via SMS) or BEC (Business-Email-Compromise).

6.2 SAT Formats

In scientific literature but also in regulations, a variety of different SAT formats are discussed and suggested [65]. What 58 vendors had in common was offering some form of e-learning through their online awareness platform. Those ranged from simple video presentations to whole mobile app ecosystems. One vendor solely offered classroom-based training. In the following, we present all the other formats that we identified.

6.2.1 Simulated Phishing Attacks. Training employees through simulated phishing emails was an extraordinarily emphasized form of SAT product. 36 vendors offered those simulations and explained the details in 200 statements. The number one argument for buying a simulation was that they would easily generate numbers – and thus would show the progress of the training effort and could be used to report the results to other stakeholders (6.4.1). Besides this, the arguments were limited: 4 stated that simulations would be particularly easy to implement and sustain (*"Year-round all-you-can-eat simulated phishing attacks"* — [V24]), and 3 that it would be beneficial to train employees in a "simulated environment" of their everyday work.

13 vendors stated that it would be best to teach employees the moment they clicked through embedded training: *"[our] patented technology turns every simulated phishing email into a tool you can use to dynamically train employees by instantly showing them the hidden red flags they missed within that email."* — [V24]. For the other vendors, how they trained employees through simulations remained unclear. However, scholars have questioned the concept of embedded and just-in-time training for phishing simulations over several years through field studies [15, 53].

14 vendors explained in 61 statements how the phishing email templates would be generated. 6 vendors explained they build templates around "real-world phishing emails", with 4 being anti-virus providers that would gather threat intelligence from their filters to generate such emails: *"Insights from [... our threat intelligence] feed real, current threats into our phishing simulation."* — [V43]. 8 offered to customize phishing templates to their customers, e. g., *"Create custom phish emails that tie into specific areas [...], e. g., a fake message coming from your HR department."* — [V13]. 6 stated to update their phishing templates regularly, based on new threats, 6 that they would have thousands of templates available and 5 that those templates would be ready-to-launch, with no customization effort required from the customer. 2 vendors explicitly wrote that their phishing templates would come in different difficulty levels for employees. Only 4 vendors gave concrete examples of what a phishing email could look like or contain, e. g., *"From fraudulent shipping confirmation messages to suspicious gift cards and refund offers."* — [V14]. 4 vendors offered simulations on media different from emails, namely *"SMiShing, vishing, and USB baiting"* — [V39]. 13 vendors offered a plug-in to the customers' email client so that *"employees can also report and delete suspicious emails with the click of a button."* — [V43]. Notably, less than half of the phishing simulation vendors saw it as worthwhile to relate training to reporting and, hence, involving the employees.

Reflecting on possible negative side-effects of phishing simulation [14, 77] one vendor explained that phishing simulations could enrage employees and offered the matching solution: *"[our product] gamifies your phishing training, so your employees no longer see you as the villain behind phishing tests."* — [V7]

6.2.2 Gamification. 19 vendors explained in 59 statements that they would offer Gamification within their SATs. This ranged from "game-like-elements", like leaderboards and the collection of badges, over serious games within e-learning, to fully standalone games: *"The more Gamification elements are included, such as a leaderboard, badges, and story arcs, the more engaging and effective the game is."* — [V17]. The selling point for Gamification was the same among all vendors, that games would create fun and raise engagement to deliver otherwise boring training content: *"we should take a page from Mary Poppins who proclaimed; 'A spoonful of sugar makes the medicine go down.' [...] So the question is, how do we add the necessary value to motivate people to get up to speed on information security? The answer: Gamification and game-based learning!"* — [V26].

6.2.3 Micro-Learning. 14 vendors explained in 45 statements that they would offer micro-learning for employees. They explained that such ("science based") micro-learnings would help to deliver training with the limited level of concentration employees have, or with the retention that would be better compared to longer training: *"Encourage retention by breaking down training into manageable, bite-sized chunks through different mediums"* — [V20].

6.2.4 Newsletter, Posters, and Escape Rooms. 12 vendors would offer their customers regular newsletters or blog posts for the employees, informing them about the latest threats, e. g., *"Subscribe to weekly content. Send fast, relevant teachable moments throughout the year."* — [V18]. 11 vendors offered printed campaign materials like posters, flyers, comics, or textbooks. 4 vendors offered in-person escape rooms or war-room exercises. Only one vendor offered in-person classroom training.

6.3 SAT Features

Here, we explain what features the vendors promoted about how their SAT products would be built.

6.3.1 Behavioral Science Methods. 22 vendors explicitly stated that parts of their training were based on "behavioral science". 9 mentioned using nudges [83] to drive human behavior with reminders or notifications: *"To change security behavior, we need to focus on nudging employees towards system 2 thinking"* — [V6]. Besides nudging, the only other explicitly stated technique related to behavioral science was the use of behavior incentives: 18 vendors mentioned certificates, badges, or rewards as successful methods: *"Certificate printing where users can view/download/print their own certificates after completing a course"* — [V24]. 2 vendors mentioned giving recognition to trainees as an essential addition to awareness training to drive employee behavior.

6.3.2 Customizability of SATs. The possibility to change SAT products according to their requirements is important for SAT managers [33, 38]. We identified three different levels of such customization among the vendors' advertisements: Customizability on an organization-wide level, group- or role-wide level, and specific user

level. Organization-wide customization would allow the training to be adapted to a company's corporate design (10 vendors), security policies (7), perceived attack surface (5), or industry sector (3).

17 vendors mentioned group- or role-wide customization, and they offer adaptable content aimed at the position and security role the targeted user has within the company. For example, 5 vendors mentioned specific "management training". The most specific group for targeted training was single users (10 vendors). These vendors mostly advertised to be able to target the most *vulnerable users*, single them out, and *"[...] take swift action – more training, new policies – and make the biggest impact on security by focusing on these users and ignoring more vigilant ones."* — [V51]. Almost all customizations require customers to perform them manually, which implies heavy effort. 8 vendors reported some automation helping administer custom training to specific user groups. Half of those vendors mentioned AI or machine learning as being responsible for automation. We cannot state how accurate this kind of automation might be. Two further customization options were the language of the training and the difficulty level of the training. 11 vendors advertised their training material as being available in at least 8 different languages, with V27 claiming 180+ languages being supported. The difficulty level of the training was either advertised as connected to metrics that offer guidance on which difficulty is appropriate (5 vendors) or as pre-defined levels that an SAT manager or the user themselves can choose from (5).

