Quantifying Security Training in Organizations Through the Analysis of U.S. SEC 10-K Filings

Jonas Hielscher
hielscher@cispa.de
CISPA Helmholtz Center for Information Security
Saarbrücken, Germany

Maximilian Golla
golla@cispa.de
CISPA Helmholtz Center for Information Security
Saarbrücken, Germany

Abstract

The Security Awareness and Training (SAT) market exceeds multiple billion dollars annually, yet reliable data on organizational adoption remains scarce. Conflicting, survey-based figures from cybersecurity vendors leave researchers and decision-makers reliant on questionable insights. A new U.S. Securities and Exchange Commission (SEC) regulation, effective since late 2023, requires companies to disclose cybersecurity strategies in annual *Form 10-K* filings, offering a more consistent data source.

In this study, we crawl and analyze filings from 5,286 U.S. companies across diverse sectors and sizes, using keyword searches and thematic analysis, which offers a lower-bound estimate of prevalent topics. We find that 78% of companies report implementing SAT and 27% conduct phishing simulations, with adoption varying significantly by sector and size. Larger companies report more extensive SAT efforts, often aligned with standards like NIST CSF. While multi-factor authentication (11%) is the most common employee-facing security control, many filings frame employees as a risk factor. Our findings help organizations critically assess SAT strategies and vendor claims, offer actionable insights for policymakers, and equip scholars with a coded dataset and crawling tools for ongoing longitudinal analysis.

CCS Concepts

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

Keywords

Security Awareness, Human-Centered Security, SEC 10-K Filings

ACM Reference Format:
Jonas Hielscher and Maximilian Golla. 2025. Quantifying Security Training in Organizations Through the Analysis of U.S. SEC 10-K Filings. In *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security (CCS '25), October 13–17, 2025, Taipei, Taiwan.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3719027.3765179

1 Introduction

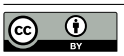
Cybersecurity is notoriously hard to measure [5, 6, 44, 45]. Not only do we have a limited understanding of the prevalence of attacks, but for a multitude of defenses, we do not have sufficient empirical evidence for whether they indeed provide what they promise. Examples include recent doubts about the effectiveness of widespread phishing simulations for employees [51, 63, 64]. It is known that stakeholders in the cybersecurity ecosystem have their own incentives when they decide to share metrics and numbers [4, 7], including public security agencies, police departments, or security vendors. In the context of *Security Awareness and Training (SAT)*, a recent study indicates that claims suggesting *"X% of successful cyberattacks start with humans"* are largely speculative, allowing any arbitrary value of X to be substituted [49].

Without reliable data, the board of directors and Chief Information Security Officers (CISOs) have difficulties determining the right cybersecurity strategy. Despite a growing billion-dollar market for SAT products [104] and numerous scientific publications [23, 28, 57], we know little about the prevalence of SAT in practice.

Although laws and regulations mandate that organizations report incidents and the measures taken to prevent future occurrences (which may include SAT) to security and privacy authorities, the general public has limited access to reports, making it difficult to obtain reliable information on SAT. So far, the "best" quantitative answers often come from cybersecurity vendors and consulting companies, potentially following a marketing agenda [7].

Form 10-K filings, required by the *U.S. Securities and Exchange Commission* (SEC) from companies meeting certain size thresholds (e. g., those with over $10 million in assets [96]), have traditionally served as an overview of corporate financial performance. Starting in December 2023, however, these reports introduced a new cybersecurity section called "Item 1C," requiring companies to disclose their risk management and cybersecurity strategies [94]. This addition reflects the growing impact of cybersecurity on corporate outcomes and the increasing interest from investors in assessing cybersecurity posture. Since Item 1C is a recent requirement, our study is the first to systematically analyze this section, offering a unique opportunity to obtain reliable insights into organizational cybersecurity practices. We hypothesized that the disclosed information might reveal whether organizations deploy SAT and employee-facing security measures (such as virtual private network (VPNs), multi-factor authentication (MFA), or password managers).

For our analysis, we developed a crawling and parsing pipeline to obtain recent Form 10-K filings from the official SEC databases and performed a mixed-method analysis of the reports. For comparison, we also crawled the previous filings that did (most often) not contain the new Item 1C. *Note*: Crawling the database is an explicitly addressed use case and happened in accordance with SEC's "fair access guidelines" [95] (see Section 3.3). We utilized qualitative coding to derive insights that enabled us to search for keywords and make quantifiable statements about the prevalence of SAT and other security measures, along the following research questions:



CCS '25, Taipei, Taiwan

ACM ISBN 979-8-4007-1525-9/2025/10
https://doi.org/10.1145/3719027.3765179

RQ1 *What is the prevalence of SAT deployment across organizations of various sizes* and industries?

RQ2 *What types of SAT programs are most commonly implemented, and how are they integrated with other employee-facing cybersecurity measures?*

RQ3 *How did Item 1C's introduction change the disclosure of human factors-related cybersecurity risks and SAT strategies?*

Findings. Notably, 78.3% of companies reported implementing SAT, with significant differences between sectors and company size. The introduction of Item 1C substantially increased the disclosure of cybersecurity strategies, while the companies' human-related cyber risk disclosure (e. g., social engineering) was already largely present in older filings. We find that the majority of companies remained vague in describing their SAT. In contrast, hundreds of companies still discussed details, e. g., the training topics, or that they would make them mandatory. Employees were primarily portrayed as a source of vulnerability, whether due to error, susceptibility to manipulation, or insider risks.

MFA (11.0%) and reporting procedures of suspicious behavior (7.9%) were the primary employee-facing security measures. Those organizations that use cybersecurity frameworks as guidelines (e. g., NIST CSF [75], 39.9%) were significantly more likely to implement SAT, phishing simulations, and MFA.

Contributions. Our analysis provides a new *ground truth* about companies' SAT strategies. This is the most extensive approach to getting quantitative and qualitative insights into SAT as deployed in U.S. organizations to date. It is also the first time SAT concepts are compared by industry sector and company size on this scale. Our data can inform boards' and CISOs' decisions by providing independent and realistic insights into the state of SAT and employee-facing security. Cybersecurity scholars can use our data and analysis approach to validate the impact of their work on organizational practice and observe long-term trends.

We provide a **replication package** (see Appendix A) containing (i) the links to all analyzed 10-K filings, (ii) the scripts that we used for crawling and data extraction, and (iii) an aggregated matrix with all keyword matches for all analyzed filings to facilitate longitudinal analyses on the topic (see Appendix A for more details). We discuss organizations' incentives for disclosing SAT strategies, the implications on usable security research and policies, and the potential of crawling companies filings for future research. Compared with previous cybersecurity studies with SEC filings (e. g., [30, 107]), our study is the most extensive, including not only larger companies like the S&P 500 (leading companies traded in the U.S.), but all sizes and all industry sectors, and is the first to analyze the newly introduced Item 1C and the first with a focus on SAT. It is also the first study to quantify the prevalence of SAT on the large-scale, beyond one survey conducted in Germany [53].

2 Background and Related Work

Next, we provide an overview of 10-K filings and review prior research related to them, with a focus on cybersecurity, SAT, and employee-facing security. We then identify the existing research gap that our work aims to address.

2.1 Form 10-K Filings and Cybersecurity

The U.S. Securities and Exchange Commission (SEC) requires U.S. companies to file various forms that disclose details about their business operations (in an overview provided by SEC, we counted 393 different types). Companies that meet certain size or public trading criteria are required to file a 10-K, which will then be made available to the general public. This includes most publicly traded companies and those with more than $10 million in assets and a significant number of shareholders [96]. *Note*: There are some rare cases where non-U.S. companies might also need to file a 10-K [99], which we neglect in our analysis. Companies are required to file a 10-K at the end of their fiscal year. The filing has 15 *items* [99] (also called sections) that disclose, for example, current *risk factors* (Item 1A), *financial data* (Item 6), or details about the companies directors (Item 10). Since Dec. 2023, the filing contains a new *Item 1C: Cybersecurity* [94]. While previously, some 10-K companies had already conducted a cyber risk assessment and disclosed it in their 10-K filing, now (almost) all companies are explicitly required to disclose their cybersecurity strategy via the new Item 1C. Regarding SAT, the SEC explicitly states that *"[for the] disclosure of management and staff training on cybersecurity; registrants may choose to make such disclosure voluntarily."* [93]. As companies and their directors are liable if the filings contain incorrect information, Item 1C is a new reliable source for the cybersecurity-related information of thousands of U.S. companies.

2.2 SEC Cybersecurity Research

Information science scholars have utilized 10-K filings before to study cybersecurity risk and disclosure – all before the introduction of Item 1C, e. g., [15, 18, 33, 34, 59, 110]. They often applied some form of qualitative coding strategies. For example, Gao et al. [30] analyzed the 10-K filings from 112 companies over 11 years and found that the cybersecurity risk disclosures got increasingly hard to understand for outsiders. We are not aware of any research that systematically crawled larger numbers of available 10-K filings. The biggest analysis of 10-K was performed by Whitaker et al. [107], who analyzed the cybersecurity risk statements of all Fortune 1000 companies. Among other things, they found that 90% of firms cited hardware/software failure as a major cybersecurity risk.

While no academic research about the new Item 1C is available to date, private consulting and security firms have already looked at it, e. g., where they reviewed all S&P 500 filings and found that 18% of companies disclosed that they have a cyber insurance [86].

2.3 Security Awareness Training

Security Awareness, *Security Training*, and *Security Education* are often used interchangeably. Hence, SAT is an under-defined term, sometimes just describing the presentation of information to increase cybersecurity awareness (commonly to new employees or as part of annual training). Other times it refers to intense hands-on training efforts [37, 48]. Our analysis reveals what activities companies summarize under the umbrella term of SAT. Missing clear definitions of SAT leads to considerable variations in its implementation [48, 49] regarding (i) the activity (newsletter, awareness months, gamification, e-learning, cyber escape rooms, phishing

simulations, hands-on, etc.) [23, 84], (ii) the covered topics (anti-phishing, password policies, social engineering), and (iii) the target groups (all employees, software developers, administrators).

Phishing simulations seem to have become a major component in organizational SAT programs. In such simulations, employees receive deceptive emails from their employer (or an external SAT vendor, providing companies with a phishing simulation platform), and their interaction with the emails (clicking, reporting) is measured. While there has been growing interest among scholars in understanding the mechanisms behind the simulations [28, 35, 78, 79, 81, 108] the three most extensive studies (all with more then 10,000 participants) concluded that there is no positive effect of those simulations on employees anti-phishing behavior [51, 63, 64]. Hence, phishing simulations are a good example of where SAT practice diverges from its tangible effects.

Quantifying SAT. There is limited research on SAT and its prevalence. Huaman et al. [53] performed telephone-assisted interviews with 5,000 small and medium-sized companies in Germany in 2021. One of their questions was built around "information security training," and 61% of companies reported deploying such.

In a survey with 1,000 organizations in 2020, the *German Federal Office for Information Security (BSI)* found that 80–90% of organizations deployed some form of "security awareness" [77]. NIST found that 85% of U.S. federal government agencies deploy phishing simulations [41], by surveying 96 federal cybersecurity employees. A 2017 survey with 1,505 small German enterprises found that less than 60% deploy SAT [50]. Surveys and reports from vendors and consulting firms should be approached with caution when considering their reliability. For instance, in 2022, the SAT vendor ThriveDX reported that 88% of 1,900 IT security professionals surveyed had implemented SAT and phishing simulations [88]. However, the reliability of this claim is undermined by the fact that 89% were existing customers, introducing a substantial bias.

