Above and Beyond: Organizational Efforts to Complement U.S. Digital Security Compliance Mandates

Rock Stevens*, Faris Bugra Kokulu*†, Adam Doupé†, and Michelle L. Mazurek
University of Maryland, †Arizona State University
{rstevens, mmazurek}@cs.umd.edu, {fkokulu, doupe}@asu.edu

***Abstract*—Organizations that provide essential services such as electricity, healthcare, and secure financial transactions are required to use digital-security compliance programs to establish a baseline of minimum security. Unfortunately, these compliance programs are known to suffer from a multitude of issues (both in how they are written and in how organizations implement them), resulting in organizations implementing their own security measures to fill actual or perceived compliance gaps. In this study, we survey 40 security professionals from six U.S. essential-service sectors to gain insight into how organizations complement compliance to fix perceived security gaps, which measures worked particularly well, and how their organizations prioritize and evaluate the measures they adopt.**

We find that organizations complement compliance programs often, with 37 of 40 participants confirming that their organizations have gone beyond what they perceive as mandated compliance measures to mitigate otherwise unaddressed risks. While participants were generally positive about these perceived complementary measures, they also reported challenges related to poor management, information saturation, and difficulty keeping complementary measures up-to-date and relevant. Based on these results, we recommend that compliance standards directly integrate guidance for carefully managing and auditing any perceived complementary measures that an organization chooses to implement and that organizations carefully plan end-to-end deployment and operation before implementing these measures.

I. Introduction

Public and private sector organizations that provide essential services must protect sensitive health and education data, secure transactions and financial records, and ensure that public utilities and services remain operational. Digital-security compliance programs are intended to help these organizations establish baseline minimum security standards to protect themselves and their users. Compliance standards specify *policies* and *technical controls*, such as disabling user accounts when employees no longer require them or encrypting stored sensitive data. Compliance is generally required for essential service organizations. Organizations that fail to comply with security standards may face significant fines (sometimes in the multi-million-dollar range) or lose access to sensitive information [10], [68].

Past evidence shows that organizations often struggle to achieve full compliance and fully compliant organizations are still vulnerable to security breaches [3], [15]–[18], [75]. Additionally, organizations that strictly adhere to compliance standards "by-the-letter" are not guaranteed security — and may even engender sub-optimal security conditions [83], [84]. Taken together, this situation adds up to a host of known issues with compliance, as identified in prior work [11], [24], [42], [46], [76]. In several cases, system administrators report taking additional steps beyond what they perceive as required for compliance to fill perceived security gaps [39], [56], [83].

In this study, we report on organizations' use of these perceived *complementary measures* — policies and technical controls enacted to mend real or perceived security gaps and exceed compliance requirements. In particular, we explore how organizations decide when to add these measures, why they believe them to be necessary, and how they choose among them. To answer these questions, we surveyed 40 security professionals from multiple U.S. essential-service sectors who represent several multi-million dollar organizations. Participants reported which complementary measures their organizations use to address which perceived security gaps, which complementary measures worked particularly well (or poorly), and how their organizations prioritize and evaluate the complementary measures they adopt. Participants cumulatively reported using more than 21 different compliance standards, including protection programs for the electric grid, healthcare, military networks, and credit card payments.

In line with prior work, we find that only 10 participants believe compliance programs are themselves sufficient to establish baseline security. This could reflect problems with the standards themselves, or could arise from the organization not properly following the standard (even if they consider themselves compliant). Furthermore, 37 of 40 participants reported implementing complementary measures to mitigate risks perceived to be unaddressed by compliance standards.

Some of the most commonly reported perceived complementary measures include multi-factor authentication, endpoint detection and response tools, periodic account-access reviews, new physical access barriers, and threat-hunting processes.

Although the specifics of how and why organizations implement perceived complementary measures vary, we find that organizations often adopt complementary measures in response to security incidents, to reduce costs, when recommended by external experts, or when requested by (sometimes non-technical) executives.

*Both authors contributed equally.

Network and Distributed Systems Security (NDSS) Symposium 2022
24-28 April 2022, San Diego, CA, USA
ISBN 1-891562-74-6
https://dx.doi.org/10.14722/ndss.2022.23107
www.ndss-symposium.org

On the whole, participants found these perceived complementary measures to be beneficial, but far from perfect. Participants are generally more satisfied with complementary efforts that require minimal human-in-the-loop interactions, but tend to believe complementary measures are more effective when organizations frequently reassess their efficacy. Participants reported numerous instances of poorly managed complementary processes, investments in unproven or incompatible "solutions," information overload, and difficulty keeping complementary measures up to date and relevant.

Our research provides novel insights into the use of perceived complementary measures within real-world organizations that face constant digital-security threats. We are able to characterize the kinds of complementary measures that organizations employ, how these complementary measures are selected and managed, and reasons why they do and do not succeed. Additionally, our study highlights real-world anecdotes that seemingly contradict sound security practices, such as organizations counter-intuitively benefiting from security incidents, instances where complementary measures hinder security, and large variances in how and why organizations decide to complement compliance.

Based on these contributions, our study provides recommendations for improving compliance standards to support the use of complementary measures when perceived to be necessary and identifies opportunities for future research in understanding the complexity of compliance guidelines and implementation.

II. Background and Related Work

We discuss compliance programs and their shortcomings, as well as prior research broadly examining human factors in security operations.

Compliance programs and challenges. The first digital-security compliance programs in the United States originated in the mid-1980s and required federal organizations to protect their information systems [67]. Compliance programs are designed to ensure organizations establish baseline security and typically have provisions for enacting sanctions for non-compliance. In this section, we review past research involving compliance programs.

Correctly understanding and implementing legal obligations in compliance program texts have been studied by many researchers. Breaux et al. focused on the difficulty of implementing compliance programs, specifically the ambiguity and complexity of the legal language that is used to describe rights and obligations that compliance programs require [15]–[18]. Similarly, Agarwal et al. proposed a flexible and modular compliance assessment framework that would help companies understand their legal obligations [3].

Complications with compliance vary by business sector, but are well documented. For instance, in finance, Rahaman et al. examined the PCI certification process, finding an alarming gap between PCI-DSS as written and its real-world enforcement [78]. Healthcare researchers have reported on the complications of implementing compliance mandates in practice and the factors that influence compliance [8], [80].

Others have documented human factors that inhibit compliance adoption and adherence, ranging from standards' lack of accounting for non-optimal human behavior [56] to resistance to formal auditing and grading [98].

Outsourcing is another influential factor that shapes compliance programs. Hui et al. analyzed how system interdependency risks interact with security compliance requirements [45]. For instance, issues with industrial control systems may allow for known critical vulnerabilities to be unaddressed while an organization can be fully compliant [13].

Lastly, researchers found that organizations often use compliance standards as baseline security checklists, and organizations may have security issues because they follow compliance "by the letter" [83], [84], [99].

In an effort to avoid costly financial sanctions, organizations invest significant time preparing for a pending compliance audit and tend to neglect audit findings until the next pending audit requires action [75]. Researchers found significant organizational and cultural changes are necessary for compliance audits to become more meaningful than "check-the-box" requirements, to include: (1) regular policy updates that can keep pace with emerging technologies, (2) flexible implementation timelines for policy revisions, and (3) complementary training programs that emphasize security with respect to individuals' personal work roles [63].