6.3.3 Sophisticated SAT Library. 27 vendors advertised the diversification of the library of SAT content in 88 statements. They wanted to show that their content would be a good fit for customers based on four principles: (I) 18 vendors explained that their content was developed by experts: CISOs (4 vendors), industry experts (5), cybersecurity experts (5), ethical hackers (2), educationalists (2), psychologists (1), scientists (1), industrial designer (1), qualified security assessor (1), or TV specialists (1), e. g., *"The game covers a wide range of topics, put together by ethical hackers and educationalists."* — [V17]. (II) 17 vendors advertised the number of available training modules. They varied heavily from 12-15, up to 2,500 modules, e. g., *"the world's largest library with 1000+ Items of security awareness training content; including interactive modules, videos, games, posters, and newsletters."* — [V24]. (III) 8 vendors explained that their content would be updated regularly, on a weekly or quarterly basis, or based on new threats that emerge, e. g., *"The course content is updated quarterly to include recent examples of successful attacks and the latest trends that criminals use."* — [V20]. (IV) Two vendors wrote they would use daily gathered threat intelligence to update their content. No statement indicated that the customers' input or even feedback from the customers' employees would inform the adaptation of the content.

6.4 SAT Success Metrics

40 vendors promised their customers help in measuring the success of their SATs. The offered metrics and measurements were manifold. 15 stated they measure employees' security knowledge during or after an SAT campaign took place. The most common form of such measurement was described as a knowledge quiz the employees would have to take. Only one vendor gave insight into what knowledge they would measure: *"measure learner comprehension for each of the nine [NIST SP 800-50 [80]] core security behaviors."* — [V21]. 5 vendors offered a baseline measurement of employees' security knowledge before implementing an SAT campaign, 9 to survey employees for feedback and learn more about their knowledge level, and 6 to test for the "security culture". 6 vendors claimed to be able to measure employees' behavior change without providing details on how they would achieve this. In contrast, one vendor gave an example of what such behavior could be: *"tie training campaigns to behavior change objectives (e. g., reducing the number of individuals compromising online account credentials)."* — [V14]. Only 2 vendors stated they use technical metrics on real user behavior (e. g., the interaction with confidential documents in instant messengers) to determine the SATs' success.

12 vendors explicitly offered to measure employees' SAT participation and engagement rate – something SAT managers are particularly interested in [33]. 19 vendors made it possible to identify the "weakest users" through their measurements, those being the users who clicked on the most phishing emails or had the lowest quiz scores. Previous research found that SAT managers have trouble identifying meaningful metrics for their SAT campaigns [38]. Accordingly, one vendor considered it tough to measure the impact of SATs on an organization's security: *"The hard bit? Knowing how many breaches a security awareness training program prevents. That's because any sane organization Is understandably reluctant to equip only half their people with training and leave the other half untrained, just to compare the results."* — [V11].

6.4.1 Phishing Metrics. 12 vendors explained in 36 statements how their customers could and should measure employees' reactions to phishing simulations. Compared with the 36 vendors that we found that offered such simulations (6.2.1), we do not know what metrics the other 24 offer. The overarching idea of phishing metrics was presented as a measurement for the overall state of employees' awareness and the success of an SAT program: *"you can easily conduct simulated phishing attacks to test employees' security awareness as part of a comprehensive security awareness training program."* — [V53]. Interestingly, only 2 vendors explicitly mentioned the click rate as a metric – which has for long been described as the go-to phishing metric [33, 47, 52, 73], even in ISO 27004 [44]. 3 vendors promised to measure more advanced user interaction with a phishing email, e. g., the activation of macros in attached office documents (a problem described as solvable through usable security measures [31]). Two vendors questioned the meaningfulness of phishing metrics: *"But sometimes standard metrics don't tell the full story. Sure, you can produce charts showing clicks on phishing emails, but how do you measure the unquantifiable, such as your employees' perception of and care for your company's security?"* — [V51]. All other vendors just offered phishing metrics without going into details about it.

6.4.2 Generating Reports. 24 vendors explained in 69 statements that with the help of their SATs, the customers could easily generate reports – for themselves and other stakeholders. Those reports were described as important to track employees' progress during an SAT campaign, to calculate some form of "human risk score", to inform further action or adaption of the campaign, or to quantify potential risks: *"Are we at risk of our financial data being compromised from phishing? Do our users offer personal data when prompted? Is BEC a*

risk for us? Learn all this and more with our robust reporting." — [V31]. With industry benchmarking, 3 vendors promised to enable their customers to compare their SAT success with other organizations. 6 vendors had special reports that could be presented to executives or CISOs in their repertoire (5.4.2), 11 advertised their easy-to-use dashboards, 4 their just-in-time reporting, and 1 their large number of possible report-layouts.

Summary – Section 6: The SAT products come with integrated measurement tools to show their success, something that they indeed need for stakeholder satisfaction [33, 37, 38]. Measurement tools are developed and provided by the same vendor that builds the product. SAT customers rely on those tools, especially phishing metrics, and otherwise lack external verification [37, 38]. Many SAT products claim to leverage behavior-change methods and various forms of engagement. Associated with customers needing to trust the products, there is a focus on extensive training and visible activity – including reports for other stakeholders – which risks these attributes serving as a proxy for SAT effectiveness.

7 Results: RQ3 – Employees

Here, we explain the image of users (employees) that the vendors transported through their claims.

7.1 Employees' Effort

The vendors stated how much time and effort employees should spend on training and security tasks. However, only 3 explicitly acknowledged that besides SAT usable security solutions would be important, e. g., *"For example, organizations should provide employees with secure communication tools to help them avoid using unsecured public channels for sharing sensitive information."* — [V6]. 11 vendors urged their customers to *"[make] security a top priority for everyone in the organization"* — [V9], or stated that *"attending security awareness training should be your top priority."* — [V47]. 3 vendors warned that employees would circumvent security if it caused friction, and 4 acknowledged that employees would have limited time for security tasks or training: *"In a world where employees are constantly asked to 'do more with less', who has time for information security training?"* — [V26].