2.4 Employee-Facing Security

Beyond SAT, organizations deploy various security measures that directly affect employees – which we refer to as *employee-facing security*. These could be organizational measures, such as the implementation of password policies [8, 31, 38, 73] or incident reporting structures [24], but also password managers [26], VPNs [87], email encryption [56], single sign-on (SSO) [87], or passkeys [65]. As with SAT, there is no definite list of what such measures should include. Frameworks, such as NIST CSF [75] remain vague when describing appropriate measures. Due to this poor overview of employee-facing security, our qualitative analysis was performed openly for any measure that might be visible to employees. There have been a variety of surveys with employees about their perception of security measures, e. g., around password policies [31, 38, 61] and also studies that aimed to quantify employee-facing security among companies, e. g., a long-term study by Gerlitz et al. [32] with 80 companies about their password expiration policy.

2.5 Research Gap

In quantifying SAT, the studies closest to ours were conducted by Huaman et al. [53] and the German BSI [77]. Both studies were based on surveys in Germany without focusing on SAT: the prevalence of SAT was measured in only one question. While surveys with company representatives might also deliver insights into companies' SAT strategies, 10-K filings have the advantage that they are legal documents that companies need to fill and where it is unlikely that false information will be presented, as those could cause existential fines. Hence, their analysis offers a reliable method to collect information about SAT that can be reproduced and does not require active participation from company representatives. Previous studies with SEC filings focused on the largest companies, such as Fortune 1000 [107] and on general risk disclosure, where we include all companies and quantify SAT.

3 Method

We crawled recent SEC 10-K filings containing "Item 1C: Cybersecurity" to enable a mixed-method analysis of the prevalence of SAT and employee-facing security across 5,286 U.S. companies. Figure 1 summarizes our method.

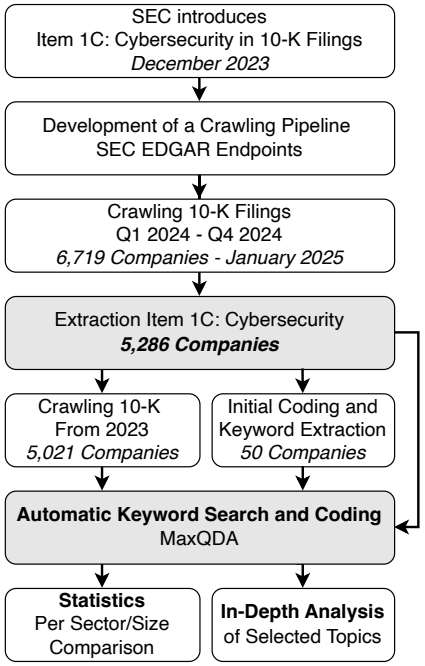


Figure 1: Workflow: Download, Item 1C extraction, coding, keyword search, statistics, and qualitative analysis.

3.1 Data Crawling

SEC generally allows crawling their websites and databases [95]. However, they limit the requests to 10 per second and state they would not provide technical support with crawlers. While 10-K filings are, in theory, publicly available on the SEC website from their EDGAR database [97], it is not possible to iterate over all 10-K reports. Likewise, a publicly available list with all exchange-listed companies does not offer a connection to the filings. Hence, we developed a multi-stage crawling process, combining different resources published by SEC to identify, locate, download, and then

convert large sets of recently published 10-K filings. Figure 1 in our replication package (see Appendix A) summarizes our crawling pipeline. The crawling provided us with the 10-K filings in a text format. Every file was named after the corresponding Central Index Key (CIK): a number up to 10 digits long that uniquely identifies each company listed by SEC.

Item 1C Extraction. The filings' HTML and plaintext versions are unstructured, with no hierarchy between elements. This issue is rooted in the legacy structure of the website, which follows the eXtensible Business Reporting Language (XBRL) [112], a standard developed over 20 years ago based on XML. As a result, sections (items) are not clearly distinguishable from surrounding text using familiar HTML-style tags or identifiers.

Additionally, as humans write the reports, they include typos and mistakes that complicate the automated parsing process, such as missing sections, missing punctuation, confusing the letter 'l' with the digit '1,' differing white space characters, differing capitalizations, singular/plural, and encoding problems. Thus, to extract Item 1C for more analysis, we used a custom regex parser written in Python, which we fine-tuned by hand over several rounds. The parser's underlying idea was to identify the items that typically come before and after Item 1C by their various names and then extract the content between those items. We provide the parser in the replication package, see Appendix A. In the following simple example the parser extracted all text before Item 2 began:

```
<div><span>Item 1C. Cybersecurity</span></div>
<div><span>Some text ...</span></div>
<div><span>Item 2. Properties</span></div>
```

The parser extracted > 99% of all Item 1C successfully (which we confirmed by manually reviewing outliers in terms of word count and file size), whereas the remaining 25 items had to be extracted manually by a member of our research team.

3.2 Analysis

The goal of this step was to obtain information stored in the unstructured text of the 10-K filing. After an initial manual inspection of some reports, we learned that a simple word analysis would be feasible due to their technical nature. For example, we could quickly identify all sentences making statements around SAT as soon as we had a list of words that identified SAT (such as, "training," "awareness," "communication," etc.). As prior work [58] highlights the importance of a case-by-case evaluation when deciding on a qualitative analysis, we initially considered relying on a large language model (LLM) for analysis. However, as we aimed for exact and reproducible results, and an initial review of the filings indicated the usage of rather straightforward terminology around SAT, we opted for the time-consuming but more exact manual analysis approach. Consequently, we chose to use MAXQDA 24 [101] for traditional qualitative coding of the filings. Our goal with the coding was not to build a new theory but to structure the data, derive key insights, and create a list of keywords that would enable us to perform statistical analysis. To analyze our insights, we used the MAXQDA complex keyword search [103], auto-coding, and code-relation browser features, among others (note that we did not use MAXQDA's AI features, as they were still experimental).

Keyword Extraction. Figure 2 summarizes the keyword creation and extraction process. In the first step, we **qualitatively coded the filings** of 50 random S&P 500 companies (10% of S&P 500) to generate an initial set of keywords (1). We opted for this approach, as we suspected that larger companies would disclose more about their cybersecurity strategy. We used those codes as the foundation for automated keyword searches across all Item 1C sections. A keyword could, for example, be "phishing training." Multiple keywords formed a concept, e. g., "phishing simulations" were identified by phishing test/training/simulation/[...]. We combined keywords to **full keyword queries** that we could utilize in the MAXQDA complex keyword search feature (2). The creation and improvement of those queries were performed iteratively. The search query results were then used to **auto-code** all identified segments (3). After every search, we **manually inspected** at least 50 of the segments (sentences or paragraphs) (4). We then excluded words that should not occur with a search query (see query below as an example). We repeated this cycle until we could not identify any false positives, e. g., did we have to exclude *CISO education* from the query for employees security education. While there is a chance of false-negatives (missed concepts/keywords), the combination of the initial coding of 50 filing, with the repeated improvement and adoption of keywords, makes this unlikely.

Additionally, we reduced complex terms, e. g., the *General Data Protection Regulation* never occur without its abbreviation *GDPR*, so the final search term could be reduced. Below, one can find an example of a keyword query for the concept of internal communication of security topics towards the employees (see Table 1 in our replication package for the final set, available in Appendix A).

```
(ALL communication
 ANY training, awareness, education
 NOT ANY board, executive, chief, committee, ciso,
 'corporate communication', telecommunication)
 WITHIN ONE SENTENCE
```

In cases where we could not eliminate the false positives, we discarded the keyword (e. g., "*audit*," as it referred to committees and audit processes unrelated to employee-facing security). The keyword query creation process had no stopping criteria. This means that whenever we found **new keywords** for an already coded concept, we would redefine the search query and rerun the search, coding, and manual inspection check (5).

Comparing Item 1C with Full Filings. In our analysis of Item 1C, we developed a set of search queries. To address RQ3 (i. e., comparisons with the full filing and previous years), we applied most of these queries to the remainder of the filing beyond Item 1C. Additionally, we crawled the 2023 filings for all companies. Some of these queries were adjusted slightly to accommodate the broader context of the filings; for instance, the term "*onboarding*" was modified to include "*AND security*" to exclude references to onboarding trainings in non-security-related items.

Qualitative Coding. For a deeper qualitative analysis, we followed the thematic analysis approach of Kuckartz [62], utilizing an inductive approach. A single, experienced coder performed the coding, while the findings were discussed within the larger research team. Since the content was well structured, e. g., compared with

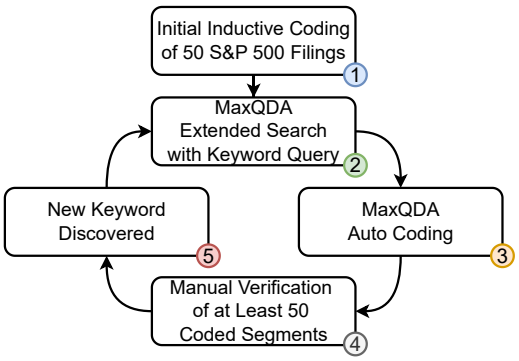


Figure 2: Our recursive keyword query creation pipeline.

interviews, we determined that one coder was sufficient to identify relevant topics. The coding process was entirely inductive and integrated into the keyword query process: during the manual verification process, codes and memos were created around the topic. The coding allowed us to identify, e. g., how the concept "*password*" was sometimes referred to as a training topic, regarding a policy, or as a part of technology like a password manager. The list of keyword queries (see Table 1 in our replication package, available in Appendix A) contains all codes and concepts that occurred during the analysis process.

Quantification. We used MAXQDA's Code Matrix Browser [102] to create a CSV export of all coded segments per filing. The exported matrix table formed the basis for all quantified statements and the statistics. Hence, our quantification is based on our keyword coding.

Data Enrichment: Industry Sector. We furthermore sought to compare SAT and employee-facing security across different industry sectors. The SEC assigns each company to one of 444 industry sectors using the U.S. Standard Industrial Classification (SIC) system. Furthermore, SEC provides a mapping of SIC codes to specific offices, which is available on their website [100]. Each SIC code is associated with one of ten offices, such as the "Office of Manufacturing" or the "Office of Life Sciences." This mapping informed our analysis by grouping companies based on their assigned offices. We merged the "Office of Finance," the "Office of Structured Finance," and the "Office of Crypto Assets," as those all represent the broader finance sector, ending up with a total of eight sectors.

Data Enrichment: Financial Data. We also aimed to classify companies by *size*, which was a challenging task given the variety in our sample of over 5,000 companies. To do this, we needed a consistent and widely available metric. However, for example, the *number of employees* is not reported in a structured way in SEC filings. *Market capitalization*, another common measure, fluctuates daily and is not included in SEC filings either. Instead, we chose to use *total assets* [92] as a proxy for company size. This value is reported annually by most companies in a structured format to the SEC and it reflects their overall financial standing in terms of U.S. dollars. Importantly, the SEC itself uses total assets as an eligibility criterion for regulatory requirements, and it allows for comparisons across companies and sectors, which is critical given the breadth of our dataset. We applied a market capitalization scale [27, 83] to group companies into six size categories, ranging from micro to mega corporations (see Table 1). This size-based analysis offers a new perspective, as earlier studies mostly focused on the largest companies (e. g., S&P 500) without further breakdown (see Section 2.2).

Table 1: We categorized companies into six groups.

Description	Total Assets (U.S. Dollar)	#[1]	%
Micro	<100 Million	1,340	25.3
Small	100 Million - 500 Million	837	15.8
Mid-	500 Million - 2 Billion	1,002	19.0
Mid+	2 Billion - 10 Billion	1,098	20.1
Large	10 Billion - 100 Billion	661	12.5
Mega	>100 Billion	111	2.1

[1] For 237 companies (4.5%), no total assets value was reported to the SEC.