In our study, instead of focusing on problems associated with compliance programs directly, we focus on how organizations perceive compliance shortcomings, and therefore work around or supplement compliance programs to fulfill their security requirements.

Human factors in security operations. Additionally, there is a considerable body of work analyzing human factors in security operations broadly. Researchers conducted a case study with New York City Cyber Command and found that proactive risk management planning (through threat modeling) had tangible benefits with minimal time and resource investments [82]. In a study on security management systems, Harmening stated that network administrators who work for organizations need to define their set of policies to cover all parts of their computer and network resources. They further added that standards that were in place some of these aged policies that organizations use might not be sufficient for current business practices [39]. Assal and Chiasson interviewed developers to explore the effect of human-centric influential factors on software security practices and their link to non-compliance [11]. Hu et al. developed an individual behavioral model to understand how top management and organizational culture influence employee compliance [42]. János and Dai found that organizational behavior and culture impacted the efficacy of security operations [51], which validates the initial findings of Kolkowska and Dhillon on organizational power and compliance [55]. Kokulu et al. similarly found numerous deficiencies within Security Operation Centers (SOCs)

stemming from insufficient training, poor communication, and evaluation criteria disconnected from meaningful performance metrics [54]. Puhakainnen and Siponen studied employee non-compliance with information security policies and found that theory-based training achieved positive results [76]. Dietrich et al. found that security misconfigurations (which some compliance programs address), have similar human deficiencies [28].

Research from Alomar et al. discusses breakdowns in trust, communication, and resourcing that inhibit the effectiveness of vulnerability disclosure programs [5]. Furnell et al. identified multiple usability concerns in incident response tools as well as the occasional need for internally-developed tools [34]. Sundaramurthy et al. highlight the consequences of "build-once-sell-to-everyone" security vendor models on SOCs and also found that in-house, tailored solutions may best support analysts' needs [87].

Focusing on security analyst performance, Sundaramurthy et al. observed burnout rates within SOCs and identified possible solutions for sustaining morale and completion of security tasks [86]. Dykstra and Paul found that analysts' fatigue and stress levels increase throughout the day, affecting their ability to perform security tasks and suggesting analysts' tools and environment need to offset frustration where possible [30]. Other researchers focused on reducing the impacts of information overload to help incident responders improve mitigation efforts against true-positive attacks [40]. Our study adds to our overall understanding of security operations by specifically exploring the use of perceived complementary measures to supplement compliance requirements.

III. Method

In this section, we discuss our survey design, our participant recruitment, and the quantitative and qualitative analysis we conducted on participant responses.

This study was reviewed and classified as "exempt" by the University of Maryland Institutional Review Board, indicative of minimal risk to human subjects and minimal collection of identifiable data. We asked participants to provide information about their professional experiences, perceptions, and background, and we did not collect personally identifiable information. Due to the sensitive nature of unmitigated security vulnerabilities, we instructed participants to only disclose information they were comfortable with sharing; additionally, we generalize many of our findings to protect organizations and systems.

A. Survey design

We designed a 21-question survey with a combination of open-ended and close-ended questions in four sections: introduction/screening, baseline understanding, assessment of complementary measures, and demographics (Appendix A). Research suggests that the quality of survey responses decreases over time, and excessively long surveys may result in a participant quitting the study [44]. To this end, we designed our surveys for experts to complete within 25–30 minutes of focused effort, in line with suggested best practices [35]. Actual completion time averaged 27.9 minutes ($\sigma = 2.4$). Participants were not compensated directly, but were invited to opt into a raffle for one of two $50 gift cards.

First, participants answered screening questions (see Section III-B) to ensure they were qualified to address our research questions.

Next, we asked two questions to better understand (1) if participants' organizations believed compliance is sufficient to protect their systems and data, and (2) if participants' organizations employed proactive security controls to address threats perceived not to be covered by compliance programs. Participants who indicated their current employer enacts defensive measures complementary to compliance controls were directed to the next section; otherwise they were directed to the demographics section.

The third section presented participants with a list of 18 proactive security controls, selected from a corpus of digital-security risk-mitigation literature [37], [89], [94] and previous research on applied security [30], [54], [82], [83]. Note that while we verified that the listed security controls were complementary to at least one standard, they are not necessarily complementary to all possible standards. We asked participants to select all of the controls they employ that they perceive to *complement* required compliance controls at their organizations. Additionally, to improve thoroughness and coverage, we allowed for participants to describe and discuss other (unlisted) security controls they may employ as perceived complementary measures.

If participants selected more than five complementary measures, we asked them to select the five controls they were most interested in discussing. We chose five controls because our survey pilot suggested that this number achieved a reasonable balance between acquiring more information and keeping the survey as short as possible. We then randomized the order of the participants' five selections and asked six questions per control. Two questions were Likert-scale questions asking (1) how frequently the participant's organization assesses the control's effectiveness and (2) how well the control has worked out for their organization. Four of these six questions were open-ended and asked participants to describe in detail: (1) why was the control implemented, (2) the aspects that worked well (or not well) with implementation, (3) how participants ensured that the perceived complementary measures were compatible with compliance standards, and (4) the key factors for prioritizing perceived complementary measures.

Next, we collected demographic information about participants' experience and perspective. These included specific work role, current business sector, years of experience, and information about their clientele.

Finally, we asked for participants' permission to contact them if we required response clarification or for future studies.

Survey pilot. Prior to broadly distributing our survey, we asked two security professionals to complete the survey and provide feedback, specifically focused on question relevance, completeness, and clarity. We updated the survey based on

pilot feedback and overall study flow; the final version of the survey is given in Appendix A.

B. Recruitment and Screening

We leveraged personal contacts, email distribution lists, and social media outlets tailored towards multiple different business sectors to assist with response diversity. Specifically, we sought participants from the following sectors: government, healthcare, financial services, consumer services, information technology, and education. We also employed snowball sampling, in which participants recommended other qualified professionals. Diversifying participants based on their current work role and business sector supports ecological validity and ensures findings represent varying perspectives.

We screened participants using four criteria: (1) they were actively employed by an organization that uses digital-security compliance programs, (2) their current job involved compliance standards, (3) their current work role, and (4) their experience level with information technology and compliance programs.

The first two factors ensure participants are dealing with compliance currently. Additionally, we selected participants who serve as security managers, security analysts, security engineers, governance experts, or software developers to increase the likelihood participants provided responses from a technical perspective.

We also screened participants to verify they were fluent in English, over 18 years old, and within the United States.

C. Data Analysis

We use both qualitative and quantitative analysis to identify themes and trends across participant responses.

Validation of complementary measures. We manually checked many of the reported complementary measures and, in our opinion, nearly all were indeed complementary, meaning that applicable compliance standards the participant reported do not actually require the measure's use.[1] We discarded responses from one respondent (not included in the 40 participants reported on below) who appeared to specify incorrect measures, and whose responses were low-quality in general. A Sankey diagram is shown in Appendix C that relates the standards to the reported complementary measures.

We performed spot checks due to the complexity of verifying, as outsiders, if a measure was required. Some participants reported compliance standards that we could not access, such as "University IT standards" or "Other financial regulations". In other cases, the standard is vague and the determination of whether a security measure is complementary is unclear. For instance, the NIST Cybersecurity Framework [65] states in PR.AC-7 that "Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)." Therefore, we cannot effectively determine whether the security measure of multi-factor authentication is complementary to the NIST Cybersecurity Framework. We therefore trusted our expert participants to follow the guidelines of our questions and to select security measures that they perceived to be complementary.