On the other hand, 14 vendors stated that employees needed continuous training to develop a routine for security tasks: *"It's about making security a habit and a part of your daily routine. You do it automatically because you know it's the right thing to do due to the behaviors installed in you while learning."* — [V6].

7.1.1 Time for Training. 30 vendors explained in 63 statements how much time employees should spend on training and how long the completion of their training modules would take. The differences were enormous: 2-3min (4 vendors), 5min (1), 8min (1), 10min (3), 15min (3), 30min (3), 45-90min (5). Employees should be trained daily (1 vendor), weekly (4), every few weeks (3), monthly (6), every few months (3), annually (1), or "regulary" (9). The smallest amount a vendor suggested was *"less than 20 minutes of employee training per year"* — [V10]. The largest was the employees' engagement every day. Following micro-learning principles, most vendors stated that training should be delivered regularly but in small doses. While all above statements were built around e-learning, 4 vendors also explained how often a phishing simulation should take place, e. g.,: *"we aim to send users at least 36 simulations a year. That's one every ten days."* — [V19].

7.2 Vulnerability or Shield?

Security scientists waver between the image of users as vulnerability and users as the victims of badly designed processes and systems – despite two very prominent efforts in 1999 to make a point for the latter [2, 78]. While human-centered and usable security scientists usually avoid blaming users and calling them the "weakest link", more technical security scientists do not. In accordance with this academic debate, the vendors put the employees on one of two sides: they are either a vulnerability of organizational security (34 vendors made 67 such statements) or need to be an active part of the defense (32 vendors made 80 such statements). In some cases, the vendors did both, e. g., *"Referring to end users as the weakest link is not to minimize their value in the organization but to shed light on the critical role each employee has in protecting the organization."* — [V55].

7.2.1 Shield. 9 vendors described employees as the "first line of defense" or "human firewall". 13 wrote that employees would need to play an active role in defense: *"awareness training builds a team of cyber-defenders and decreases the chances of a socially engineered cyberattack. By implementing a strong training program, your employees will be ready at your defense, and your organization significantly more fortified."* — [V44]. One vendor even explained how employees would need to help the security team fix their mistakes: *"the results of phishing training will show weaknesses in network defenses that security teams must address."* — [V43]. In contrast, 3 vendors described employees as the "last-line-of-defense". 14 generically stated that employees would need to be part of the defensive strategy. 5 vendors explained that since technical solutions would not be effective enough, it would be up to the employees to defend their organizations: *"Further, as cybercriminals become more advanced, some tools, especially free or budget solutions, can become less effective at flagging suspicious messages. That means it's up to your employees to help your company win the fight against phishing."* — [V5].

7 vendors explained that employees would be the strongest line of defense that an organization could have. While all those statements seem to be somehow similar, there is a subtle difference: being at the forefront of organizational defenses means that technical security will not do its job. Being in the last line means that all the technical protections must have failed first before the employees must take action. The latter seems to be the more appropriate perspective, as security can only be a secondary task for employees [11]. However, all those statements had in common that they put a burden, responsibility, and tasks on the employees.

7.2.2 Vulnerability. 15 vendors used some form of the "employees are the weakest link", and 9 stated that employees would be lazy and dangerous. Vendors gave concrete examples of human errors that would lead to data breaches: *"losing a portable user device, using weak passwords, [...]. No security program can effectively address cyber risk without [...] human vulnerability."* — [V2]. 2 vendors

described employees as "easy prey", e. g., *"Attackers go for the low-hanging fruit: humans"* — [V24]. In this regard, 6 vendors explained that *"all it takes is one click to leave your organization's sensitive information to hackers"* — [V14]. 5 saw the largest attack surface on organizations in terms of employees. 14 vendors described poor judgments and different forms of human error as dangerous: *"Human error caused by careless users who fall for social engineering attacks has become organizations' greatest threat."* — [V54].

Summary – Section 7: SAT vendors aim to teach their customers how to think about their employees and then offer the "right tooling" to change them. SAT customers get the problem description and solution from the same source: the vendors. By discussing the user as a potential "shield" or "vulnerability", vendors discuss how to change the user and co-opt them as part of the organization's defense. This is all while users also have productive work to do, where vendors' products are not informed by employees' needs for usable security/SAT.

8 Discussion

Here, we discuss our findings concerning our research questions and provide suggestions to advance the field of SAT.

8.1 Characterizing the Market

Regarding generalizability, our search brought up a heterogeneous set of SAT vendors from multiple countries with different company sizes and focuses. Our method was successful in discovering vendors that were not part of the Gartner list [29], approximately 50% of our dataset (Section 4). Despite the heterogeneity in the vendors' backgrounds, our analysis showed rather homogenous claims and promises: there was little differentiation between the vendors. Hence, there is a clear indication that our findings generalize well for those customer needs expressed in the search terms (online Appendix [39]). This generalization seems to also hold across various countries (with vendors originating in 14 countries).

8.2 Matching Customer Demands

Although a few vendors state that they offer novel ways to handle human risk by focusing on certain behaviors, vendors use similar claims to sell their products. Diversification is more clearly seen in terms of meeting customer needs (Section 6.3), by way of, e. g., bigger content libraries or easier integration.

Vendors' product claims closely match what SAT managers appear to need. What is of interest is the matching of the occupational needs of the manager, more so than the users that the manager serves – in its annual report, the US SANS Institute[5] reports that SAT managers *lack time for program management* [41–43], which was confirmed in academic studies [33, 34, 38]. The vendors appear to accommodate SAT managers with limited time resources on the customer side. Most sales arguments were based on making life easy for the managers (Section 5.1) through easy setup, integration, and administration. Other points from SANS reports matched the vendors' claims as well: the *inability to engage employees* was met with a wide number of activities (e. g., Gamification) that are conveyed as effective in engaging employees (Section 5.2), whereas the *lack of relevant SAT program metrics* was met with a variety of purportedly easy-to-implement measurements that would generate detailed reports (Section 6.4). Notably, any *limits on training time per employee* were met with a repeated call (supposedly towards CISOs or higher management) to make SAT a top priority (Section 7.1). This hints at the success of SAT products seeming to rely in part on non-security priorities somehow being deemphasized to make way for security, most notably as expectations of highly regular security training.