Correlation Tests. Our analysis provided a matrix containing binary information (*true*/*false*) for all concepts identified for all filings. Additionally, every filing was mapped to one of eight industry sectors and six size categories. Based on this matrix, we performed correlation tests. We aimed to test the correlation between different concepts (e. g., to validate whether cybersecurity frameworks like NIST CSF could be a predictor for SAT). As all data points were nominal, we employed the Chi-squared test of independence [66]. For significant results (p-value < 0.05), we calculated Cramér's V [20] to measure the strength of the association, which is interpreted as *weak* (V < 0.1), *moderate* (0.1 ≤ V < 0.3), *strong* (0.3 ≤ V < 0.5), or *very strong* (V ≥ 0.5) [19]. Cramér's V presents a scaled version of the Chi-squared test, which facilitates more meaningful comparisons of effect sizes across analyses. This strength validation was necessary as $n = 5,286$ was quite large, and hence, we expected many significant correlations but with limited effect sizes. The data preprocessing and statistical analysis were performed in Python using the data analysis libraries pandas and SciPy.

3.3 Ethics Considerations

The ethics committees at CISPA's partner universities review and provide feedback exclusively on ethical aspects of research projects involving human subjects and/or personal data. While our project did not fall under these categories, we adhered to key principles outlined in the Menlo Report [91]. This included conducting a thorough risk-benefit analysis and collaborating with peers experienced in crawling and analyzing cybersecurity datasets to ensure the project followed ethical research standards.

We accessed the SEC database in accordance with their "fair access guidelines" [95], which state: "*Please use efficient scripting, downloading only what you need, and moderate requests to minimize server load. Current guidelines limit each user to a total of no more than 10 requests per second, regardless of the number of machines used to submit requests.*" To ensure compliance, we implemented a rate-limiting mechanism in our scripts and utilized Selenium with authentic HTTP headers to reflect our research setup.

Our research relies exclusively on publicly available data and does not disclose information that is not already in the public domain. Since no vulnerabilities are revealed, we have identified no risks posed to organizations or individuals as a result of this work.

Item 1C. CYBERSECURITY

Cybersecurity Strategy and Risk Management

The [redacted] comprehensive cybersecurity program is supported by policies and procedures designed to protect our systems and operations as well as the sensitive personal information and data of our clients and customers from foreseeable cybersecurity threats. This program is an integral component of our enterprise risk management program.

Core to our security model is our defense-in-depth framework, comprising multiple layers of processes and technologies that help prevent, detect, and respond to threats. Our approach to safeguarding against external threats incorporates a suite of preventive technologies, including malicious email blocking, defenses against automated attacks and multifactor authentication. These strategies act to proactively intercept and neutralize cyber threats to help ensure data remains secure within our environment. Event monitoring technologies run continuously, detecting suspected intrusion attempts and alerting our Cybersecurity Incident Response team. [Redacted] undertakes a number of critical security processes to mitigate and protect against cybersecurity risks, which include but are not limited to:

• **Identity and Access Management**. Employees are provided with the minimum amount of access required to perform their jobs using role-based access control methodology, which defines access to our information systems based on job function. Privileged or elevated access to our systems is subject to supplemental approval requirements, increased authentication processes, and additional logging and monitoring.

• **Security Awareness and Training**. Events and education activities are hosted throughout the year, such as the Cybersecurity Awareness Month, expos, videos, training programs and frequent phishing simulations. [Redacted] continuously trains workforce members on the importance of preserving the confidentiality and integrity of customer data.
All new hires have mandatory information protection and privacy training as part of their onboarding, and all workforce members complete an annual cybersecurity refresh training.

• ...

Figure 3: An exemplary excerpt of a Form 10-K Item 1C, which discloses SAT and authentication strategies.

To avoid shifting any direct blame or praise on single companies, we decided against linking the quotes from the 10-K filings to the companies' names in the presentation of our results. Furthermore, our research and measurements are intended to provide valuable contributions to the research community and industry by offering reliable insights into organizational cybersecurity practices.

3.4 Limitations

The analysis focuses exclusively on U.S. companies, as only these entities file 10-K reports. Additionally, the study is limited to publicly traded companies, excluding public agencies and non-traded entities. Nevertheless, we think our sample provides a representative cross-section across industry sectors and sizes, encompassing companies with revenues ranging from millions of dollars to some of the largest corporations in the world, such as Apple Inc.

While companies are now required to disclose their cybersecurity strategies in the 10-K, they are not explicitly mandated to include details about SAT or employee-facing security practices. Some companies may implement measures without reporting them, so our numbers represent a lower bound and should be interpreted accordingly.

Although we manually verified sample codings in our automated keyword strategy (see Section 3.2), minor inaccuracies may persist. For instance, mentions of multi-factor authentication in filings could, in some cases, refer to end-user MFA rather than employee MFA. Conversely, specific keywords describing relevant concepts may not have been identified. However, given the large sample size of more than 5,000 filings, such errors would have a negligible impact on the overall percentages and, consequently, on our conclusions.

The filings vary in style and detail, and authorship cannot be determined. While some boilerplate exists, the most significant identified text cluster involved 35 filings (see Section 4.8).

Finally, our keyword queries for the entire filings were intentionally more restrictive than those used for Item 1C to minimize errors (see Table 1 in our replication package, available in Appendix A). As a result, there were instances where concepts identified in Item 1C were not detected across the broader filings. For example, in the case of "*reporting functions*," we were unable to formulate a broader query without false positives. Despite these limitations, we are confident that our findings and conclusions remain robust and meaningful.

4 Results

Next, we present the results of our analysis, comparing new 10-K filings with Item 1C to older ones. Where relevant, we link our findings to prior work. Table 2 summarizes key quantitative findings, focusing on the most relevant correlations with moderate or strong effect sizes. All reported correlations (except those in Table 2 and 3) have $p < .001$, so we only report V (the effect size). In the tables, we denote the significance levels with asterisks. A full list of significant correlations is included in our replication package (see Appendix A).

4.1 Dataset

On January 2nd, 2025, we collected all available 10-K filings from the last four quarters. Because the SEC organizes its filings database by calendar quarters, our **2024 dataset** includes all 10-K filings submitted between January 1st and December 31st, 2024. Since companies have varying fiscal year-end dates, these filings do not necessarily correspond exactly to the 2024 calendar year. This crawling provided us with 6,719 filings. 455 filings had no Item 1C, 678 stated that

Table 2: An overview of our results with the most prevalent topics identified.

Content	Item 1C Only 2024[2]									Full 10-K		Effect Size
Year										2024	2023	
	All (C_{24})	Energy & Transportation	Finance	Industry	Life Science	Manufacturing	Real Estate & Construction	Technology	Trade & Service	**All** (F_{24})	**All** (F_{23})	**All** (C_{24})
n	**5,286**	546	767	565	728	705	548	605	671	**5,286**	**5,021**	
Awareness Training (SAT)	76.9%	80.6%	85.3%	73.6%	72.3%	78.0%	69.9%	78.8%	78.7%	78.3%	23.6%	$p < .001, V = .123$
Phishing Simulation	24.4%	22.3%	30.5%	22.8	19.0%	28.2%	27.0%	20.3%	24.1%	26.5%	1.6%	$p < .001, V = .080$
Annual SAT	23.2%	22.0%	32.7%	23.7%	12.4%	22.8%	23.5%	25.5%	22.2%	23.2%	2.4%	$p < .001, V = .125$
Mandatory SAT	12.1%	15.2%	15.6%	11.5%	7.6%	9.9%	13.9%	13.7%	11.6%	12.1%	1.1%	$p < .001, V = .074$
Onboarding	5.3%	2.2%	6.6%	6.0%	4.7%	3.3%	7.5%	6.0%	5.5%	5.3%	0.1%	$p < .001, V = .063$
Tabletop (Management)	21.1%	20.3%	26.1%	17.0%	10.9%	23.0%	19.7%	25.8%	25.5%	22.4%	0.6%	$p < .001, V = .118$
MFA	10.2%	11.9%	11.0%	10.4%	7.4%	11.9%	9.3%	9.1%	11.0%	11.0%	2.1%	No correlation
Reporting Functions	7.9%	7.9%	9.4%	7.8%	8.0%	7.9%	7.1%	6.9%	7.3%	N/A[3]	N/A	No correlation
Passwords	4.8%	5.3%	3.8%	5.5%	6.7%	3.8%	5.8%	4.1%	3.9%	12.6%	7.8%	No correlation
Social Engineering	6.4%	4.0%	9.3%	6.0%	7.3%	6.7%	6.6%	5.1%	5.7%	32.8%	20.1%	$p = .004, V = .080$
Malware	15.2%	15.4%	13.7%	17.9%	13.2%	14.8%	19.3%	13.4%	14.0%	51.7%	30.2%	$p = .011, V = .047$
Cyber Insurance	24.7%	24.7%	24.3%	23.7%	27.7%	25.7%	22.4%	25.6%	27.7%	48.0%	32.4%	$p < .001, V = .085$
NIST CSF	39.9%	50.2%	43.7%	40.7%	25.7%	43.3%	36.7%	41.2%	41.3%	39.9%	2.0%	$p < .001, V = .131$
ISO 27001	7.9%	4.9%	5.6%	8.8%	2.3%	7.0%	4.0%	19.5%	11.8%	7.9%	1.5%	$p < .001, V = .182$

[2] In total, 151 companies (2.9%) were not assigned to any sector.

[3] We report "N/A" as we were unable create a keyword query for "Reporting Functions" for the full 10-K filing with a sufficiently low false-positive rate.

they omitted Item 1C, and 294 companies just stated that Item 1C did not apply to them, e. g., *"Our sole business activity has been identifying and evaluating suitable acquisition transaction candidates. Therefore, we do not consider that we face significant cybersecurity risk and have not adopted any cybersecurity risk management program."* This left us with **n=5,286** filings. **5,021** of those companies also filed a 10-K in **2023**, which we also crawled and analyzed, even though almost all of them did not include a dedicated Item 1C, as the new SEC regulation only became effective on December 15th, 2023. Figure 3 is an excerpt of an Item 1C, where information about Identity & Access Management (IAM) and SAT are disclosed. On average an **Item 1C contained 731 words** ($median = 695$, $min = 95$, $max = 8,107$), and the **full 10-K filings contained 65,431 words** ($median = 62,179$, $min = 4,413$, $max = 292,584$).

We denote three different types of quantitative results: (i) C_{24} for all numbers extracted from Item 1C from 2024, (ii) F_{24} for all numbers from the full 10-K filing 2024 (note that those full filings include Item 1C), and (iii) F_{23} for the full 10-K filing from 2023.

4.2 Cybersecurity Threats

The companies disclosed various threats related to the behavior of their employees: F_{24}=58.7% wrote about **phishing** attacks and F_{24}=32.8% about **social engineering**, e. g., *"Remote working environments may be less secure and more susceptible to hacking attacks, including phishing and social engineering attempts that seek to exploit events."* For comparison, F_{24}=51.7% wrote about **malware**. No company wrote about *vishing*, but F_{24}=0.5% about *smishing*.

The filings portrayed the companies' employees as a liability or risk. F_{24}=37% reported **employees' error as a potential threat**: *"Threats may result from human error, fraud or malice on the part of employees or third parties."* Additionally, F_{24}=9.1% wrote about their employees as potential insiders: *"[We maintain] an insider threat program to detect, investigate and mitigate insider threat risks to [our] assets, data, services and personnel globally."* C_{24}=0.7% called employees a "first line of defense": *"Our employees represent the foundation of cybersecurity protection and are a key line of defense, and we seek to strengthen their ability to target risks by proactively training active employees and contractors each year."*

The threat of social engineering correlated significantly with SAT with a moderate effect size ($V = .119$), as did phishing simulations ($V = .177$). The phishing threat correlated significantly with phishing simulations, with a moderate effect size ($V = .127$).