Iterative open coding. Two researchers independently analyzed all participant open-ended responses using iterative open coding, creating a *codebook* to categorize responses based on labels [85]. For each response, coders may identify one or more applicable category labels. These categories are then aggregated into broader themes [95].

If a survey response was unclear, coders would request clarification or further information from the participant via email (if the participant had consented to additional contact within their survey response); otherwise, discard the response. Only two potential participants' responses were discarded.

To establish a baseline codebook, the two researchers jointly coded a random 10% of the data set (n=4). This established a working set of label definitions.

Next, each researcher independently coded a new subset of the data (n=5) and calculated the resulting Krippendorff's Alpha ($\alpha = 0.8594$) across the entire codebook. Krippendorff's Alpha measures inter-rater reliability — a measure of consistency among independent coders — while accounting for chance agreements [41]. An α value above 0.8 indicates high reliability [58], [62].

All disagreements during this iteration were associated with participants' use of technical jargon that could have multiple interpretations. All disagreements were fully resolved, the codebook was updated, and the researchers again independently coded a new subset of the data (n=5), with an $\alpha = 0.8229$. With two consecutive independent IRR scores above 0.8, the two researchers split the remaining 26 responses and independently coded them using a shared, collaborative codebook.

The two researchers iteratively updated the codebook as needed; when revisions were made, the researchers re-coded previously analyzed answers accordingly. We repeated this process until we resolved all disagreements and the codebook was stable. Both coders attained thematic saturation [21, pg. 113-115] in each of the five codebook subsets prior to exhausting the list of participant responses. The final codebook is given in Appendix B.

Statistical analysis. We asked two Likert-scale questions about each complementary control participants described: their satisfaction with the control and how frequently that control is assessed. Note that we use *satisfaction* as shorthand for the question wherein we asked our participants to tell us how well a certain complementary security measure worked for their organization.

To compare satisfaction across groups of controls, we used an ordinal logistic, mixed-model (random effect) regression [22]. This approach is appropriate for ordinal, non-continuous Likert data, while accounting for multiple answers from individual participants. We added the adaptive Gauss-

[1] We did not include supplementary documents associated with the specified standard.

Hermite quadrature approximation with ten quadrature points to the model for better accuracy and fitting [77]. Full details of this regression are given in Appendix VI.

To examine whether satisfaction is correlated with frequency of assessment, we used the non-parametric Kendall rank correlation coefficient, appropriate for ordinal data [1].

In both cases, we use $\alpha = 0.05$.

D. Limitations

Like all research, our work should be interpreted in the context of its limitations.

For each finding, we provide counts for the number of participants who expressed that theme (and where relevant, the number of applicable security controls) to provide context. However, it is possible that participants may have omitted mentioning a specific concept when responding to open-ended questions rather than explicitly disagreeing with the concept. Therefore, we do not use statistical hypothesis tests for these questions, nor do we intend to imply prevalence.

Our recruitment messages and consent waiver explained the purpose of the study, which may lead to a self-selection bias such that personnel most interested in the study were more likely to anonymously participate. However, this may also suggest that participants were prepared to think more critically about how compliance affects their security decisions.

All participants self-reportedly work directly with compliance standards and their experiences with compliance may reduce the possibility of demand characteristics — an experimental artifact in which participants unconsciously change their behavior to perform well within a study [73]. By allowing participants to complete anonymous online surveys, participants may be more likely to provide open-ended, candid feedback without fear of attribution or negative impacts from their employers [31].

We selected the complementary measures from a corpus of digital-security risk-mitigation literature and previous research on applied security, which might have led to a non-representative set of perceived complementary measures. We believe that we mitigated this issue by providing the opportunity for our participants to introduce unlisted measures.

In instances where participants indicated that their organization employs five or more complementary measures, we asked the participant to select five controls they were most interested in discussing. This response limit may have introduced some bias into our results. We felt this was acceptable to ensure we asked about controls for which participants were highly knowledgeable and/or most willing to provide detailed responses.

We acknowledge that long surveys can induce fatigue; however, we saw no evidence of participants' answers degrading in quality or depth in later portions of the survey. Consistent response quality may be attributed to participants' enthusiasm about the topic or that they found the topic important. Our average survey completion time is consistent with other completion times across multiple fields of study [79].

When our participants mention that they believe compliance programs are insufficient to establish baseline security, this might be for a number of reasons besides flaws in the compliance program itself. This expert opinion could vary based on the extent of the organization's implementation of the compliance program or based on the expert's experience (or lack thereof) with the compliance program's implementation. While we cannot know for certain *why* the compliance program is insufficient, our results shed light on the complementary measures that organizations do employ to address the shortcomings of compliance programs (either in the implementation or specification).

Our participants are from a variety of business sectors, and correspondingly their organizations are subject to a range of different compliance standards, adding variance to their experiences. In addition, there might be variance in the punitive factors in compliance enforcement based on the participant's industry or experience. However, our primary goal is to understand the processes by which organizations select and manage perceived complementary measures, regardless of which standards they are supplementing; as we discuss later, we find clear patterns and continuities across multiple participants' situations.

Lastly, the limitations of surveying expert participants, and of self-reported data in general, are well documented [23], [96]. Throughout this study, participant responses represent their informed, but not infallible, perceptions of security compliance. Although we manually validated many responses, we acknowledge that some participants may believe a measure is complementary when in reality it is part of the compliance program. However, given the wide variance in security implementation across various sectors, these responses represent expert insight into how compliance standards are understood and implemented in practice in complex real-world organizations. As such, the resulting insights about how and why organizations decided to add complementary measures are meaningful even if these decisions are not always correct. Quantitative and qualitative research best practices indicate that expert survey responses are reliable for identifying salient trends and reaching valid conclusions [12], [29].

IV. Results

In this section, we present the results of our study on the use of perceived complementary measures to address the shortcomings of digital security compliance programs within organizations that provide essential services. We report participant demographics, describe the ways in which participants reported that compliance programs left their organizations exposed to risk, detail the corresponding controls organizations implement as complements, and discuss the various issues that arise when implementing these perceived measures.

Throughout this section, we annotate prevalence by describing with n the number of participants that reported a particular finding and with c the number of controls to which the particular finding was reported to apply.

Metric	Count
Sector	
Consumer services	3
Education	7
Financial services	1
Government	14
Healthcare	4
Information tech	11
Job Role	
Compliance	6
Management	22
Security Analyst	6
Developer	4
Security Engineer	2
Education	
Graduate degree	27
B.S.	11
Associates	1
PNTA	1

Metric	Count
Org Size	
0–50	5
51–150	3
151–500	9
501–1000	3
1000+	20
Clientele	
1–500	6
501–5000	10
5001–10k	2
10k–100k	9
100k+	13
Experience (yrs)	
2–5	5
6–10	9
11–15	8
16–20	7
>20	11

TABLE I: Participant demographics (n=40). First column highlights represented business sectors, current work roles, and educational background. Second column describes the number of employees at participants' organizations, the size of participants' clientele, and experience levels.