[5]While the SANS institute is an SAT vendor itself and its reports need to be read with care, multiple findings are in accordance with (more neutral) scientific findings.

8.3 Employees Archetypes

We find several "archetypes" that tell a story about employees (i.e., end-users) in organizations. By looking across vendors and their offerings (Section 7.2), we see variance and contradictions. There are representations of users familiar from existing research, such as users being described as the "weakest link", but also the user as a problem to fix, or the user as an under-utilized defense or spare resource in need of calibration. There is a contradiction when offerings frame the user as a liability yet somehow amenable to being retrained or upskilled – this subtly implies that security problems are wholly internal to the user, who can be remade to interact more productively with their environment (for security).

Taking a step back, the spread of variations on a "user as weakest link" framing would seem to imply that security management and security behaviors are two different worlds that never meet – we say this as, presumably, users would not appreciate being referred to in this way. Yet, the language continues to be used as if never challenged [27, 35, 69, 82]. This language does little to prepare SAT managers to engage effectively with users [64], or otherwise implies that SAT managers must carry two separate framings for two different conversations when talking to the vendor or the user.

We also noticed that the narrative about the employee captures a moment in time, not a journey. From our analysis, we saw no direct consideration of the employee who is on the other side and has *already* completed the training and, in turn, how a security manager should think of such users. A lack of narrative about "already trained" users may, paradoxically, appeal to a 'warrior' or protector narrative among CISOs [19], wherein the job can never be considered as complete, and vigilance must be maintained. The current model of SAT offering perhaps speaks to the customer who believes users create problems, or equally, the customer who does not know what users are doing [8, 64]. The issue here is that the message from vendors results in users being stuck in this state.

8.4 The Absence of Technology Usability

Our analysis shows that whether the technologies and processes a user interacts with are *usable* is not part of the conversation (Section 7.1). It could rationally be argued that usability is more aptly part of other engagements with e. g., technology providers. Yet, issues that may benefit from considering more usable solutions are seemingly portrayed by SAT vendors as being solvable with training. Prior research has argued that increasing security compliance should first address the *design* of solutions [12]. Yet, we see SAT vendors looking beyond design and suggesting that

non-compliance and compliance challenges can be addressed with further training. This defers any need for a synergy of SAT and more effective technologies around the user.

However, SAT vendors can only solve every problem with SAT – it is, by the nature of the market, the one tool in their toolbox. Vendors are not incentivized to imply a connection between effective SAT for users and effective technologies. Vendors may rationally assume that making organizational IT infrastructure usable for users is not their problem. There is then no incentive – and no way unless they are also the software/solutions provider – for them to get involved in a conversation about whether the technology in an organization is already usable. An unspoken assumption then appears to guide the market, where SAT vendors are not – at least visibly – incentivized to signpost that workable IT should be assured before SAT is provided. This points to the distance between usable systems and "security hygiene" in infrastructure [60], and a more popularized "cyber hygiene" as a set of secure working behaviors. Where a disconnect between these two "hygienes" has been noted elsewhere [55], our analysis provides a possible explanation.

8.5 Externalities Created by Vendors

Vendors provide SAT to managers in a customer organization, who then deploy it to users. Where vendors convey that SAT is easy to deploy (Section 5.1), this means that the customer is invested in a narrative where the user is perhaps the only stakeholder they can appeal to – or blame – if it does not work as expected. This isolates the vendor and the customer from fault if the SAT does not work. Unfortunately, this arrangement does not guarantee that SAT *will* work, relying on the users to ensure this. Perhaps ironically, this would be the same users often framed in practice and research as the "weakest link". Further, usability has little visibility. This implies, by omission, that the user needs no support to adopt secure behaviors and that enacting SAT and secure behaviors is problem-free, such as when managing credentials securely or if a user believes they have clicked on a real phishing link (Section 6.2.1).

Vendors' actions burden users with the need to do more to make the SAT appear successful. Our results show that vendors' talk of success relies on the amount of SAT and the harnessing – perhaps saturation – of user attention through different channels. This makes customers responsible for making it happen in practice and ramping up user engagement. There are then vendor-created externalities, i.e., costs created for other stakeholders without accountability coming back to the vendor. Best practices and regulations require that the SAT be in place, but they do not define a recourse if the SAT is considered ineffective. This ought to be addressed by ensuring the usability and relevance of SAT in regulations so that not all the burden sits with the user via the customer. We revisit this need in our recommendations in Section 8.7 and Section 8.8.

8.6 Asymmetries: A SAT Lemons Market?

We found vendors address customers' logistical needs (Sections 5.1 and 5.4), but they also tell customers how to think of employee behavior and what to do about the human (Section 7.2.1). SAT customers use the SAT vendors' tools to measure the success of the products they buy from those same vendors [37, 38]. Vendors control how the SAT is measured and by what measure success is defined. Hence, information asymmetry exists, where customers cannot readily measure SAT products in an independent manner, for instance, to measure the fit of SAT within organization processes. We then could consider the SAT market as a lemons market [6, 7], where an information quality problem exists. Following Moore's [56] theory, this would be the case where a customer is not measuring the right aspects and must be empowered to measure the right thing, or at least ask the right questions to a vendor. It is assumed that SAT will lead employees to behave securely if SAT engagement rates go up and simulated phishing click rates go down (Section 6.4). When an employee does not behave securely, something is assumed wrong with the person, not with the SAT. If the SAT does not change secure behavior, this problem does not come back to the vendor but stays with the customer, who then challenges employees as to why they do not behave securely. This is not to say that SAT products cannot work, but if the user is framed as problematic while SAT is framed as guaranteed to transform behavior, this points the blame at users when the customer's expectations are unmet.

8.7 Recommendations for Practitioners

Usability Support in Regulations. Regulations, like laws or security frameworks, seem to significantly influence the implementation of SATs (Section 5.4.1). Currently, user support is invisible and not the responsibility of any stakeholder [38]. Many regulations require SAT to be in place. Still, here we encourage introducing requirements regarding supporting employees who struggle with adapting secure behavior or otherwise, checking and ensuring usability so that there will be no such struggle. This would ensure that helpdesk or support demands are managed in step with usability [57] toward a more joined-up definition of sociotechnical security hygiene. Ideally, this would lead vendors and customers to develop alternative strategies to address employees' struggles beyond having (re-)training as the only available remedy. Currently, if a user cannot put the training into action, especially if SAT managers are encouraged to believe that they do not need to get involved in direct user engagement (Section 5.1), there are limited options to help a user work more securely if they have difficulties with the SAT – repeating the SAT is a blunt solution.