Summary: Employees Seen as Cyber Risk

C_{24}=64.5% of companies report at least one cyber threat directly linked to employees' behavior. Employees are primarily portrayed as a source of vulnerability, whether due to error, susceptibility to manipulation, or insider risks.

4.3 Security Awareness and Training

C_{24}=76.9% and F_{24}=78.3% reported deploying some form of **SAT**, e. g., *"Mindful that human error can be a significant factor in cybersecurity incidents, our employees undergo regular training to stay informed about the latest threats and best practices."* *Real Estate*

& Construction companies reported the lowest implementation rate (C_{24}=69.9%) and *Finance* the highest (C_{24}=85.3%). We also got some insight into the **frequency of SAT**, with C_{24}=23.2% conducting them annually, C_{24}=3.8% quarterly, C_{24}=2.4% monthly, and C_{24}=21.2% "regularly." C_{24}=12.1% made SAT mandatory for their employees and C_{24}=5.3% rolled-out SAT during the employee **onboarding process**. C_{24}=3.0% reported that SAT would be delivered by a **third-party provider** (SAT vendor [49]): *"Cybersecurity awareness training of our employees, incident response personnel and senior management, including through the use of third-party providers for regular mandatory trainings."* The correlation between sector and SAT was significant, with a moderate effect size (V = .123).

Types of SAT. **Phishing simulations** were the primary reported activity (C_{24}=24.4%, F_{24}=26.5%): *"All employees and contractors are required to participate in the ethical cyber phishing campaign program."* Again, *Finance* companies lead the charts (C_{24}=30.5%), and *Life Sciences* were in the last place (C_{24}=19.0%). In addition to SAT for employees, C_{24}=21.1% of companies explained that their board of directors would conduct cybersecurity **tabletop exercises** (at least once per year) to prepare the management team for cybersecurity incidents, which significantly correlated with sector (V = .118): *"The cybersecurity, legal, and executive leadership teams also participated in a data security incident tabletop exercise in Dec. 2023 to simulate responses to a ransomware attack and use the findings to improve the company's processes and technologies."*

Besides those, most companies stayed abstract in describing activities, just citing "**employee training**" or "training and awareness." An exemplary exception: *"In addition to online training, employees are provided with cybersecurity-related information through several different methods, including event-triggered awareness campaigns, recognition programs, security presentations, intranet articles, videos, system-generated communications, email publications, and various simulation exercises."* C_{24}=4.6% wrote about **internal communication** about cybersecurity risks towards their employees, C_{24}=0.5% reported conducting an "Awareness Month" and C_{24}=0.8% to send out cybersecurity newsletters to their employees, e. g., *"Employees also receive periodic cybersecurity awareness messages and each October, in recognition of Cybersecurity Awareness Month, are invited to presentations throughout the month from internal and external cyber experts covering diverse cyber topics."*

Training Topics. C_{24}=20.0% of companies got into the details about training topics, e. g., *"[...] trainings on the following topics: the company's information security policy; information security incident response plan; HIPAA, PCI compliance; GDPR and CCPA; [...] Social engineering (identification and common red flags), social media safety best practices, internet security best practices, and incident response training for end-users; and phishing."* Among the most prevalent training topics where (i) attacks, such as social engineering (C_{24}=4.1%), or insider threats (C_{24}=1.1%), (ii) defenses such as data privacy procedures (C_{24}=7.8%), or mobile device security (C_{24}=1.4%), (iii) and concrete behavior suggestions such as incident reporting (C_{24}=5.5%), or password usage (C_{24}=2.1%).

Success of SAT. C_{24}=16.8% companies reported testing their employees with SATs, e. g., *"Employees and contractors are evaluated for timely completion of the trainings, on corresponding quiz scores, and based on how they fare tackling mock phishing emails."* C_{24}=0.7% explicitly stated that employees **who failed** phishing simulations or tests would have to **take extra security training**, e. g., *"Any failures trigger a retraining exercise if not properly reported and a monthly training vignette on cybersecurity awareness."*

Target Groups. C_{24}=11.3% of companies reported that they would deploy SAT for "**all employees**," C_{24}=1.6% wrote about SAT for their "**workforce**." C_{24}=5.1% required SAT for their contractors and C_{24}=1.1% for their part-time and temporary employees: *"We ensure that all employees, including part-time and temporary employees, undergo cybersecurity training and compliance programs at least annually."* C_{24}=2.4% stated that they would offer "**specialized**" training, depending on the job role: *"Personnel with significant security responsibilities receive specialized education and training on their roles and responsibilities prior to being granted access to systems and resources."* C_{24}=0.5% specified that they had SAT in place for their **software developers**: *"Employees whose work is more pertinent to cybersecurity management and risk, such as software development, receive additional and more specialized training."*

Summary: Training Widespread

The vast majority of companies implement SAT, with significant differences between sectors. While phishing simulations are the most prevalent form of SAT, less than C_{24}=24.4% reported using them. Few companies disclosed their training topics, which consist of attacks, defenses, and desired employee behavior.

4.4 Employee-Facing Security Mechanisms

Beyond SAT, we got insights into what types of employee-facing security mechanisms companies deploy. C_{24}=10.2% of companies report requiring **MFA**: *"[The company] and the Registrant Subsidiaries maintain access-management controls, including a layered multi-factor authentication process for network and system access."* C_{24}=7.9% wrote that they would provide their employees with ways to **report suspicious activities**: *"Our awareness training provides clear reporting and escalation processes in the event of suspicious activity."* This was often presented as a form of mandatory duty for employees: *"[...] educate employees about cybersecurity threats and help them understand their responsibility in identifying, mitigating, and reporting security concerns or threats."* C_{24}=6.1% reported having an **Identity and Access Management (IAM)** system in place. Here, the companies often got more specific about how they handled access to their systems, e. g., *"The company's identity and access management systems are integrated with human resource applications and processes to facilitate provisioning and de-provisioning of badges and logical system access."* C_{24}=7.0% companies wrote about a **cybersecurity culture**, with little detail on what that means, beyond *"fostering a corporate culture that prioritizes cybersecurity at all levels."* Within this context, 12 companies wrote about "*Security Champion Programs*" [13, 14, 29, 70]: *"We designate certain employees as security champions throughout [company name] to respond to cybersecurity incidents in accordance with our incident response plan."* C_{24}=17.9% reported having **security policies** for their employees in place: *"Our policies require each of our employees to contribute to our data security efforts."* *Note*: We filtered for policies explicitly

mentioning employees, while C_{24}=73.2% generally reported having policies in place. Beyond MFA and password managers (see below), the only other security-related tool employees could use were **VPNs** for remote work, which C_{24}=1.0% wrote about: *"We introduced always-on VPN in an effort to better restrict off-campus network access in light of the increase in the number of our employees working remotely."* C_{24}=0.6% wrote about Single-Sign-On (SSO): *"Access control is tightly managed with single sign-on, MFA, and sensitive data access limited by least-privilege authorization appropriate for job duties and reviewed quarterly."* Only two companies wrote anything related to **usable security principles**, namely that they implemented *"a user-friendly phishing reporting tool in Outlook"* for their employees.

Passwords. C_{24}=4.8% wrote about passwords. Looking at the whole 10-K, F_{24}=12.6% mentioned passwords, the discrepancy mainly being that the risk of *password theft* and credential compromise was explained outside Item 1C: *"[We] detected a compromise of two unique passwords used to access [our] customers' information."* C_{24}=2.1% wrote about passwords as a training topic. In all other cases, the companies stated they would have certain **password requirements** or policies in place. Only a few companies got into more detail about their password policies, e. g., *"Passwords must be changed upon first logon and all privileged account passwords (e. g., root, super user, [...]) must follow our password guidelines."* C_{24}=0.3% explicitly stated that they would enforce **password change policies**: *"All desktop and laptop computers must be password protected and must be changed every 90 days."* Only one company wrote about **FIDO**, but more likely in the context of their products: *"Some of our products are certified under specific technical standards or guidelines, such as FIPS 140-2 and FIDO."* Eight reported utilizing **password managers**: *"One threat was identified: insecurely stored credentials. This was responded to by implementing an encrypted password manager company-wide."*

Correlation. Implementing MFA was significantly correlated with phishing simulations with a moderate effect size (V = .149), as were passwords with phishing (V = .136). The threat of social engineering was significantly correlated with passwords (V = .225).

Summary: Employee-Facing Security Rarely Disclosed

The minority of filings discuss employee-facing security tools and tasks. Those that do assign employees responsibility for the organization's defense. MFA and incident reporting functionalities are the primarily reported tools, provided to employees.

4.5 Regulations and Frameworks

As regulations heavily influence the SAT strategy of companies [43, 47, 49], we also collected information about the cybersecurity regulations and frameworks companies reported to implement [106]. Companies often reported cybersecurity regulations outside of Item 1C, so here we report the F_{24} numbers.

The most commonly referred cybersecurity compliance framework cited was **NIST CSF** with F_{24}=39.9%. However, only for some companies was it clear that they implemented all aspects of the framework. F_{24}=4.6% reported to have been certified under SOC 2 [3], and F_{24}=7.9% under **ISO 27001** [55], e. g., *"With regard to cybersecurity, we regularly provide training, [...] in compliance with our ISO 27001 certifications and best practices." Note*: Some companies stated that they would not fully comply with the new ISO 27001:2022 standard and hence it remains vague whether they are currently certified. F_{24}=8.0% reported that they might fail to comply with the *Payment Card Industry Data Security Standard* (*PCI DSS*), e. g., *"Compliance with the PCI DSS may not prevent all security incidents [...] our failure to comply with these payment card industry rules [...] could adversely impact our business."*

The EU **GDPR** occurred in F_{24}=30.8% of reports, but in most cases rather as a risk than as a standard the companies implement, e. g., *"In particular, serious breaches of the GDPR can result in administrative fines of up to 4% of annual worldwide revenues."* F_{24}=28.1% reported the same threat through the **CCPA** (California Consumer Privacy Act) [17], where our quantitative results confirm previous qualitative work that found that CCPA and GDPR were perceived as threats [59, 110]. Additionally, F_{24}=48% reported having a **cyber insurance** or were planning to obtain one: *"We maintain a cybersecurity insurance and have retained relevant incident response services." Note*: In some cases, companies wrote that they would be insured for cyber threats, but were uncertain how much damage would be covered in case of an incident. Hence, this large number of almost 50% might need further in-depth investigation.

Correlation. NIST CSF correlated with mandatory SAT (V = .154), annual SAT (V = .164), quarterly SAT (V = .109), SAT in general (V = .243), phishing simulations (V = .184) and tabletop exercises for management (V = .215). Having cyber insurance significantly correlated with SAT (V = .164) and phishing simulations (V = .142).

Summary: NIST CSF and Cyber Insurance Linked to SAT

Companies that implement NIST CSF or hold cyber insurance are significantly more likely to adopt SAT and phishing simulations.

4.6 Small vs. Large Cooperations

One can observe a pattern that the bigger the company, the more likely it is to implement various forms of SAT – except mega-sized companies, which were often slightly below the large-sized ones. For example, only C_{24}=52.8% of micro-sized companies reported SAT, vs. C_{24}=89.3% of large companies. Similarly, C_{24}=11.5% of micro-sized companies implemented phishing simulations, vs. C_{24}=33.3% of large companies. There was also a steep increase in companies having cyber insurance in place (C_{24}=16.3% micro-sized vs. C_{24}=30.0% large), following NIST CSF (C_{24}=16.6% micro-sized vs. C_{24}=60.1% large) or being ISO 27001 certified (C_{24}=2.1% micro-sized vs. C_{24}=12.1% large). Notable exceptions to this rule were passwords, which C_{24}=5.8% of micro-sized, C_{24}=4.5% of small, but only C_{24}=3.8% of large companies reported about, and also MFA (C_{24}=9.1% micro-sized vs. C_{24}=7.8% large). Table 3 compares key concepts and outlines this trend visually.