A. Participants

We recruited 100 participants for this study. In total, we discarded 41 responses due to a lack of participant qualification and 19 partial responses. Among the remaining 40 participants whose responses we analyze, we achieved data saturation by the fifteenth participant. These response rates, rejection rates, and population size were consistent with previously published studies with similar methods, participant types, and goals [7], [14], [19], [91]. Table I describes our overall sample, and detailed information about each participant is provided in Appendix B.

Our study participants included security managers (e.g., CIOs, CISOs, and SOC directors), specialists in compliance and governance, developers of security software, security engineers, and security analysts. Ten participants served as senior security officials for multi-million dollar organizations with client bases of more than 100,000 customers. These organizations represented six business sectors: consumer services, education, financial services, government, healthcare, and information technology. Twenty-six participants had more than 10 years of experience. Overall, our participants averaged 15.33 years of experience ($\sigma = 7.13$) working in information technology alongside compliance standards; median experience was 15 years.

Specific experiences of our participants may vary depending on the particular compliance standards in effect and how organizations perceive the shortcomings of the standard. The top 30% of compliance standards most frequently used by our participants are: National Institute of Standards and Technology (NIST) Cybersecurity Framework (n=33), Health Insurance Portability and Accountability Act (HIPAA) (n=17), Payment Card Industry Data Security Standard (PCI DSS) (n=14), Federal Information Security Management Act (FISMA) (n=12), and at least one document from the International Organization for Standardization (ISO) (n=12). Figure 1 shows the distribution of compliance standards in greater detail. The full list is reported in Appendix C.

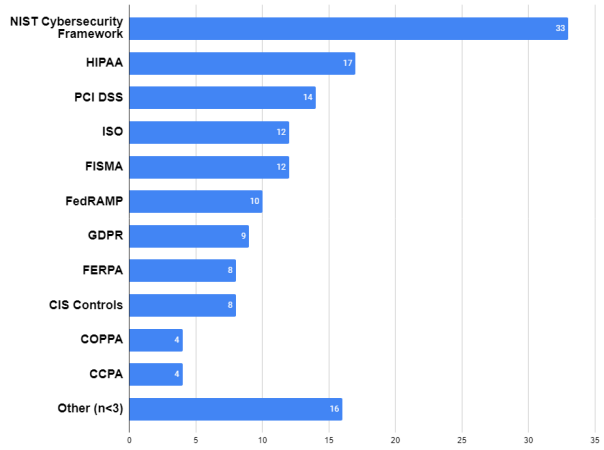

Fig. 1: Distribution of standards used by participants. We aggregate standards used by three or fewer participants under "Other." A complete list of standards and acronyms is given in Appendix C.

B. Compliance is insufficient

As discussed in Section II, many previous works detail complications with organizations implementing compliance programs. The following results provide further evidence from multiple business sectors that compliance programs are often perceived to be insufficient for establishing baseline levels of security against common threats.

Overall, only 10 of 40 participants felt that their organizations were adequately protected from most threats by compliance programs. Seven participants were unsure about the protection provided, and 23 indicated that compliance insufficiently protected their organizations and systems. Participant P17 stated that compliance failed to protect their organization from "nearly all threats. Compliance is so high-level and abstract it is nothing more than a 'CYA' [cover your ass] effort to make leaders invest in security." Similar sentiment was shared by other participants, with 21 participants indicating that compliance was in some ways disconnected from addressing realistic threats faced by their respective organizations. Of note, this negative sentiment was shared by a majority of participants across all business sectors except for finance. Participant P11 — our only participant from the finance sector — offered their view of why they believed compliance standards were sufficient:

> *"Compliance standards are sufficient because there are SO many. The financial industry is literally choked with compliance standards. The real issue is whether the financial companies can implement those standards with enough flexibility to keep up*

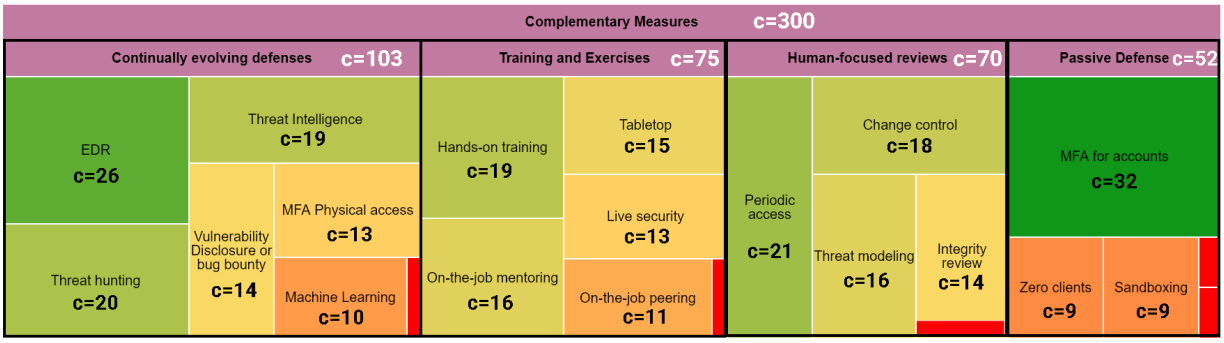

Fig. 2: Distribution of complementary measures used by participants across four categories of controls. Block size and color indicate prevalence, with MFA reported as the most-used complementary measure (c=32) and five different controls mentioned only once each.

> *with the changing threats, and that will depend upon the organization." (P11)*

In total, 37 participants indicated that they employed supplemental security controls (not required by compliance) to mitigate unaddressed threats. Here, seven of the ten participants who previously indicated that compliance was sufficient for their organization explained that their organization faced specific threats and that compliance standards were too abstract to account for these threats. Participant P28 summarized the sentiment of these 37 participants, stating that:

> *"[Compliance is] a baseline to ensure you're thinking about controls in many domains at a minimal/moderate [level]. Very often even the baseline controls are not even implemented well to begin with. [Compliance is] a starting point not a destination." (P28)*

We then asked participants what specific threats were unaddressed by compliance programs, as implemented in their organizations. We categorized these responses, and the largest category was emerging threats (n=10). Participant P19 stated that "published standards do not have sufficient flexibility and adaptability to changing threat types and methodologies. They serve only to resolve known or historic issues." These attitudes align well with findings in prior work. Compliance standards vary in how often they are updated, but nearly all fail to provide feedback opportunities after major version releases [83], and malicious exploit development surpasses the ability of compliance authors to modernize standards [2].

Twelve participants indicated that compliance fails against sophisticated attacks; three participants from the government sector indicated that nation-state actors are not deterred by compliance. P37 reported that compliance programs "only protect against 80% of threats (i.e. the low hanging fruit)," suggesting organizations are exposed to moderate and sophisticated attacks. Compliance was particularly concerning to P04: "we are a high profile target via name and reputation," and because of that compliance leaves them "vulnerable to attacks." An analysis of nation-state attack methods again highlights the gap between the speed and complexity of their attacks and the efficacy of compliance programs [26].

Seven participants stated that compliance does not adequately protect organizations from insider threats (n=7). This aligns with prior work suggesting insider threats possess privileged insight that allows them to bypass superficially-implemented defenses required by compliance [25], [47], [48], [90].

Other threats perceived to be uncovered by compliance but mentioned less frequently were: relying on self-reporting for security issues (n=1), denial of service attacks (n=1), phishing attempts (n=1), and untrained compliance auditors (n=1) who require modifications to security that have "no traceability to mission/business requirements."