Support the Whole User Journey. SAT offerings framed the user journey as moving from lacking training and skills to embedding the necessary skills. What happens after the user is secure was not quite so clear. Vendor websites seemed to address only the start of the journey predominantly.

Ongoing, tailored training for already-secure users would conceivably result in ongoing business (and a favorable product lock-in), yet 'training for the untrained' was positioned as the solution to all user needs. We can only posit that support for the already-secure user is more expensive per head than upfront training packages or that this is an issue of vendor capabilities – they can tune media and engagement products. Still, they cannot troubleshoot limitations created by customers' complex IT systems and policies. It adds more weight, time, and uncertainty to the dialogue to accommodate user needs. Yet, e. g., Brunken et al. [14] show that pulling an SAT product in without this prior consultation can impose a range of unwanted costs onto an organization.

8.8 Recommendations For Researchers

Empower Customers with Requirements. To reduce externalities and information quality issues (Sections 8.5, 8.6), potential customers need independent ways to validate the SATs' impact. They could identify critical externalities if they had questions to ask the vendors, informed by human-centered research. The anti-phishing case study of Brunken et al. [14] highlights where qualifying questions could have helped a customer anticipate the workload on the IT helpdesk and other stakeholders following phishing simulations. This would also presumably help SAT vendors too, by setting more realistic customer expectations (as well as holding them more accountable for the effects their products have on users within an organization). Academics should categorize externalities in the field, focusing on newly deployed SAT or organizations changing SAT vendors. A set of questions should emerge for the SAT tendering process to surface expectations on non-security stakeholders.

Disentangle SAT & Technology. Vendors offer to customize their SAT to organizations (Section 6.3.2). However, we found no sign of vendors adapting their SAT to the technologies their customers use, e. g., a specific password manager or VPN product they have deployed. Hence, the employees can not be directly trained on a particular routine around the technologies they need to use. This incidentally implies that aspects particular to a specific technology product do not need to be considered for SAT to be effective. We recommend empirical research to map the distance between training and everyday instantiation of that training, where users potentially do hidden work to contextualize what they've learned.

9 Conclusion

Here, we qualitatively analyzed the public claims of 59 SAT vendors based on Google search terms that $n = 30$ SAT professionals provided us. SAT vendors offer a variety of techniques to help their customers with their limited time resources and satisfy management and regulators. Employees' needs and sustainable security behavior are not the focus of the products, and the success metrics offered do not provide insight into those. We conclude that incentives to design SATs to improve (usable) security measurably are missing on the vendor and customer side. However, adapted regulations can change those incentives without vendors risking losing their market.

Acknowledgments

We thank our participants for their contribution to our search. We thank Arthur Borem, Elleen Pan, Madison Pickering, and Maximilian Golla for their proofreading. The work was supported by the PhD School "SecHuman – Security for Humans in Cyberspace" by the federal state of NRW, Germany, and partly also by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA - 390781972.

References

[1] Jemal Abawajy. 2014. User preference of cyber security awareness delivery methods. *Behaviour & Information Technology* 33, 3 (2014), 237–248.
[2] Anne Adams and Martina Angela Sasse. 1999. Users are not the enemy. *Commun. ACM* 42, 12 (1999), 40–46.
[3] George A Akerlof. 1978. The market for "lemons": Quality uncertainty and the market mechanism. In *Uncertainty in economics*. Elsevier, Oxford, 235–251.
[4] Omer Akgul, Richard Roberts, Moses Namara, Dave Levin, and Michelle L. Mazurek. 2022. Investigating Influencer VPN Ads on YouTube. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, New York, 876–892. https://doi.org/10.1109/SP46214.2022.9833633
[5] Eric Amankwa, Marianne Loock, and Elmarie Kritzinger. 2014. A conceptual analysis of information security education, information security training and information security awareness definitions. In *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)*. IEEE, New York, 248–252. https://doi.org/10.1109/ICITST.2014.7038814
[6] Ross Anderson. 2001. Why information security is hard – an economic perspective. In *Seventeenth Annual Computer Security Applications Conference*. IEEE, IEEE, New York, 358–365.
[7] Ross Anderson and Tyler Moore. 2006. The economics of information security. *science* 314, 5799 (2006), 610–613.
[8] Debi Ashenden and Darren Lawrence. 2016. Security dialogues: Building better relationships between security and business. *IEEE Security & Privacy* 14, 3 (2016), 82–87.
[9] Debi Ashenden and Angela Sasse. 2013. CISOs and organisational culture: Their own worst enemy? *Computers & Security* 39 (2013), 396–405.
[10] Stefan Bauer, Edward WN Bernroider, and Katharina Chudzikowski. 2013. End User Information Security Awareness Programs for Improving InformationSecurity in Banking Organizations: Preliminary Results from an Exploratory Study. In *WISP 2012 Proceedings*, Vol. 2012. AISeL, Amsterdam, 1–17.
[11] Adam Beautement, Ingolf Becker, Simon Parkin, Kat Krol, and Angela Sasse. 2016. Productive Security: A Scalable Methodology for Analysing Employee Security Behaviours. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, Denver, CO, 253–270. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/beautement
[12] Adam Beautement, M. Angela Sasse, and Mike Wonham. 2008. The compliance budget: managing security behaviour in organisations. In *Proceedings of the 2008 New Security Paradigms Workshop* (Lake Tahoe, California, USA) *(NSPW '08)*. Association for Computing Machinery, New York, NY, USA, 47–58. https://doi.org/10.1145/1595676.1595684
[13] Virginia Braun and Victoria Clarke. 2021. One size fits all? What counts as quality practice in (reflexive) thematic analysis? *Qualitative research in psychology* 18, 3 (2021), 328–352.
[14] Lina Brunken, Annalina Buckmann, Jonas Hielscher, and M. Angela Sasse. 2023. To Do This Properly, You Need More Resources: The Hidden Costs of Introducing Simulated Phishing Campaigns. In *32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, Anaheim, CA, 4105–4122. https://www.usenix.org/conference/usenixsecurity23/presentation/brunken
[15] Deanna D Caputo, Shari Lawrence Pfleeger, Jesse D Freeman, and M Eric Johnson. 2013. Going spear phishing: Exploring embedded training and awareness. *IEEE security & privacy* 12, 1 (2013), 28–38.
[16] Anthony Carella, Murat Kotsoev, and Traian Marius Truta. 2017. Impact of security awareness training on phishing click-through rates. In *2017 IEEE International Conference on Big Data (Big Data)*. IEEE, IEEE, New York, 4458–4466.
[17] Sunil Chaudhary, Vasileios Gkioulos, and Sokratis Katsikas. 2022. Developing metrics to assess the effectiveness of cybersecurity awareness program. *Journal of Cybersecurity* 8, 1 (05 2022), tyac006. https://doi.org/10.1093/cybsec/tyac006
[18] Victoria Clarke, Virginia Braun, and Nikki Hayfield. 2015. Thematic analysis. *Qualitative psychology: A practical guide to research methods* 222, 2015 (2015), 248.
[19] Joseph Da Silva. 2023. Protection, expertise and domination: Cyber masculinity in practice. *Computers & Security* 133 (2023), 103408.
[20] Joseph Da Silva and Rikke Bjerg Jensen. 2022. " Cyber security is a dark art": The CISO as Soothsayer. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2 (2022), 1–31.
[21] Adéle Da Veiga and Jan HP Eloff. 2010. A framework and assessment instrument for information security culture. *Computers & security* 29, 2 (2010), 196–207.
[22] June de La Cruz and Sanchari Das. 2022. SoK: A Proposal for Incorporating Accessible Gamified Cybersecurity Awareness Training Informed by a Systematic Literature Review. In *Proceedings 2022 Symposium on Usable Security*, Katherine Krombholz and Prashanth Rajivan (Eds.). Internet Society, Reston, VA, 1–13. https://doi.org/10.14722/usec.2022.23080
[23] Mete Eminağaoğlu, Erdem Uçar, and Şaban Eren. 2009. The positive outcomes of information security awareness training in companies–A case study. *information security technical report* 14, 4 (2009), 223–229.
[24] European Commission. 2023. Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive).
[25] Matthias Fassl, Alexander Ponticello, Adrian Dabrowski, and Katharina Krombholz. 2023. Investigating Security Folklore: A Case Study on the Tor over VPN Phenomenon. *Proc. ACM Hum.-Comput. Interact.* 7, CSCW2, Article 344 (oct 2023), 26 pages. https://doi.org/10.1145/3610193
[26] Tobias Fertig and Andreas Schütz. 2020. About the measuring of information security awareness: a systematic literature review. In *Proceedings of the 53rd Hawaii International Conference on System Sciences*. AISeL, Amsterdam, 1–10.