Following NIST CSF correlated significantly with company size with a strong effect size (V = .328), as did SAT (V = .324). Significant correlations with moderate effect size with company size were, phishing simulations (V = .328), IAM (V = .113), cyber insurance (V = .123), and tabletop exercises (V = .268), among others.

Summary: Security Practices Scale with Size

Larger companies are more likely to adopt SAT, phishing tests, NIST CSF, and cyber insurance, among other best practices.

4.7 Changes Through Introducing Item 1C

The introduction of Item 1C significantly changed the amount of details companies disclose about their cybersecurity strategies. We found that only with the introduction of Item 1C one could extract **meaningful information about SAT** and employee-facing security from the filings. For example, in 2023, only F_{23}=23.6% of companies reported implementing SAT, vs. F_{24}=78.3% in 2024. It remains unclear whether this difference stems from the increase in SAT adoption, or from introducing the new mandatory item. Likewise, minimal details were disclosed about SAT, such as that only F_{23}=0.1% reported having SAT during onboarding, compared with F_{24}=5.3%. Regarding employee-facing security, for example, only F_{23}=8.1% wrote about employee policies, compared with C_{24}=17.9%. Additionally, technical employee-facing security measures were almost entirely absent in 2023, such as MFA (F_{23}=2.1%) and only showed up within Item 1C in 2024 (F_{24}=11.0%). The same goes for tabletop training for the board of directors (F_{23}=0.6% vs. F_{24}=21.1%) and SAT details like the frequency (F_{23}=2.4% vs. F_{23}=23.2%). The few companies that went into details in 2023 about their SAT strategy and employee-facing security did so under *Item 1A Risk Factors*. We also found some indication they did so because they had to comply with sector-specific regulations, e. g., *"The regulations require [...] use of multi-factor authentication."* In other cases, SAT just occurred as part of an enumeration of various trainings, e. g., *"[we] train on topics such as anti-discrimination and harassment, cybersecurity, diversity, equity and inclusion awareness, safety, and important company policies [...]."* We also found that **Item 1C adds** more information about **cybersecurity mitigation**, while the *cybersecurity risks* could also be found in older 10-K filings and outside of Item 1C. Threats such as phishing and social engineering were often reported outside Item 1C, while mitigations (e.g., phishing simulations) appeared within. This aligns with existing practices, as "Item 1A Risk Factors" has long included cybersecurity risks. For example, F_{23}=20.1% of companies did already report social engineering as a threat in 2023 (e. g., *"As the COVID-19 pandemic progressed, we observed an increase in cybersecurity incidents across the industry, predominantly ransomware and social engineering attacks."*), compared with F_{24}=32.8%, while only C_{24}=6.4% of companies disclosed this risk directly in Item 1C. The companies massively increased their disclosure about cybersecurity regulations and frameworks, such as NIST CSF, which went up from F_{23}=2.0% to F_{23}=39.9%. Table 2 shows an increase in disclosure in all concepts in 2024.

Summary: New SEC Rules Boost SAT Disclosure

Following the new SEC regulations, companies disclose vastly more insights into their SAT strategies (and cybersecurity in general) both within Item 1C and in other parts of the filing.

4.8 Default 10-K Text Blocks

In our qualitative coding, we found that the Item 1C texts differed in their content and structure – more so than other items that were much more standardized. However, we also discovered **reappearing phrasings and text** snippets across various companies. For example, we found the following text in 35 different 10-K filings. *"To deter and detect cyber threats, we annually provide all employees, including part-time and temporary employees, with a data protection, cybersecurity and incident response and prevention training and compliance program [...]."* This indicates that professional consulting firms have started advising their clients on Item 1C; hence, we might see more **harmonization in Item 1C** in the future. A text similarity analysis might be a worthwhile future research project [69].

Summary: Copy-Pasted SAT Disclosures

Some filings used the exact same or very similar text snippets to disclose their SAT/cybersecurity strategies.

5 Discussion

Next, we analyze our findings in response to the research questions and discuss insights for researchers, decision-, and policymakers.

Based on our keyword analysis, we can confirm that 10-K filings are a valuable source for gaining detailed insights into companies' SAT and employee-facing security strategies – despite SAT disclosure in 10-K filings being voluntary [93]. The newly introduced Item 1C notably changed what companies disclose about their strategies (see Section 4.7). Even outside of Item 1C, the new SEC regulations forced companies to reconsider their cybersecurity disclosure, specifically regarding cyber risks. Across all sectors and sizes, around 78% of companies reported implementing SAT, but the differences in sectors are significant. As one might expect, the (heavily regulated) finance sector leads the charts in SAT, mandatory employee training, phishing simulations, and other areas. Other significant differences, e. g., that Life Science reported the lowest adoption of MFA and disclosure of human-related threats, could not be easily explained. Exploring these differences is a worthwhile target for future research, as it may inform sector-specific cybersecurity legislation or targeted SAT interventions.

Those companies that consider NIST CSF, are significantly more likely to implement SAT. Companies with cyber insurance are significantly more likely to have SAT and phishing simulations in place. This is remarkable, as cyber insurances often do not cover phishing-related incidents [22, 111]. The sector-specific differences, combined with the significant relationship between NIST CSF and cyber insurance with the prevalence of SAT, showcase the influence of such cybersecurity standards on SAT, confirming previous qualitative work [1, 42, 43, 48, 49, 90].

Phishing simulations are the primary specified form of SAT. However, with only 26.5%, they are less prevalent compared with what we expected, based e. g., on the estimate of NIST for U.S. government agencies [41]. With growing evidence that those simulations offer no positive effect on employees' behavior [51, 63, 64] and scholars warning of unwanted negative side effects [67, 82, 105], the British cybersecurity agency NCSC recommends avoiding them [16, 72]. 10-K filings offer a valuable source to monitor the trend of those

Table 3: Prevalence of selected topics, based on the size of the companies (C_{24}).

	n	Micro 1,340	Small 837	Mid- 1,002	Mid+ 1,098	Large 661	Mega 111	Effect Size
Awareness Training (SAT)	4,065	52.8%	80.0%	84.1%	88.5%	89.3%	88.3%	$p < .001, V = .342$
Phishing Simulation	1,292	11.5%	20.9%	27.5%	34.1%	33.3%	23.4%	$p < .001, V = .200$
Annual SAT	1,228	11.3%	19.5%	24.2%	33.9%	32.4%	38.7%	$p < .001, V = .207$
Mandatory SAT	642	5.3%	11.8%	13.4%	14.1%	17.5%	18.0%	$p < .001, V = .133$
Onboarding	281	3.3%	6.8%	4.8%	7.5%	5.6%	2.7%	$p < .001, V = .064$
Tabletop (Management)	1,113	5.1%	15.9%	25.6%	31.2%	35.1%	30.6%	$p < .001, V = .268$
MFA	539	9.1%	9.1%	11.5%	11.8%	7.9%	8.1%	$p = .007, V = .047$
Reporting Functions	417	5.7%	8.2%	8.2%	8.5%	10.0%	11.7%	$p = .016, V = .043$
Passwords	252	5.8%	4.5%	5.3%	3.6%	3.8%	3.6%	No correlation
Social Engineering	216	4.0%	5.5%	7.7%	8.3%	6.5%	11.7%	$p < .001, V = .066$
Malware	802	14.3%	14.3%	16.1%	15.8%	15.0%	14.4%	No correlation
Cyber Insurance	1,307	16.3%	24.5%	25.7%	31.1%	30.0%	25.2%	$p < .001, V = .123$
NIST CSF	2,111	16.6%	32.9%	44.1%	55.7%	60.1%	59.5%	$p < .001, V = .328$
ISO 27001	415	2.1%	6.3%	10.2%	11.1%	12.1%	10.8%	$p < .001, V = .137$

simulations over the long run, to investigate whether the simulation advocates (CISOs and SAT vendors [47, 49]) or the critiques (scholars, Google, NCSC [67, 82, 105]) will lead the way.

Our findings present a lower bound. For example, we can conclude that *at least* a quarter of companies conduct phishing simulations, though the actual number may be higher. This is because the SEC does not explicitly require companies to disclose SAT activities, such as phishing simulations, in Item 1C. While hundreds of companies disclose details about their SAT strategy (type of SAT, topics, target groups, etc.), the majority do not or only enumerate the SAT as one defensive measure among a list of technologies and controls. Nevertheless, we could derive insights into SAT despite 10-K filings being structured governance documents. We showcase that the *human factor* is now part of most companies' cybersecurity strategies. However, as we discuss below, the employee-facing security methods might diverge from usable security advocates' understanding of humans, users, and employees.

Employees' Role. Employees are insiders, error-prone, untrained, operate with malicious intent, and are susceptible to phishing and social engineering. Whenever the filings discuss employees, they are portrayed in such a negative way. Employee blaming is still commonplace in cybersecurity [113] and there is a lack of a positive employee image in the filings (see Section 4.2). In other, non-cybersecurity-related parts of the filings, companies portray their employees as valuable assets. Microsoft, for example, writes: *"We aim to recruit, develop, and retain world-changing talent from a diversity of backgrounds. To foster their and our success, we seek to create an environment where people can thrive and do their best work. We strive to maximize the potential of our human capital resources by creating a respectful, rewarding, and inclusive work environment."*

This discrepancy in portraying employees relates to the problematic mindset of cybersecurity professionals. Usable security scholars have pointed out that a negative portrayal of employees is a danger to effective organizational cybersecurity [9, 70, 113]. A positive relationship between the security department and the employees is essential for employees' willingness to report potential incidents [76] – which hundreds of companies are expecting from their employees (see Section 4.4). We also identify a lack of usable security considerations in the filings (see Section 5.3).

We argue that 10-K filings should paint a more realistic image of the employees: (i) disclosing how many incidents were caused by insiders with malicious intent, (ii) enumerating the tools provided to employees for their effective self-defense (such as password managers with auto-fill functions), and (iii) explaining what efforts were made to adapt security policies to the realistic needs of employees working towards a productive goal.

Alternative SAT for Smaller Companies. Our findings show clear differences based on company size (see Section 4.6): larger companies report higher levels of SAT adoption, greater compliance, and more frequent use of cyber insurance. This supports prior work suggesting that smaller companies tend to lag in implementing security *best practices* [2, 11, 53, 109]. However, given recent debates around the effectiveness of such practices, such as phishing simulations [51, 63, 64] or even SAT more broadly [12], we argue that this lag should not be automatically seen as a disadvantage. Instead, we encourage researchers and policymakers to investigate how SAT is actually used in smaller organizations. For example, informal methods like word-of-mouth may play a key role in knowledge sharing. In line with Kocksch et al. [60], it is also possible that employees in smaller companies simply *care more* about protecting their organizations – a factor worth further exploration.

Limited Disclosure. Our data indicates that companies do not disclose all aspects of their employee-facing security measures. For example, only eight companies report deploying password managers. Similarly, password policies [31, 54] are most likely in place in most companies, where we find that less than 1.0% write about this topic. Hence, our dataset can quantify the prevalence of SAT, but it can not be used to quantify all types of employee-facing security. This might change when major security frameworks and regulations explicitly discuss employee-facing security measures.