To proactively defend their organizations from these perceived unaddressed threats, our 40 participants reported that they collectively employ 300 complementary measures to augment compliance. (As detailed in Section III-A, participants were asked to select all applicable complementary measures from a predetermined list of 18, and offered space to report up to five additional measures under 'other.') After deduplicating the 'other' responses, we obtained a final list of 23 unique complementary measures that we bin within four different categories: (1) training and exercises, (2) human-focused reviews, (3) passive defense, and (4) continually evolving defenses. *Training and exercises* involve employees gaining exposure to defensive techniques interactively through hands-on training (n=19), formal mentorship programs (n=16), and tabletop "talk-through" exercises (n=15). *Human-focused reviews* are triggered by events and require human-in-the-loop interactions. Examples include change control boards that review and approve changes to digital systems (n=18), periodic account access reviews (n=21), or proactively assessing risks and developing mitigation strategies through threat modeling (n=16). *Passive defenses* involve technologies that infrequently require human interaction; examples include multi-factor authentication (MFA) for account protection (n=32) and zero-client hosts that provide users with new, pristine workstations for every use (n=9). Lastly, *continually evolving defenses*

require extensive human-in-the-loop involvement to actively reduce threat exposure. The most used continually evolving defenses include endpoint detection and response tools (EDR) (n=26), which focus on detecting and investigating suspicious activities on endpoint systems such as workstations; implementing physical access controls (n=13) due to both physical and digital organizational changes (e.g., office swaps, new server rooms, or influx in hiring); threat hunting (n=20), where defenders attempt to identify and defeat known or unknown threats that have already bypassed existing security; and threat intelligence (n=19), information feeds that inform defenders about emerging threats and recent events.

The full list of reported controls is included in Appendix D and illustrated in Figure 2.

C. Going beyond compliance

Given that participants report compliance programs insufficiently address threats, we next explore how and why organizations choose to complement compliance controls. More than any other reported reason, we find that compliant organizations implement perceived complementary measures after they encounter a security incident. Other key factors include reducing overall costs and gaining better insight into network activity. Overall, we find that participants generally have a positive outlook on perceived complementary measures and the benefits they provide their respective organizations.

Security incidents lead organizations to adopt new controls. While we did not specifically ask if participants' organizations were the victims of a security breach, many offered that past incidents were a driving factor for implementing complementary measures (n=21, c=40). These incidents exposed security gaps not previously addressed by compliance programs (at least as implemented at the organization), compelling organizations to take action. This reinforces previous research that organizations make decisions based on risk exposure [43]. Participant P36 offered insight into their incident:

> *"We had a public data breach... a misconfigured database I think? There was immediate pressure to prove to higher [management] that we were doing something to make sure it didn't happen again in the future." (P36)*

Security incidents at already-compliant organizations inherently demonstrate that baseline compliance, as implemented in practice, provides insufficient protection. To help mend security gaps exposed by incidents, 16 participants implemented continually evolving defenses (MFA, c=10), 14 implemented passive defenses (EDR, c=4), five implemented human-focused reviews (account access review, c=4), and five implemented training and exercises to help mitigate future incidents (tabletop, c=3). P27, a manager in healthcare, explained their reasoning for moving to EDR after suffering a breach despite deploying compliance-mandated anti-virus:

> *"AV is just flatly insufficient. Attackers often use "living off the land" tools, [EDR] helps to detect and prevent normal tools used in bad ways." (P27)*

Participant P29 reported that their organization "does not embrace complementary measures, which has led to several incidents," resulting in adoption of complementary defenses after the incidents. Participants (n=2) touched on the reactive inclinations of their respective organizations, with P23 stating that their organization waits until "incidents or threats appear, [then] prioritization changes."

We note that even though organizations implemented perceived complementary measures after an incident, not all of the new controls were directly related to the previous incident. By implementing new complementary measures after incidents — whether or not related to the original problem — security teams signaled to their organization that they were dedicating resources (e.g., money and personnel) to improve overall security (n=3).

In addition to actual incidents, red teams — digital security professionals who act as an adversary to assess networks and systems — have a similar impact on implementing complementary measures. This make sense, as red teams are essentially controlled incidents. Three participants reported that they are more likely to initiate complementary improvements to compliance programs after a penetration test. This aligns with prior work suggesting that formal vulnerability reports can have a large impact [5], [97].

Organizations seek controls that reduce costs. Twenty participants indicated that budgetary constraints were key factors in deciding to implement controls not perceived as required by compliance. Five of these 20 said that if they were to complement compliance, the new complementary measures would need to reduce task completion times and overall costs. Participant P15 seeks "potential for asymmetric gains – [controls that let] a human do the same work 10x faster, or achieving quality/thoroughness that would be unachievable by any number of humans." P40 looks for automation and "time-savings by reducing staff labor hours." Business re-engineering researchers highlight these concepts as best practices, choosing to optimize the total effectiveness of employees rather than downsizing [38]. Similarly, P14 stated that some solutions "may be limiting if [they] are too time or labor intensive," and their organization will avoid hiring new personnel to extend security beyond compliance.

When advocating for solutions that augment compliance, P09 and P10 had to appeal to senior management in terms of return on investment and getting the most "bang-for-buck." However, Participant P24 indicates this is not always the case:

> *"Larger-budgeted enterprises can initiate security decisions at various levels based on what is needed, [while] organizations with low funding need to invest time into basic measures such as routine reviews of patch management and privileged account access or other inexpensive proactive measures like tabletop reviews of incident response scenarios and in-person user training (that is actually engaging and informative)." (P24)*

The notion that larger-budgeted organizations permit lower echelons of decision makers to test various perceived complementary controls is corroborated by P33, who said technicians at their organization are permitted to "[perform] pilots to determine if solutions were right for the need."

Machine learning (ML) (n=3), on-the-job mentorship (n=4), and hands-on training (n=3) were other controls perceived as not required by compliance that participants selected to address skill shortages and overcome hiring limitations. P37, when discussing machine learning, stated that "humans do not scale and are in short supply, and security data is growing exponentially." P26 similarly reported that they use ML because there is "not enough staff to keep up with human analysis" required to monitor compliance-mandated security platforms. P08 uses on-the-job mentoring at their organization because many of their employees are entry-level and have little to no compliance experience; they said it is in their organization's best interest to "mentor our young employees to ensure they will be vigilant in the requirements of compliance and overall site security."

Some participants (n=2) cautioned about letting budgetary constraints drive security decisions when adopting perceived complementary measures. P16 lamented their organization's decision to adopt EDR technologies: "we bought trash solutions from the lowest bidder."

There are unspoken benefits to having an incident. Budgeting constraints not only affect the adoption of complementary measures, but in some cases create perverse incentives. Participant P31 stated that the occurrence of incidents actually helps security teams advocate for a higher budget prioritization. Participants P02 and P27 similarly discuss an often unspoken trade-off between security and budgeting. "If you have perfect security, you obviously don't need your whole budget so let's give it to someone else that needs things more," stated P02. For P27, "security breaches are a strong, public-facing signal that something is wrong and resources need to be applied to fix it. Embarrassment will continue until it is fixed." These comments fit with prior observations that security practitioners constantly compete for a slice of their organization's overall budget and must consistently demonstrate a return on security investments [6], [81]. This reality may motivate security teams to roll out complementary measures over time, continually demonstrating to budget-controlling officials a need for growth beyond baseline compliance security.