[27] Dinei Florêncio and Cormac Herley. 2013. Where do all the attacks go?. In *Economics of information security and privacy III*. Springer, Springer, Berlin, 13–33.

[28] Anjuli Franz, Verena Zimmermann, Gregor Albrecht, Katrin Hartwig, Christian Reuter, Alexander Benlian, and Joachim Vogt. 2021. SoK: still plenty of phish in the sea—a taxonomy of user-oriented phishing interventions and avenues for future research. In *Proceedings of the Seventeenth USENIX Conference on Usable Privacy and Security (SOUPS'21)*. USENIX Association, USA, Article 18, 19 pages.

[29] Gartner. 2023. Products In Security Awareness Computer-Based Training Market. https://www.gartner.com/reviews/market/security-awareness-computer-based-training

[30] Moritz Gruber, Christian Höfig, Maximilian Golla, Tobias Urban, and Matteo Große-Kampmann. 2022. "We may share the number of diaper changes": A Privacy and Security Analysis of Mobile Child Care Applications. *Proceedings on Privacy Enhancing Technologies* 3 (2022), 394–414.

[31] Marco Gutfleisch, Maximilian Peiffer, Selim Erk, and Martina Angela Sasse. 2021. Microsoft Office Macro Warnings:A Design Comedy of Errors with Tragic Security Consequences. In *Proceedings of the 2021 European Symposium on Usable Security* (Karlsruhe, Germany) *(EuroUSEC '21)*. Association for Computing Machinery, New York, NY, USA, 9–22. https://doi.org/10.1145/3481357.3481512

[32] Barbara Guttman and Edward A. Roback. 1995. An Introduction to Computer Security: the NIST Handbook. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-12.pdf

[33] Julie Haney, Jody Jacobs, Susanne Furman, and Fernando Barrientos. 2022. Approaches and challenges of federal cybersecurity awareness programs. In *NIST Reports*. NIST Interagency/Internal Report (NISTIR), National Institute of Standards ..., Gaithersburg, 1–73.

[34] Julie Haney, Jody Jacobs, Susanne M Furman, et al. 2022. Federal Cybersecurity Awareness Programs A Mixed Methods Research Study. In *NISTIR 8420*. NIST, Gaithersburg, 1–48. https://doi.org/10.6028/NIST.IR.8420

[35] Ryan Heartfield, George Loukas, and Diane Gan. 2016. You are probably not the weakest link: Towards practical prediction of susceptibility to semantic social engineering attacks. *IEEE Access* 4 (2016), 6910–6928.

[36] Cormac Herley. 2009. 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* (Oxford, United Kingdom) *(NSPW '09)*. Association for Computing Machinery, New York, NY, USA, 133–144. https://doi.org/10.1145/1719030.1719050

[37] Jonas Hielscher, Uta Menges, Simon Parkin, Annette Kluge, and M. Angela Sasse. 2023. "Employees Who Don't Accept the Time Security Takes Are Not Aware Enough": The CISO View of Human-Centred Security. In *32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, Anaheim, CA, 2311–2328. https://www.usenix.org/conference/usenixsecurity23/presentation/hielscher

[38] Jonas Hielscher and Simon Parkin. 2024. "What Keeps People Secure is That They Met The Security Team": Deconstructing the Incentive Structure of Organizational Security Awareness. In *33nd USENIX Security Symposium (USENIX Security 24)*. USENIX Association, Philadelphia, PA. https://www.usenix.org/conference/usenixsecurity24/presentation/hielscher

[39] Hielscher et al. 2023. Online Appendix. https://doi.org/10.4121/5e7d7ae2-c639-4bcc-8664-a4ad5526868e.