While regulations and cyber insurance are significantly correlated with SAT, our data does not explain when companies choose

to report their SAT strategy in detail or not. It might be based on who creates the cybersecurity disclosure in the filings, likely professional consulting firms, law firms, auditors, security vendors, the internal risk and audit committee, or even the cybersecurity managers themselves in larger companies, while in smaller companies, the management team themselves might be involved in writing the 10-K. There might also be additional pressure from shareholders, such as the insurance companies, or customers. Investigating those influences is a worthwhile target for future research, e. g., through a survey with a random sample of companies, their cybersecurity managers or the members of their risk- and audit committees.

Future 10-K Developments. While we have found many nuances in the various Item 1C sections, we can expect a more standardized way of reporting cybersecurity strategies in the future. Once it is established, regulators and investors might rely on big consulting firms to provide their clients with exact text snippets. We have already seen indications of this in the current filings (see Section 4.8). This might reduce the variance that future qualitative work can uncover, and could also lead to an increase in SAT strategy disclosure.

5.1 Guidance for Researchers

It was recently uncovered that a science-practitioner gap exists between usable security scholars and decision-makers in organizations [39, 40, 47]. Hence, scholars need to validate whether their research enters organizational practice. Our approach to collecting and analyzing those large quantities of data allows for such validation. It already sheds light on the absence of usable security as a larger concept, not equalized with SAT, and can be used to monitor trends over the longer term, e. g., in the changing prevalence of phishing simulations or changing training topics. In the following, we discuss the potential of SEC filings as data sources and equivalent sources from other countries.

Rich Data in 10-K Filings. Multiple other pieces of information are present in the 10-K filings, such as the reporting structure between the board of directors and the CISOs, cybersecurity governance, the experience of the CISO, and data around previous incidents. The companies especially disclosed extensive details about their CISOs (e. g., their level of experience, education, and to whom they report). As there have been years-long debates about CISO skill-sets and their placement in organizations [10, 21, 47, 68, 71, 85], Item 1C holds great potential to collect other quantitative insights.

Incident Correlation. As the companies in our dataset are also required to disclose any severe security incident via an 8-K filing [93] (since 2024), we aim to correlate 8-K's with changes in the 10-K filings over time, e. g., whether incidents lead to changed employee-facing security strategies. As 8-K filings are used to disclose a variety of information, not only cybersecurity incidents, there are hundreds of them, published every week (i. e., in 2024, there are more than 69,000). An initial test revealed that filtering for keywords like "cybersecurity" does not yield promising results. An initial task will be to create an 8-K incident filtering pipeline.

Other Large-Scale Data Sources. While there is a lack of information on organizations' employee-facing security strategies, over the years, cybersecurity scholars have successfully collected large datasets about breaches and incidents and optimized crawling techniques in the process [52, 89]. Others simply paid organizations to get their datasets, e. g., [80]. While we crawled data from the U.S., there is the potential to utilize web crawling to collect insights from around the world. Information could be found in annual reports, press briefings, and news articles. For example, the *European Repository of Cyber Incidents* (EuRepoC) is already collecting such data based on selected news sources in a semi-automatic manner [25]. Analyzing larger and more diverse data sets would enable a comprehensive picture of organizations outside the U.S., the smallest companies, and non-traded entities.

Regulations outside the U.S. do not require cybersecurity strategy disclosures with the same level of detail as the recent SEC regulations. Nevertheless, companies in other countries often include cybersecurity strategies in their annual reports. For instance, an examination of annual reports from German companies revealed that several firms report engaging in SAT. Consequently, applying crawling techniques to annual reports from companies in other jurisdictions could present a valuable research avenue.

5.2 Guidance for Decision-Makers

CISOs and Boards of Directors can use our numbers and insights to benchmark their strategies against the industry average. They can also utilize the insights to challenge cybersecurity vendors' reports and white papers, e. g., when they report about the prevalence of SAT. As stated above, companies should critically reflect on how their employees are portrayed in filings. As our analysis shows that thousands of companies rely on SAT techniques with questionable effects, namely phishing simulations [51, 63, 64], especially decision makers should be cautions with just following perceived best-practices of their peers. This would be especially important for larger companies that report to implement more of those practices (see Table 3), have access to more resources, and need to follow more regulations and frameworks (see Section 4.6). As previous work has found that CISOs value insights from academic cybersecurity research, as long as the results are presented in *short executive summaries* [47], we plan to create and distribute such a summary of our key findings to the various CISO communities.

5.3 Guidance for Policy Makers

Only one company explicitly mentioned usable security. This finding is perhaps unsurprising, as our analysis indicates that SAT initiatives are often compliance-driven (see Section 4.5). Currently, usable security considerations have yet to be incorporated into regulations, norms, and standards [36, 47]. Previous work has reported multiple times how regulations directly influence companies' leadership's perception of employee-facing security [47, 59, 74]. As long as usable security considerations – such as (i) reducing workload through security policies, (ii) introducing usable security tools, and (iii) minimizing friction caused by security tasks – remain absent from regulations, they are unlikely to gain the attention of organizational leadership. Consequently, these considerations will not be reported as part of a security strategy. Outside of cybersecurity, companies use their 10-K filings to report increases in and potential threats to their productivity, *"Although we are working to provide an effective and engaging workplace, with more employees working*

remotely, it is increasingly challenging to keep employee engagement and productivity high." We argue that it should be the default to report on the impact of cybersecurity on employees' productivity, and policymakers should demand such reporting.

6 Conclusion

This study analyzed 10-K filings submitted to the SEC to gain insights into companies' Security Awareness and Training (SAT) strategies in the U.S. Our findings should be interpreted as a lower bound, as companies might implement SAT without disclosing it. However, this data must be considered reliable, given that companies and their directors are required to certify the accuracy of these filings and are held liable for any inaccuracies. Our analysis shows that at least 78.3% of companies implement SAT, and 11.0% deploy MFA for their employees. The differences between sectors are significant, as is the correlation between SAT and cybersecurity regulations. Likewise, larger companies are significantly more likely to implement SAT. Companies primarily portray their employees as a threat without any usable security considerations. Our research can be seen as a first step towards more evidence-based SAT research that is independent of numbers from sources with questionable incentives, such as cybersecurity vendors or agencies.

Acknowledgments

We would like to thank Tony Vance (Virginia Tech), who inspired us for this research with his talk at SHB 2024 in Harvard. Thanks to Simon Lenau (CISPA) for their help with our statistics. We would also like to thank Simon Parkin (TU Delft), Carolyn Guthoff (CISPA), and Matthias Fassl (CISPA) for their valuable feedback.

References

[1] Adel Ismail Al-Alawi and Sara Abdulrahman Al-Bassam. 2019. Assessing the Factors of Cybersecurity Awareness in the Banking Sector. *Arab Gulf Journal of Scientific Research* 37, 4 (June 2019), 17–32.

[2] Abdulmajeed Alahmari and Bob Duncan. 2020. Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence. In *Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA '20)*. IEEE, Dublin, Ireland, 1–5.

[3] American Institute of CPAs. 2011. System and Organization Controls 2 (SOC 2) – Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy. https://www.aicpa-cima.com/resources/landing/system-and-organization-controls-soc-suite-of-services, as of September 10, 2025.

[4] Ross Anderson. 2021. *Security Engineering: A Guide to Building Dependable Distributed Systems* (3 ed.). Wiley, Hoboken, New Jersey, USA.

[5] Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Carlos Ganán, Tom Grasso, Michael Levi, Tyler Moore, and Marie Vasek. 2019. Measuring the Changing Cost of Cybercrime. In *Workshop on the Economics of Information Security (WEIS '19)*. Oxford University Press, Boston, Massachusetts, USA, 1–32.

[6] Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Michel J.G. van Eeten, Michael Levi, Tyler Moore, and Stefan Savage. 2013. Measuring the Cost of Cybercrime. In *The Economics of Information Security and Privacy*, Rainer Böhme (Ed.). Springer, Berlin, Germany, 265–300.

[7] Ross Anderson and Tyler Moore. 2006. The Economics of Information Security. *Science* 314, 5799 (Oct. 2006), 610–613.

[8] Mirian Ariana, Ho Grant, Savage Stefan, and Voelker Geoffrey M. 2023. An Empirical Analysis of Enterprise-Wide Mandatory Password Updates. In *Annual Conference on Computer Security Applications (ACSAC '23)*. ACM, Honolulu, Hawaii, USA, 150–162.

[9] Debi Ashenden and Darren Lawrence. 2016. Security Dialogues: Building Better Relationships Between Security and Business. *IEEE Security & Privacy* 14, 3 (May 2016), 82–87.

[10] Debi Ashenden and Angela Sasse. 2013. CISOs and Organisational Culture: Their Own Worst Enemy? *Computers & Security* 39, Part B (Nov. 2013), 396–405.

[11] Maria Bada and Jason R.C. Nurse. 2019. Developing Cybersecurity Education and Awareness Programmes for Small- and Medium-Sized Enterprises (SMEs). *Information and Computer Security* 27, 3 (June 2019), 393–410.

[12] Maria Bada, Angela M. Sasse, and Jason R.C. Nurse. 2015. Cyber Security Awareness Campaigns: Why Do They Fail to Change Behaviour?. In *International Conference on Cyber Security for Sustainable Society (CSSS '15)*. Sustainable Society Network, Coventry, United Kingdom, 118–131.

[13] Ingolf Becker, Simon Parkin, and M. Angela Sasse. 2017. Finding Security Champions in Blends of Organisational Culture. In *Workshop on Usable Security and Privacy (USEC '17)*. ISOC, San Diego, California, USA.

[14] Odette Beris, Adam Beautement, and M. Angela Sasse. 2015. Employee Rule Breakers, Excuse Makers and Security Champions: Mapping the Risk Perceptions and Emotions That Drive Security Behaviors. In *New Security Paradigms Workshop (NSPW '15)*. ACM, Twente, Netherlands, 73–84.

[15] Henk Berkman, Jonathan Jona, Gladys Lee, and Naomi Soderstrom. 2018. Cybersecurity Awareness and Market Valuations. *Journal of Accounting and Public Policy* 37, 6 (Nov. 2018), 508–526.

[16] David C. 2022. NCSC Blog: Telling Users to 'Avoid Clicking Bad Links' Still Isn't Working. https://www.ncsc.gov.uk/blog-post/telling-users-to-avoid-clicking-bad-links-still-isnt-working, as of September 10, 2025.

[17] California State Legislature. 2018. California Consumer Privacy Act (CCPA). https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4., as of September 10, 2025.

[18] Jing Chen, Elaine Henry, and Xi Jiang. 2023. Is Cybersecurity Risk Factor Disclosure Informative? Evidence From Disclosures Following a Data Breach. *Journal of Business Ethics* 187, 1 (Sept. 2023), 199–224.

[19] Jacob Cohen. 1988. *Statistical Power Analysis for the Behavioral Sciences* (2 ed.). Routledge, New York City, New York, USA.

[20] Harald Cramér. 1946. *Mathematical Methods of Statistics*. Princeton University Press, Princeton, New Jersey, USA.

[21] Joseph Da Silva and Rikke Bjerg Jensen. 2022. "Cyber Security Is a Dark Art"': The CISO as Soothsayer. In *ACM Conference on Computer-Supported Cooperative Work and Social Computing (CSCW '22)*. ACM, Virtual Conference, 365:1–365:31.

[22] Savino Dambra, Leyla Bilge, and Davide Balzarotti. 2020. SoK: Cyber Insurance – Technical Challenges and a System Security Roadmap. In *IEEE Symposium on Security and Privacy (SP '20)*. IEEE, Virtual Conference, 1367–1383.

[23] Sanchari Das and Junibel De La Cruz. 2022. SoK: A Proposal for Incorporating Accessible Gamified Cybersecurity Awareness Training Informed by a Systematic Literature Review. In *Workshop on Usable Security and Privacy (USEC '22)*. ISOC, San Diego, California, USA.