Compliance measures do not provide requisite network insight. Participants reported that they need complementary measures to assist with decision-making because the insights provided by compliance controls were insufficient; this accords with findings from Kokulu et al. [54]. For example, participants reported that in their experience standard compliance controls lacked visibility into network traffic flows and user activities (c=35). Participant P36 explained one point of frustration with the NIST Cybersecurity Framework, General Data Protection Regulation, California Consumer Privacy Act, and other financial standards:

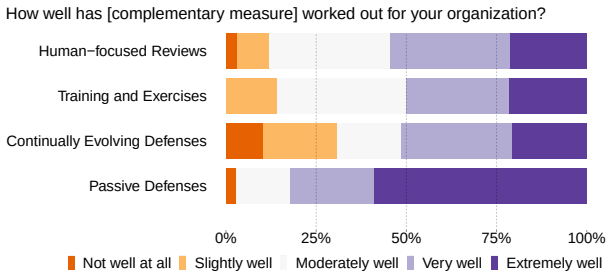

Fig. 3: Participants' satisfaction with complementary measures, per labeled category.

> *"It's impossible to defend a network where I can't tell you how many workstations are attached. How many belong to us? We can't connect what users are visiting what sites, so how can I tell who downloaded malware?" (P36)*

Complementary measures, therefore, are often intended to provide improved understanding, allowing managers and technicians to make better defensive decisions. In fact, participants (c=36) indicated they employed perceived complementary measures to enhance the effectiveness of other digital defenses, some of which were mandated by compliance programs. Participant P28 uses EDR to support compliance-mandated anti-virus and post-incident reporting:

> *"Simple signature based AV is dead. EDR tooling gives a much richer vision of process execution that is valuable for both detection and forensics." (P28)*

Participant P32 decided to use MFA to complement their password policies and provide "an additional level of security that assists in reducing the occurrence of gaining access to critical systems."

Organizations rely on external recommendations. Sixteen participants indicated that they rely heavily on the advice of experts from outside their organization or on external marketing to make security decisions not required by compliance (n=16). Four participants stated that the reputation of external experts plays a role in whether they adopt the recommendation or not (n=4). Participant P37 spends "a good bit of time finding vendors with truly useful technologies and not just well-marketed snake oil" when following up on external recommendations.

Executive-level decisions made in isolation are seen as harmful. Several participants reported that executives within organizations, some without technology backgrounds, make decisions to complement compliance without input from their technicians (n=5). This led to frustrations within the organization, with P22 feeling that many decisions about perceived complementary measures were based on "political pressure" to partner with a particular vendor, or "based entirely on [the] whim of [the] CIO" without an operational need or threat model to justify the decisions. Similarly, P23 said complementary measures such as threat intelligence are "often

Control Category	Odds Ratio	Conf. Int.	p-value
Passive Defenses (c=52)	–	–	–
Training and Exer. (c=75)	0.16	[0.06, 0.47]	0.0008*
Human-focused Rev. (c=70)	0.19	[0.07, 0.52]	0.0012*
Cont. Evolving Def. (c=103)	0.11	[0.04, 0.29]	<.0001*

*Statistically significant

TABLE II: Summary of regression modeling participant satisfaction levels as a function of control category. Results demonstrate that passive defenses were preferred over other complementary measure categories

Proactive Control Group	τ	Correlation	p-value
Passive Defense	0.08	Weak (+)	0.6057
Training and Exer.	0.21	Weak (+)	0.2002
Human-focused Rev.	0.23	Weak (+)	0.1148
Cont. Evolving Def.	0.26	Weak (+)	0.0137*

*Statistically significant

TABLE III: Ordinal association between participants' satisfaction level with each control and their reported assessment frequency.

seen as a 'check the block' [box] function for executives to claim they are doing things" to defend the network from threats perceived to be uncovered by compliance — often without a clear understanding of the expected outcomes.

P06 warned about the misalignment of resources based on these types of decisions, recalling a time when their organization chose to buy a new security platform rather than exploring why their existing tools failed: "Interesting technology is great but if it doesn't address a critical need, we end up working on less important needs." P30 stated, "once it is determined what product is wanted [by managers], security is brought in to assess [the solution], which is slightly backwards." P22 made a similar point discussing their company's implementation of EDR: "It was a dumpster fire" because the purchased solution only worked on a fraction of the company's systems.

Bottom-up recommendations to managers shaped implementation strategies. Eight participants who were managers said they implemented perceived complementary measures based on technician-identified needs to address security gaps that remain despite compliance standards. In total, managers implemented 26 controls based on bottom-up suggestions from security employees. Managers said they adopted these controls to reduce the time required to accomplish tasks, improve overall performance, and enhance shared ownership of the security situation.

Organizations generally have a positive outlook on perceived complementary measures. Thirty participants indicated that their complementary measures had valuable outcomes for their organizations. More specifically, seven participants reported that their security investments made their organization's overall attack surfaces smaller. For example, P03 stated that their use of vulnerability disclosure programs, threat hunting, and live security exercises identified "numerous gaps that scoped tests required annually did not find." Three participants stated that MFA counterbalances weak password policies, such as those from the Internal Revenue Service [83]. P13 enjoys not needing "to remember complex passwords, just need pin" for an MFA smart card, while P15 stated MFA removes attack vectors associated with passwords like pass-the-hash [70] or hash cracking.

We also determined, using the quantitative analysis methods discussed in Section III-C, that participants preferred perceived complementary measures that did not require much effort to maintain. As depicted in Figure 3, the passive defense category — measures that require minimal human-in-the-loop interaction — had the highest overall sentiment scores (averaging 4.35 out of 5, $\sigma = 0.95$) and served as the baseline for our ordinal logistic regression. Participants, as shown in Table II, were significantly more satisfied with passive defenses than with any other category of perceived complementary controls. In fact, the point estimates for the odds ratios indicate that participants were only 10-20% as likely to express higher satisfaction in the other categories as they were for passive defenses.

Additionally, we find that participants are more satisfied with perceived complementary measures when they are assessed frequently. Using Kendall's τ (Table III), we find a significant but weak positive correlation — indicating that satisfaction is higher when assessments are more frequent — for continually evolving defenses. Similar correlations are observed for the other three categories, but these trends do not reach statistical significance.

D. Additional measures are not a panacea

Despite participants generally having a favorable outlook, participants also warn that perceived complementary measures are not one-size-fits-all. In this section, we highlight a range of challenges and complications associated with adoption of perceived complementary measures.

Positive benefits come at a cost. Participants' efforts to fix security gaps perceived to be uncovered by compliance programs came at a cost to the organization — consuming time, money, or additional human capital (n=37).

As one example of such a trade-off, training and exercises invest in the technical competency of the workforce but also require employees to spend time away from their primary jobs. P36, for example, noted this challenge: "We usually see instant benefits after training. ... We typically cycle people through training in small groups so the overall security team still functions." P02 similarly warned about significant planning obligations leading up to exercises: "two planners from our SOC participated in [about] 100 hours of planning for 12 hours of training." Mentorship programs similarly improve security posture at the cost of additional person-hours. P35 praised that these programs "Raise talent level. Strengthen internal rapport, structure, work product[s]. Shorten responses and knowledge transfer [during] emergencies." However, P36 cautioned that mentorship requires effort and planning: "If you don't set aside

time for it, it isn't happening. But if you set aside time for it, plan for what isn't being done during that time."