[40] Doron Hillman, Yaniv Harel, and Eran Toch. 2023. Evaluating Organizational Phishing Awareness Training on an Enterprise Scale. *Computers & Security* 1 (2023), 103364.

[41] SANS Institute. 2021. *2021 SECURITY AWARENESS REPORT – MANAGING HUMAN CYBER RISK*. Technical Report. SANS Institute.

[42] SANS Institute. 2022. *2022 SECURITY AWARENESS REPORT – MANAGING HUMAN CYBER RISK*. Technical Report. SANS Institute.

[43] SANS Institute. 2023. *2023 SECURITY AWARENESS REPORT – MANAGING HUMAN CYBER RISK*. Technical Report. SANS Institute.

[44] ISO Central Secretary. 2016. *Information Technology – Security techniques – Information Security Management – Measurement*. Standard ISO/IEC TR 29110-1:2016. International Organization for Standardization, Geneva, CH.

[45] ISO Central Secretary. 2022. *ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements*. Standard ISO/IEC TR 29110-1:2016. International Organization for Standardization, Geneva, CH.

[46] Jody L. Jacobs, Julie M. Haney, and Susanne M. Furman. 2023. Measuring the Effectiveness of U.S. Government Security Awareness Programs: A Mixed-Methods Study. In *HCI in Business, Government and Organizations*, Fiona Nah and Keng Siau (Eds.). Springer Nature Switzerland, Cham, 14–33.

[47] Daniel Jampen, Gürkan Gür, Thomas Sutter, and Bernhard Tellenbach. 2020. Don't click: towards an effective anti-phishing training. A comparative literature review. *Human-centric Computing and Information Sciences* 10, 1 (2020), 1–41.

[48] Andrew Jaquith. 2007. *Security metrics: replacing fear, uncertainty, and doubt*. Pearson Education, London.

[49] Khando Khando, Shang Gao, Sirajul M Islam, and Ali Salman. 2021. Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & security* 106 (2021), 102267.

[50] Jan H. Klemmer, Marco Gutfleisch, Christian Stransky, Yasemin Acar, M. Angela Sasse, and Sascha Fahl. 2023. "Make Them Change It Every Week!": A Qualitative Exploration of Online Developer Advice on Usable and Secure Authentication. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS '23)*. Association for Computing Machinery, New York, NY, USA, 2740–2754. https://doi.org/10.1145/3576915.3623072

[51] Udo Kuckartz. 2012. *Qualitative inhaltsanalyse (German)*. Beltz Juventa, Weinheim.

[52] Ponnurangam Kumaraguru, Justin Cranshaw, Alessandro Acquisti, Lorrie Cranor, Jason Hong, Mary Ann Blair, and Theodore Pham. 2009. School of phish: a real-world evaluation of anti-phishing training. In *Proceedings of the 5th Symposium on Usable Privacy and Security* (Mountain View, California, USA) *(SOUPS '09)*. Association for Computing Machinery, New York, NY, USA, Article 3, 12 pages. https://doi.org/10.1145/1572532.1572536

[53] Daniele Lain, Kari Kostiainen, and Srdjan Čapkun. 2022. Phishing in organizations: Findings from a large-scale and long-term study. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, IEEE, New York, 842–859.

[54] Benedikt Lebek, Jörg Uffen, Michael H. Breitner, Markus Neumann, and Bernd Hohler. 2013. Employees' Information Security Awareness and Behavior: A Literature Review. In *2013 46th Hawaii International Conference on System Sciences*. IEEE, New York, 2978–2987. https://doi.org/10.1109/HICSS.2013.192

[55] Kaie Maennel, Sten Mäses, and Olaf Maennel. 2018. Cyber hygiene: The big picture. In *Secure IT Systems: 23rd Nordic Conference, NordSec 2018, Oslo, Norway, November 28-30, 2018, Proceedings 23*. Springer, USA, 291–305.

[56] Tyler Moore. 2010. The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection* 3, 3 (2010), 103–117. https://doi.org/10.1016/j.ijcip.2010.10.002

[57] Simon Parkin, Aad van Moorsel, Philip Inglesant, and M. Angela Sasse. 2010. A stealth approach to usable security: helping IT security managers to identify workable security solutions. In *Proceedings of the 2010 New Security Paradigms Workshop* (Concord, Massachusetts, USA) *(NSPW '10)*. Association for Computing Machinery, New York, NY, USA, 33–50. https://doi.org/10.1145/1900546.1900553

[58] Daniel Pedley, Tania Borges, Alex Bollen, Jayesh Navin Shah, Sam Donaldson, Steven Furnell, and David Crozier. 2020. UK DCMSC: Cyber security skills in the UK labour market 2020.

[59] Marcus Pendleton, Richard Garcia-Lebron, Jin-Hee Cho, and Shouhuai Xu. 2016. A Survey on Systems Security Metrics. *ACM Comput. Surv.* 49, 4, Article 62 (dec 2016), 35 pages. https://doi.org/10.1145/3005714

[60] Shari Lawrence Pfleeger, M Angela Sasse, and Adrian Furnham. 2014. From weakest link to security hero: Transforming staff security behavior. *Journal of Homeland Security and Emergency Management* 11, 4 (2014), 489–510.

[61] Julia Prümmer, Tommy van Steen, and Bibi van den Berg. 2024. A systematic review of current cybersecurity training methods. *Comput. Secur.* 136, C (feb 2024), 20 pages. https://doi.org/10.1016/j.cose.2023.103585

[62] Issa Qabajeh, Fadi Thabtah, and Francisco Chiclana. 2018. A recent review of conventional vs. automated cybersecurity anti-phishing techniques. *Computer Science Review* 29 (2018), 44–55. https://doi.org/10.1016/j.cosrev.2018.05.003

[63] Reethika Ramesh, Anjali Vyas, and Roya Ensafi. 2023. "All of them claim to be the best": Multi-perspective study of VPN users and VPN providers. In *32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, Anaheim, CA, 5773–5789. https://www.usenix.org/conference/usenixsecurity23/presentation/ramesh-vpn

[64] Lena Reinfelder, Robert Landwirth, and Zinaida Benenson. 2019. Security Managers Are Not The Enemy Either. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–7. https://doi.org/10.1145/3290605.3300663

[65] Benjamin Reinheimer, Lukas Aldag, Peter Mayer, Mattia Mossano, Reyhan Duezguen, Bettina Lofthouse, Tatiana von Landesberger, and Melanie Volkamer. 2020. 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)*. USENIX Association, Berkely, 259–284. https://www.usenix.org/conference/soups2020/presentation/reinheimer

[66] Karen Renaud and Wendy Goucher. 2014. The curious incidence of security breaches by knowledgeable employees and the pivotal role a of security culture. 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*. Springer, Springer, Berlin, 361–372.