[24] Thomas Ecabert, Fabian Muhly, and Verena Zimmermann. 2024. Implications of Cyber Incident Reporting Obligations on Multinational Organizations Headquartered in Switzerland. *International Cybersecurity Law Review* 5, 4 (Sept. 2024), 585–614.

[25] European Repository of Cyber Incidents. 2025. EuRepoC: European Repository of Cyber Incidents. https://eurepoc.eu, as of September 10, 2025.

[26] Florian M. Farke, Lennart Lorenz, Theodor Schnitzler, Philipp Markert, and Markus Dürmuth. 2020. "You still use the password after all" – Exploring FIDO2 Security Keys in a Small Company. In *Symposium on Usable Privacy and Security (SOUPS '20)*. USENIX, Virtual Conference, 19–35.

[27] Financial Industry Regulatory Authority, Inc. 2022. Market Cap Explained. https://www.finra.org/investors/insights/market-cap, as of September 10, 2025.

[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 *Symposium on Usable Privacy and Security (SOUPS '21)*. USENIX, Virtual Conference, 339–358.

[29] Trevor Gabriel and Steven Furnell. 2011. Selecting Security Champions. *Computer Fraud & Security* 2011, 8 (Aug. 2011), 8–12.

[30] Lei Gao, Thomas G. Calderon, and Fengchun Tang. 2020. Public Companies' Cybersecurity Risk Disclosures. *Journal of Accounting Information Systems* 38, 100468 (Sept. 2020), 1–22.

[31] Eva Gerlitz, Maximilian Häring, and Matthew Smith. 2021. Please do not use !?_ or your License Plate Number: Analyzing Password Policies in German Companies. In *Symposium on Usable Privacy and Security (SOUPS '21)*. USENIX, Virtual Conference, 17–36.

[32] Eva Gerlitz, Maximilian Häring, Matthew Smith, and Christian Tiefenau. 2023. Evolution of Password Expiry in Companies: Measuring the Adoption of Recommendations by the German Federal Office for Information Security. In *Symposium on Usable Privacy and Security (SOUPS '23)*. USENIX, Anaheim, California, USA, 191–210.

[33] Cristi Gleason, Zhejia Ling, and Rong Zhao. 2020. Selective Disclosure and the Role of Form 8-K in the post-Reg FD Era. *Journal of Business Finance & Accounting* 47, 3-4 (Nov. 2020), 365–396.

[34] Lawrence A. Gordon, Martin P. Loeb, and Tashfeen Sohail. 2010. Market Value of Voluntary Disclosures Concerning Information Security. *Management Information Systems Quarterly* 34, 3 (Sept. 2010), 567–594.

[35] William J. Gordon, Adam Wright, Ranjit Aiyagari, Leslie Corbo, Robert J. Glynn, Jigar Kadakia, Jack Kufahl, Christina Mazzone, James Noga, Mark Parkulo, et al. 2019. Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions. *JAMA Network Open* 2, 3 (March 2019), 1–9.

[36] Marco Gutfleisch, Jan H. Klemmer, Niklas Busch, Yasemin Acar, M. Angela Sasse, and Sascha Fahl. 2022. How Does Usable Security (Not) End Up in Software Products? Results From a Qualitative Interview Study. In *IEEE Symposium on Security and Privacy (SP '22)*. IEEE, San Francisco, California, USA, 893–910.

[37] Barbara Guttman and Edward A. Roback. 1995. An Introduction to Computer Security: The NIST Handbook. https://csrc.nist.gov/pubs/sp/800/12/final, as of September 10, 2025.

[38] Hana Habib, Pardis Emami Naeini, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2018. User Behaviors and Attitudes Under Password Expiration Policies. In *Symposium on Usable Privacy and Security (SOUPS '18)*. USENIX, Baltimore, Maryland, USA, 13–30.

[39] Julie M. Haney, Clyburn Cunningham, and Susanne M. Furman. 2024. Towards Bridging the Research-Practice Gap: Understanding Researcher-Practitioner Interactions and Challenges in Human-Centered Cybersecurity. In *Symposium on Usable Privacy and Security (SOUPS '24)*. USENIX, Philadelphia, Pennsylvania, USA, 567–586.

[40] Julie M. Haney, Clyburn Cunningham, and Susanne M. Furman. 2024. Towards Integrating Human-Centered Cybersecurity Research Into Practice: A Practitioner Survey. In *Workshop on Usable Security and Privacy (USEC '24)*. ISOC, San Diego, California, USA.

[41] Julie M. Haney, Jody Jacobs, Susanne M. Furman, and Fernando Barrientos. 2022. *Approaches and Challenges of Federal Cybersecurity Awareness Programs*. Technical Report NISTIR 8420A. National Institute of Standards and Technology.

[42] Julie M. Haney and Wayne Lutters. 2020. Security Awareness Training for the Workforce: Moving Beyond "Check-the-Box" Compliance. *Computer* 53, 10 (Oct. 2020), 91–95.

[43] Julie M. Haney and Wayne Lutters. 2024. From Compliance to Impact: Tracing the Transformation of an Organisational Security Awareness Programme. *Cyber Security: A Peer-Reviewed Journal* 8, 2 (Oct. 2024), 110–130.

[44] Cormac Herley and Wolter Pieters. 2015. "If You Were Attacked, You'd Be Sorry": Counterfactuals as Security Arguments. In *New Security Paradigms Workshop (NSPW '15)*. ACM, Twente, Netherlands, 112–123.

[45] Cormac Herley and P.C. Van Oorschot. 2017. SoK: Science, Security and the Elusive Goal of Security as a Scientific Pursuit. In *IEEE Symposium on Security and Privacy (SP '17)*. IEEE, San Jose, California, USA, 99–120.

[46] Jonas Hielscher and Maximilian Golla. 2025. Replication Package: "Quantifying Security Training in Organizations Through the Analysis of U.S. SEC 10-K Filings". https://doi.org/10.6084/m9.figshare.28789001, as of September 10, 2025.

[47] 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 *USENIX Security Symposium (SSYM '23)*. USENIX, Anaheim, California, USA, 2311–2328.

[48] Jonas Hielscher and Simon Parkin. 2024. "What Keeps People Secure Is That They Met the Security Team": Deconstructing Drivers and Goals of Organizational Security Awareness. In *USENIX Security Symposium (SSYM '24)*. USENIX, Philadelphia, Pennsylvania, USA, 3295–3312.

[49] 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 *ACM Conference on Computer and Communications Security (CCS '24)*. ACM, Salt Lake City, Utah, USA, 2666–2680.

[50] Annette Hillebrand, Antonia Niederprüm, Saskja Schäfer, and Sonja Thiele. 2018. Current IT Security Situation in SME: Summary of Representative Survey Results. https://www.wik.org/veroeffentlichungen/veroeffentlichung/aktuelle-lage-der-it-sicherheit-in-kmu, as of September 10, 2025.

[51] Grant Ho, Ariana Mirian, Elisa Luo, Khang Tong, Euyhyun Lee, Lin Liu, Christopher A. Longhorst, Christian Dameff, Stefan Savage, and Geoffrey M. Voelker. 2025. Understanding the Efficacy of Phishing Training in Practice. In *IEEE Symposium on Security and Privacy (SP '25)*. IEEE, San Jose, California, USA, 1–18.

[52] MC. Jordan Howell and George W. Burruss. 2020. *Datasets for Analysis of Cybercrime* (1 ed.). Springer, Cham, Switzerland, Chapter 10, 207–219.

[53] Nicolas Huaman, Bennet von Skarczinski, Christian Stransky, Dominik Wermke, Yasemin Acar, Arne Dreißigacker, and Sascha Fahl. 2021. A Large-Scale Interview Study on Information Security in and Attacks against Small and Medium-sized Enterprises. In *USENIX Security Symposium (SSYM '21)*. USENIX, Virtual Conference, 1235–1252.

[54] Philip G. Inglesant and M. Angela Sasse. 2010. The True Cost of Unusable Password Policies: Password Use in the Wild. In *ACM Conference on Human Factors in Computing Systems (CHI '10)*. ACM, Atlanta, Georgia, USA, 383–392.

[55] International Organization for Standardization. 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, Switzerland.

[56] Apu Kapadia. 2007. A Case (Study) for Usability in Secure Email Communication. *IEEE Security & Privacy* 5, 2 (March 2007), 80–84.

[57] 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, 102267 (July 2021), 1–22.

[58] Elisabeth Kirsten, Annalina Buckmann, Abraham Mhaidli, and Steffen Becker. 2024. Decoding Complexity: Exploring Human-AI Concordance in Qualitative Coding. *CoRR* abs/2403.06607 (March 2024), 1–6.

[59] April Klein, Raffaele Manini, and Yanting Shi. 2022. Across the Pond: How US Firms' Boards of Directors Adapted to the Passage of the General Data Protection Regulation. *Contemporary Accounting Research* 39, 1 (March 2022), 199–233.

[60] Laura Kocksch, Matthias Korn, Andreas Poller, and Susann Wagenknecht. 2018. Caring for IT Security: Accountabilities, Moralities, and Oscillations in IT Security Practices. In *ACM Conference on Computer-Supported Cooperative Work and Social Computing (CSCW '18)*. ACM, New York City, New York, USA, 92:1–92:20.

[61] Saranga Komanduri, Richard Shay, Patrick Gage Kelley, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Serge Egelman. 2011. Of Passwords and People: Measuring the Effect of Password-Composition Policies. In *ACM Conference on Human Factors in Computing Systems (CHI '11)*. ACM, Vancouver, British Columbia, Canada, 2595–2604.

[62] Udo Kuckartz and Stefan Rädiker. 2024. *Qualitative Content Analysis: Methods, Practice, Implementation with Software and Artificial Intelligence (German Version)* (6 ed.). Beltz Juventa, Weinheim, Germany.

[63] Daniele Lain, Tarek Jost, Sinisa Matetic, Kari Kostiainen, and Srdjan Capkun. 2024. Content, Nudges and Incentives: A Study on the Effectiveness and Perception of Embedded Phishing Training. In *ACM Conference on Computer and Communications Security (CCS '24)*. ACM, Salt Lake City, Utah, USA, 4182–4196.

[64] Daniele Lain, Kari Kostiainen, and Srdjan Capkun. 2022. Phishing in Organizations: Findings from a Large-Scale and Long-Term Study. In *IEEE Symposium on Security and Privacy (SP '22)*. IEEE, San Francisco, California, USA, 842–859.

[65] Leona Lassak, Elleen Pan, Blase Ur, and Maximilian Golla. 2024. Why Aren't We Using Passkeys? Obstacles Companies Face Deploying FIDO2 Passwordless Authentication. In *USENIX Security Symposium (SSYM '24)*. USENIX, Philadelphia, Pennsylvania, USA, 7231–7248.

[66] Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. 2017. *Research Methods in Human Computer Interaction* (2 ed.). Morgan Kaufmann, Cambridge, Massachusetts, USA.

[67] Matt Linton. 2024. Google Security – On Fire Drills and Phishing Tests. https://security.googleblog.com/2024/05/on-fire-drills-and-phishing-tests.html, as of September 10, 2025.

[68] Michelle René Lowry, Zeynep Sahin, and Anthony Vance. 2022. Taking a Seat at the Table: The Quest for CISO Legitimacy. In *International Conference on Information Systems (ICIS '22)*. AIS, Copenhagen, Denmark, 1–14.

[69] Otgonpurev Mendsaikhan, Hirokazu Hasegawa, Yukiko Yamaguchi, and Hajime Shimada. 2020. Quantifying the Significance and Relevance of Cyber-Security Text Through Textual Similarity and Cyber-Security Knowledge Graph. *IEEE Access* 8 (Sept. 2020), 177041–177052.