In another example of trade-offs associated with complementary measures, participants noted that human-focused reviews require organizations to trade speed for enhanced security. Participant P12 stated change control in their organization "slowed down change but increased reliability"; P20 made similar comments. According to P35, human-focused reviews in general should have mechanisms for "temporarily breaking beaucracy" under urgent circumstances and should optimize everyday timelines when possible — factors often not accounted for in compliance programs [83].

Participants also reported usability concerns with passive defenses (n=11) that diverted a significant amount of time away from other security tasks. MFA, the most commonly employed complementary measure, also had the most usability concerns. Six participants (n=6), representing each surveyed business sector, stated the security benefits of MFA came with usability challenges including lost smart cards, the migration of soft tokens to new phones, and lost hardware tokens (thus, corroborating complications discussed by Neware et al. [66]). Similarly, P17 and P19 highlight security-usability trade-offs in the use of zero-client systems, which have no host operating system or storage and instead serve a clean virtual desktop that is erased after each use. Zero-client systems can create an "easy to establish 'gold' standard [that can be] updated as needed," (P17), but the lack of "persistence or personalization of the operating environment" (P19) can inhibit required work.

P25 indicated that some organizations implement controls without thinking about the "next step" of usability. For example, with sandboxing, their organization suffers from usability "challenges [in] getting samples from the live environment to the [forensics] sandbox in a safe manner." Mapping out end-to-end use cases may provide a benefit in adopting new technologies.

P21 noted trade-offs in implementing end-to-end encryption, a passive defense measure: the security and privacy benefits "must be balanced with needs for logging, troubleshooting and forensics," including creating challenges during incident investigation.

Complementary measures should not conflict with compliance. While complementary measures are intended to augment compliance controls, they are not always fully compatible with existing compliance standards as implemented. Participants reported that for 46 implemented complementary measures (c=30 from the government sector), there was no check for compatibility with compliance. P21's comment about end-to-end encryption, for example, noted that this complementary measure may inhibit collection of logging data that is required under some compliance regimes.

Sometimes incompatibilities between compliance controls and perceived complementary measures are more nuanced: P19 claimed that tabletop exercises do not have anything to do with compliance. However, considering compliance while executing tabletop exercises may help ensure participants practice compliant actions such as protecting sensitive information from improper disclosure [52], [88].

However, some participants did report that their organizations carefully consider compatibility when implementing perceived complementary measures. Participant P28 described their organization's methodical selection process for ensuring compatibility with existing programs. Five participants reported that they looked specifically for MFA solutions marketed as "compliance-ready" before buying, a trend previously identified by Julisch et al. [53]. When incompatible issues arise, P40 stated they "encourage self-report[ing]" when compliance may have been violated, which runs contrary to many zero-tolerance policies that enact financial sanctions for all infractions [68].

Poorly-managed measures provide reduced benefit. Eleven participants reported instances of perceived complementary measures that provided reduced or even no benefit when poorly managed within their organization (n=11). Participant P27 indicated that their organization paid "six figures" for intrusion detection systems that remained in storage and were never set up (a pilot participant also reported a similar situation).

P25 said of their vulnerability disclosure program: "developing the program was great... informing everyone of its existence has been a struggle." As a result, few vulnerabilities have been discovered or remediated. In contrast, P24 said marketing for their disclosure program yielded high participation with "over 100 vulnerabilities identified" despite their organization being at least facially compliant. However, uncovering vulnerabilities using a disclosure program may still not be sufficient if there is no plan in place to manage them: P01's organization had issues reported, but they "go into a backlog where they don't get remediated." This finding accords with other examples of mismanagement of vulnerability disclosure programs [5].

Three participants reported financial losses when implementing threat hunting because their organization hired unqualified employees and did not adequately understand their own networks (n=3). Participant P17 stated that it "turns out finding unknown threats from systems that aren't baselined is hard." Since their organization's compliance programs did not require up-to-date documentation (such as network maps), the organization paid hunters to sift through a network that its own administrators did not understand. P16 similarly said, "we go where we fear the threats are, rather than where they actually are," that their organization often "ignores their [threat hunters'] findings," and "fails to train, equip, or employ [threat hunters] properly." P12 was "not convinced [their organization] brought in the right hunters." As with vulnerability disclosure programs, threat hunting measures may fail if the organization is not prepared to use them effectively.

Three participants emphasized the importance of managing routine human-focused reviews, which is a known weakness in compliance standards themselves [83]. P12 complained that their organization does not perform account-access reviews as frequently as their internal policy requires; P24 offered that ac-

cess reviews "don't work well unless you commit to a routine schedule, and make time to conduct the review." Additionally, P24 warned that change-control review boards "can become extremely bureaucratic and provide the opportunity for non-decision makers to become gatekeepers that slow down the process." Of note, P24 indicated that missed change-control board response deadlines significantly delayed approvals for a new security platform. These comments suggest that perceived complementary measures sometimes reify problems with baseline standards (as implemented) rather than alleviating them.

Keeping complementary measures relevant is difficult. A key weakness of compliance is staying up to date with current technology and best practices [83], but perceived complementary measures often struggle with the same challenge. In total, 13 participants warned about the difficulties of keeping complementary measures relevant.

Participants argued that organizations should ensure training and exercises are congruent with the current threat landscape to maximize effectiveness (n=3). P16, expressing their frustrations with live security training, stated "We let morons design them. They are not grounded in reality and are at least five years behind [current] threats."

Information does not equate to actionable intelligence. Ten participants reported that their organizations struggle to act on the information gained from implemented complementary measures (n=10), with four complaints specifically focused on threat intelligence (n=4).

Participant P16 lamented "information overload," indicating that their organization's implementation of threat intelligence "is neither timely, nor actionable. It is designed to give the illusion of insight, without forcing meaningful change." P17's organization likewise "struggles to quickly integrate paid vendor intel into our analysis systems," and similarly, P13 has "yet to see any complementary measures taken based on threat intel." P19 mentions that information overload of this kind can delay responses: "current models for developing and evaluating threat intelligence have been successful in timely development of information but have not provided sufficient time to mitigate across the domain." This sentiment corroborates prior findings that return-on-investment for threat intelligence varies [61].

Outside of threat intelligence, P24 warns that information is not sufficient when it is not used properly: "Logs from agents may not be collected properly or reviewed by personnel with the proper training."

V. Discussion

In this paper, we examine how U.S. organizations supplement perceived shortcomings of their digital-security compliance programs. We find that security professionals rely on a wide range of perceived complementary measures to address the threats their organizations face. While many security professionals described their experiences with effective methods of complementing compliance, they also reported numerous inefficiencies and challenges that can occur when implementing perceived complementary measures.

Based on these results, we make some recommendations for improving both compliance standards themselves and the ways that organizations try to supplement them. These advice, which should be interpreted in the context of the limitations discussion in Section III-D, are designed to support practitioners who think their compliance programs are insufficient, regardless of whether the shortcoming originates in the standard itself or in the organization's implementation of it.

Integrating complementary measures into compliance. Our work echoes others in finding that compliance standards are perceived as insufficient on their own, leading many organizations to introduce complementary measures.