[67] Aaron Roberts. 2021. The Cybersecurity Wild West. In *Cyber Threat Intelligence: The No-Nonsense Guide for CISOs and Security Managers*. Springer, Berlin, 1–16.

[68] Puspita Kencana Sari, Nurvita Trianasari, et al. 2014. Information security awareness measurement with confirmatory factor analysis. In *2014 International Symposium on Technology Management and Emerging Technologies*. IEEE, IEEE, New York, 218–223.

[69] Martina Angela Sasse, Sacha Brostoff, and Dirk Weirich. 2001. Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT technology journal* 19, 3 (2001), 122–131.

[70] Bruce Schneier. 2004. *Secrets and lies: Digital security in a networked world.* Wiley, Indianapolis, Ind.
[71] Andreas E Schütz. 2018. Information security awareness: it's time to change minds.
[72] Margaret W Smith. 2019. Information asymmetry meets data security: The lemons market for smartphone apps. *Pol'y Persp.* 26 (2019), 85.
[73] Thomas Sutter, Ahmet Selman Bozkir, Benjamin Gehring, and Peter Berlich. 2022. Avoiding the hook: influential factors of phishing awareness training on click-rates and a data-driven approach to predict email difficulty perception. *IEEE Access* 10 (2022), 100540–100565.
[74] Elinor Tsen, Ryan KL Ko, and Sergeja Slapnicar. 2022. An exploratory study of organizational cyber resilience, its precursors and outcomes. *Journal of Organizational Computing and Electronic Commerce* 32, 2 (2022), 153–174.
[75] U.S. Department of Homeland Security. 2012. The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research.
[76] VMR: Verified Market Research. 2023. Global Security Awareness Training Software Market Size. https://www.verifiedmarketresearch.com/product/security-awareness-training-software-market/
[77] Melanie Volkamer, Martina Angela Sasse, and Franziska Boehm. 2020. Analysing simulated phishing campaigns for staff. In *Computer Security: ESORICS 2020 International Workshops, DETIPS, DeSECSys, MPS, and SPOSE, Guildford, UK, September 17–18, 2020, Revised Selected Papers 25.* Springer, Springer, Berlin, 312–328.
[78] Alma Whitten and J. D. Tygar. 1999. Why Johnny can't encrypt: a usability evaluation of PGP 5.0. In *Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8* (Washington, D.C.) *(SSYM'99).* USENIX Association, USA, 14.
[79] Mark Wilson and Joan Hash. 2003. Building an Information Technology Security Awareness and Training Program. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-50.pdf
[80] Mark Wilson, Joan Hash, et al. 2003. Building an information technology security awareness and training program. *NIST Special publication* 800, 50 (2003), 1–39.
[81] Zuopeng Zhang, Wu He, Wenzhuo Li, and M'Hammed Abdous. 2021. Cybersecurity awareness training programs: a cost–benefit analysis framework. *Industrial Management & Data Systems* 121, 3 (2021), 613–636.
[82] Verena Zimmermann and Karen Renaud. 2019. Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies* 131 (2019), 169–187.
[83] Verena Zimmermann and Karen Renaud. 2021. The nudge puzzle: matching nudge interventions to cybersecurity decisions. *ACM Transactions on Computer-Human Interaction (TOCHI)* 28, 1 (2021), 1–45.

A Online Questionnaire

Landing Page.
Welcome!

Thank you for supporting us in our research on Cybersecurity Awareness & Training!

In the following, we have compiled four questions about security awareness & training in companies. Answering this questionnaire should take a maximum of 5 minutes. You can take part in this survey if you have already had contact with security awareness & training, e. g., because you have already had to develop or assess a training.

We look forward to your answers!

Data Privacy Statement. [...]

Pre-Screening.

(1) Have you already dealt with security awareness, security training, security culture?
  (a) Yes, several times a week
  (b) Yes, several times per month
  (c) Yes, several times per year
  (d) Yes, more than a year ago
  (e) No, not at all so far

(2) What role does security awareness & training play for you? [Multiple answers possible]
  (a) As part of my work I create awareness campaigns or training
  (b) As part of my work I sell awareness campaigns or training
  (c) I am just generally interested in Security Awareness & Training
  (d) Security Awareness & Training were part of my education/studies
  (e) I do research on Security Awareness & Training
  (f) Something else
  (g) Security Awareness & Training does not play a role yet

Scenario.
Here's the scenario:
Imagine you are responsible for Security Awareness & Training in a company. Your bosses have asked you to look for a suitable vendor who sells security awareness & training products so that your security awareness & training can be expanded.
Your task:
What keywords or phrases would you use to search for such a vendor that offers suitable products for you and your company? Each search term can consist of several words.
Name as many search terms or phrases as you can think of.

Vendor Preference.

(1) What would you look for when choosing a security awareness & training provider? [Key points, or complete sentences]

Demographics. Finally, three short questions about you so that we can better classify the survey results.

(1) What do you work, or are you currently studying mainly?
  (a) I work as a Security Awareness Manager
  (b) I work for a security awareness & training provider
  (c) I work as a Security Consultant
  (d) I work in a different role in security
  (e) I work in a different role
  (f) I study IT security or computer science
  (g) I study something else
  (h) I do something completely different
(2) How old are you?
  (a) Younger than 18
  (b) 18-24
  (c) 25-34
  (d) 35-44
  (e) 45-54
  (f) 55-64
  (g) 65-74
  (h) 75-84
  (i) 85 or older
(3) Which gender do you identify with?
  (a) Female
  (b) Male
  (c) Non-binary
  (d) My own identification
  (e) I don't want to answer