[70] Uta Menges, Jonas Hielscher, Laura Kocksch, Annette Kluge, and M. Angela Sasse. 2023. Caring Not Scaring – An Evaluation of a Workshop to Train Apprentices as Security Champions. In *European Workshop on Usable Security (EuroUSEC '23)*. ACM, New York, NY, USA, 237–252.

[71] Pedro Monzelo and Sergio Nunes. 2019. The Role of the Chief Information Security Officer (CISO) in Organizations. In *Conferência da Associação Portuguesa de Sistemas de Informação (CAPSI '19)*. APSI, Lisbon, Portugal, 1–14.

[72] National Cyber Security Centre. 2024. Phishing Attacks: Defending Your Organisation. https://www.ncsc.gov.uk/guidance/phishing, as of September 10, 2025.

[73] Alexandra Nisenoff, Maximilian Golla, Miranda Wei, Juliette Hainline, Hayley Szymanek, Annika Braun, Annika Hildebrandt, Blair Christensen, David Langenberg, and Blase Ur. 2023. A Two-Decade Retrospective Analysis of a University's Vulnerability to Attacks Exploiting Reused Passwords. In *USENIX Security Symposium (SSYM '23)*. USENIX, Anaheim, California, USA, 5127–5144.

[74] Jens Opdenbusch, Jonas Hielscher, and Martina Angela Sasse. 2025. "Where Are We on Cyber?" – A Qualitative Study on Boards' Cybersecurity Risk Decision Making. In *Symposium on Network and Distributed System Security (NDSS '25)*. ISOC, San Diego, California, USA.

[75] Cherilyn Pascoe, Stephen Quinn, and Karen Scarfone. 2024. The NIST Cybersecurity Framework (CSF) 2.0. https://doi.org/10.6028/NIST.CSWP.29, as of September 10, 2025.

[76] Clare M Patterson, Jason RC Nurse, and Virginia NL Franqueira. 2024. "I Don't Think We're There Yet": The Practices and Challenges of Organisational Learning from Cyber Security Incidents. *Computers & Security* 139, 103699 (April 2024), 1–18.

[77] Agnieszka Pawlowska and Benedikt Scherer. 2021. German BSI: IT Security While Working from Home in 2020 (German Version). https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Umfrage-Home-Office/umfrage_home-office-2020.pdf, as of September 10, 2025.

[78] 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 *Symposium on Usable Privacy and Security (SOUPS '20)*. USENIX, Virtual Conference, 259–284.
[79] Fabio Rizzoni, Sabina Magalini, Alessandra Casaroli, Pasquale Mari, Matt Dixon, and Lynne Coventry. 2022. Phishing Simulation Exercise in a Large Hospital: A Case Study. *Digital Health* 8 (March 2022), 1–13.
[80] Sasha Romanosky. 2016. Examining the Costs and Causes of Cyber Incidents. *Journal of Cybersecurity* 2, 2 (Dec. 2016), 121–135.
[81] Katharina Schiller, Florian Adamsky, Christian Eichenmüller, Matthias Reimert, and Zinaida Benenson. 2024. Employees' Attitudes Towards Phishing Simulations: "It's Like When a Child Reaches Onto the Hot Hob". In *ACM Conference on Computer and Communications Security (CCS '24)*. ACM, Salt Lake City, Utah, USA, 4167–4181.
[82] Markus Schöps, Marco Gutfleisch, Eric Wolter, and M. Angela Sasse. 2024. Simulated Stress: A Case Study of the Effects of a Simulated Phishing Campaign on Employees' Perception, Stress and Self-Efficacy. In *USENIX Security Symposium (SSYM '24)*. USENIX, Philadelphia, Pennsylvania, USA, 4589–4606.
[83] Shobhit Seth, Gordon Scott, and Suzanne Kvilhaug. 2024. Market Capitalization Sizes. https://www.investopedia.com/investing/market-capitalization-defined/, as of September 10, 2025.
[84] Karzan H. Sharif and Siddeeq Y. Ameen. 2020. A Review of Security Awareness Approaches with Special Emphasis on Gamification. In *International Conference on Advanced Science and Engineering (ICOASE '20)*. IEEE, Duhok, Iraq, 151–156.
[85] Raghvendra Singh, Pavankumar Mulgund, and Sanjukta Das Smith. 2024. Exploring the Evolving Balance of Power Between CISOs and CIOs: A Qualitative Perspective. In *Americas Conference on Information Systems (AMCIS '24)*. AIS, Salt Lake City, Utah, USA.
[86] Rob Sloan. 2024. S&P 500 Proxy Statements: What Companies Disclose About Their Cybersecurity Programs. https://www.zscaler.com/resources/industry-reports/sp-500-cyberssecurity-risk-management.pdf, as of September 10, 2025.
[87] Jonah Stegman, Patrick J. Trottier, Caroline Hillier, Hassan Khan, and Mohammad Mannan. 2023. "My Privacy for Their Security": Employees' Privacy Perspectives and Expectations When Using Enterprise Security Software. In *USENIX Security Symposium (SSYM '23)*. USENIX, Anaheim, California, USA, 3583–3600.
[88] ThriveDX. 2022. Cybersecurity Awareness Training Study. https://web.archive.org/web/20230104143405/https://2714581.fs1.hubspotusercontent-na1.net/hubfs/2714581/TDX%20Downloads/2022-TDX-Cybersecurity-Awareness-Training-Study-Final%201.pdf, as of September 10, 2025.
[89] Kieron Turk, Sergio Pastrana, and Ben Collier. 2020. A Tight Scrape: Methodological Approaches to Cybercrime Research Data Collection in Adversarial Environments. In *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW '20)*. IEEE, Genoa, Italy, 428–437.
[90] Betsy Uchendu, Jason R.C. Nurse, Maria Bada, and Steven Furnell. 2021. Developing a Cyber Security Culture: Current Practices and Future Needs. *Computers & Security* 109, 102387 (Oct. 2021), 1–23.
[91] U.S. Department of Homeland Security. 2012. The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research. https://www.caida.org/publications/papers/2012/menlo_report_actual_formatted/, as of September 10, 2025.
[92] U.S. Securities and Exchange Commission. 1941. Regulation N-5B-1: §270.5b-1 Definition of "Total Assets". https://www.law.cornell.edu/cfr/text/17/270.5b-1, as of September 10, 2025.
[93] U.S. Securities and Exchange Commission. 2023. Public Company Cybersecurity Disclosures: Final Rules. https://www.sec.gov/files/33-11216-fact-sheet.pdf, as of September 10, 2025.
[94] U.S. Securities and Exchange Commission. 2023. SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies. https://www.sec.gov/files/rules/final/2023/33-11216.pdf, as of September 10, 2025.
[95] U.S. Securities and Exchange Commission. 2024. Developer Resources. https://www.sec.gov/about/developer-resources, as of September 10, 2025.
[96] U.S. Securities and Exchange Commission. 2024. Exchange Act Reporting and Registration. https://www.sec.gov/resources-small-businesses/going-public/exchange-act-reporting-registration, as of September 10, 2025.
[97] U.S. Securities and Exchange Commission. 2024. The Electronic Data Gathering, Analysis, and Retrieval (EDGAR) System. https://www.sec.gov/edgar/searchedgar/companysearch.html, as of September 10, 2025.
[98] U.S. Securities and Exchange Commission. 2024. Webmaster Frequently Asked Questions. https://www.sec.gov/about/webmaster-frequently-asked-questions, as of September 10, 2025.
[99] U.S. Securities and Exchange Commission. 2025. How to Read a 10-K. https://www.sec.gov/answers/reada10k.htm, as of September 10, 2025.
[100] U.S. Securities and Exchange Commission. 2025. Standard Industrial Classification (SIC) Code List. https://www.sec.gov/search-filings/standard-industrial-classification-sic-code-list, as of September 10, 2025.
[101] VERBI GmbH. 2023. MAXQDA 24: Software for Qualitative Data Analysis. https://www.maxqda.com, as of September 10, 2025.
[102] VERBI GmbH. 2025. MAXQDA: Code Matrix Browser – Visualizing Codes Per Document. https://www.maxqda.com/help-mx24/visual-tools/code-matrix-browser-visualizing-codes-per-document, as of September 10, 2025.
[103] VERBI GmbH. 2025. MAXQDA: Global Text Search. https://www.maxqda.com/help-mx24/text-search/global-text-search, as of September 10, 2025.
[104] Verified Market Research. 2024. Global Security Awareness Training Software Market Size. https://www.verifiedmarketresearch.com/product/security-awareness-training-software-market/, as of September 10, 2025.
[105] Melanie Volkamer, Martina Angela Sasse, and Franziska Boehm. 2020. Analysing Simulated Phishing Campaigns for Staff. In *European Symposium on Research in Computer Security (ESORICS '20)*. Springer, Guildford, United Kingdom, 312–328.
[106] Wenjia Wang, Seyed Masoud Sadjadi, and Naphtali Rishe. 2024. A Survey of Major Cybersecurity Compliance Frameworks. In *IEEE Conference on Big Data Security on Cloud (BigDataSecurity '24)*. IEEE, New York City, New York, USA, 23–34.
[107] Jonathan Whitaker and Shital Thekdi. 2024. You Cannot Spell Risk Without "I-S": The Disclosure of Information Systems Risks by Fortune 1000 Firms. *Risk Analysis* 2024, 9 (Sept. 2024), 1–17.
[108] Emma J. Williams, Joanne Hinds, and Adam N. Joinson. 2018. Exploring Susceptibility to Phishing in the Workplace. *International Journal of Human-Computer Studies* 120 (Dec. 2018), 1–13.
[109] Flynn Wolf, Adam J. Aviv, and Ravi Kuber. 2021. Security Obstacles and Motivations for Small Businesses from a CISO's Perspective. In *USENIX Security Symposium (SSYM '21)*. USENIX, Virtual Conference, 1199–1216.
[110] Richmond Y. Wong, Andrew Chong, and R. Cooper Aspegren. 2023. Privacy Legislation as Business Risks: How GDPR and CCPA are Represented in Technology Companies' Investment Risk Disclosures. In *ACM Conference on Computer-Supported Cooperative Work and Social Computing (CSCW '23)*. ACM, Minneapolis, Minnesota, USA, 82:1–82:26.
[111] Daniel W. Woods and Rainer Böhme. 2021. How Cyber Insurance Shapes Incident Response: A Mixed Methods Study. In *Workshop on the Economics of Information Security (WEIS '21)*. Oxford University Press, Virtual Conference, 1–35.
[112] XBRL International. 2003. Extensible Business Reporting Language (XBRL) 2.1 Specification. https://specifications.xbrl.org/xbrl-essentials.html, as of September 10, 2025.
[113] 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 (Nov. 2019), 169–187.

A Replication Package

We provide a replication package to promote open science and enable the **full reproducibility** of our results (find the online repository here: [46]). While the package does not include the 10-K filing documents, we provide a comprehensive list of URLs linking directly to these filings, allowing them to be easily downloaded. The replication package includes the following components: (i) A PDF document with the list of keyword queries and a figure describing the crawling pipeline. (ii) A list of URLs for all 10-K filings included in our analysis. While the SEC explicitly states that *"EDGAR public filing content are free to access and reuse"* [98] and hence publishing a list of URLs should be feasible, the SEC also states that there might be rare cases where filing content (like copyright protected images of the companies) is not free to reuse. Due to those legal uncertainties around uploading the filings directly, only the URL list is provided. (iii) The Python code used to crawl, transform, and extract the 10-K filings and Item 1C sections. (iv) A matrix containing all 10-K filings and the concepts identified within each filing. Combined with search queries, this matrix facilitates direct reproducibility of our results and enables further statistical analyses. (v) The code used to perform the statistical calculations. (vi) A summary table of our statistical analysis results.