Section IV-C shows that, in many cases, these perceived complementary measures can effectively reduce organizations' attack surface. Complementary measures that gain significant adoption and acceptance are promising candidates for incorporation back into revised compliance standards as requirements. Standards authors should formalize mechanisms for audited organizations to provide feedback about the complementary measures they are using, why they are using them, and how well they are working. This feedback would enable standards authors to observe trends at scale and identify generalizable benefits for participating organizations, while still taking into account concerns about overwhelming smaller organizations with more requirements before deciding what to add [9].

Moreover, such feedback could help standards authors identify instances where multiple organizations are misinterpreting requirements and incorrectly perceiving some controls as complementary. This would provide an opportunity for standards bodies to make clarifications that would improve compliance fidelity overall.

Documenting complementary measures' use cases also provides an opportunity to assist with compliance compatibility. Specifically, standards can be written to directly recognize that going beyond baseline compliance is often perceived as desirable or even necessary. Here, standards authors can create provisions that require organizations to document and carefully manage any perceived complementary measures they implement, without explicitly prescribing what those measures might be, and without simply expanding the standard to include all measures that might be useful, which would quickly become unwieldy. This would be similar to guidelines provided by the U.S. Food and Drug Administration [32].

In particular, standards could require that organizations (and therefore auditors) ensure: (1) a holistic management program is in place, (2) any perceived complementary measures that are implemented are routinely monitored and/or adjusted, (3) employees are provided with requisite training to understand and implement any perceived complementary measures that are adopted, and (4) incidents related to any implemented perceived complementary measures are reported and remediated. This approach would allow organizations to decide whether the need for any particular perceived complementary measure is sufficient to be worth the cost of properly managing it. Further, this approach could build in mechanisms for auditors

to help organizations recognize when what they perceive as complementary measures should instead be treated as included portions of the compliance program.

Recommendations must come from reputable sources. Section IV-C shows that organizations frequently rely on advice from security tool vendors or external experts such as red teams when deciding to implement perceived complementary measures. But — as this study shows — these sources may not always lead to security benefits: organizations are left to sift through vendors' "snake oil" solutions, and some implementation strategies fail to address actual security problems. The security operations community could develop a centralized clearinghouse to aggregate data about the efficacy of complementary measures, to help organizations make better implementation decisions and understand what worked well (or poorly) before investing. Anonymizing "success stories" and making them publicly available may also help overcome common security secrecy [100].

Keeping pace with evolving threats and technologies. Compliance programs struggle with agility and responsiveness to evolving threats and technologies — often driving organizations to implement complementary measures. Efforts to make compliance standards more responsive could reduce the need for perceived complementary measures; but, as others have noted, rapid compliance changes may have negative organizational impacts, particular in organizations with fewer resources [63], [83].

Our findings suggest that some perceived complementary measures suffer similarly from insufficient timeliness. When not implemented carefully, use of complementary measures can move the problem of outdated solutions to a new arena, outside compliance standards but still creating risks. It is important for decision-makers to understand that responsiveness is a systemic issue and compliance is not solely to blame.

Organizational factors are critically important. Although our participants generally believe that complementary measures are helpful, when these measures are not planned for, they may fail to fill security gaps or induce new problems. Organizations must choose their perceived complementary measures carefully to align with actual need, plan for end-to-end use cases prior to implementation, and routinely revisit them to ensure they remain up to date and correct.

Here, we offer a slight modification to an old adage: if a thing is worth doing, it is worth doing well *and routinely*. Throughout Section IV-D, we find instances of organizations investing in perceived complementary measures but not following through on required security tasks, such as buying new security platforms and failing to actually use them, missing critical security events because analysts failed to check logs, or delaying the approval of a much-needed security platform because a change-review board missed their response deadline. Routine checkups, reassessments, and deadlines can help eliminate these problems.

Our participants report that organizations sometimes choose to spend money on new perceived complementary controls that may or may not be relevant, rather than understand why their current security strategy failed. Instead of triaging a problem and potentially identifying a training or configuration deficiency, purchasing new equipment or services is sometimes seen as a better demonstration that the security team is "doing something" about the issue. Organizations should consider a broader range of possible mediations and optimize complementary measures against actual observed threats or gaps.

Lastly, organizations need to have support in place prior to deploying complementary measures. Participants reported instances of perceived complementary measures generating information (e.g., vulnerability disclosure, threat intelligence, or security logs) without a plan for how to process the data. Similarly, participants reported cases where training and skills mismatches inhibit the efficacy of complementary measures such as threat hunting. Prior work suggests that investing in employee training and planning carefully for end-to-end use cases could help to avoid these issues [5], [30], [34], [40], [51], [54], [82], [86], [87]. As with agility, management problems related to security controls are systemic and cannot be blamed solely on challenges with compliance standards themselves.

Future work: A deeper look. Our single participant from the financial sector believed that finance-related standards provided sufficient threat coverage, in part because of the sheer quantity of applicable standards. While we obviously cannot generalize from one participant, we did find their confidence notable. Future research could specifically explore the efficacy of financial-sector compliance programs, to understand whether this view is widely held. If so, researchers could further investigate which features of financial-sector compliance make it more effective, and to what extent these features could be extended to other sectors.

Additionally, our study focused on U.S.based organizations, participants, and compliance standards. Future studies should attempt to determine if findings from U.S. organizations generalize to organizations in various global markets.

VI. Conclusion

While compliance is a critical aspect of an organization's digital security, it is far from a panacea. Organizations consistently identify gaps in the security guarantees they obtain from compliance — gaps that may arise from problems with the standards themselves, or from local implementations of them. Regardless of their source, these gaps expose the organization and its users to risk of an attack. Thus, organizations implement what they believe to be complementary measures beyond compliance; while these efforts offer benefits, they also often face organizational inertia and risk. We hope that our results will spur the development of improved compliance mandates that acknowledge that organizations will often want to implement complementary measures, and that provide guidance for accommodating these dynamic organizational needs while maintaining oversight of the overall security posture.

ACKNOWLEDGMENTS

The authors would like to thank all study participants for their time and invaluable contribution.

This work was supported in part by a grant from the Defense Advanced Research Projects Agency (DARPA) FA875019C0003. The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.

REFERENCES

[1] H. Abdi, "The kendall rank correlation coefficient," *Encyclopedia of Measurement and Statistics*, 2007.

[2] L. Ablon and T. Bogart, "Zero days, thousands of nights," 2017.

[3] S. Agarwal, S. Steyskal, F. Antunovic, and S. Kirrane, "Legislative compliance assessment: framework, model and GDPR instantiation," in *Annual Privacy Forum (APF)*. Springer, 2018.

[4] A. Aidman, "Children's online privacy." *Educational Leadership*, vol. 58, no. 2, pp. 46–47, 2000.

[5] N. Alomar, P. Wijesekera, E. Qiu, and S. Egelman, "You've got your nice list of bugs, now what? Vulnerability discovery and management processes in the wild," in *Symposium on Usable Privacy and Security (SOUPS)*, 2020.

[6] E. E. Anderson and J. Choobineh, "Enterprise information security strategies," *Computers & Security*, vol. 27, no. 1-2, pp. 22–29, 2008.

[7] D. Andrews, B. Nonnecke, and J. Preece, "Electronic survey methodology: A case study in reaching hard-to-involve internet users," *International Journal of Human-Computer Interaction*, vol. 16, no. 2, pp. 185–210, 2003.

[8] D. L. Anthony, A. Appari, and M. E. Johnson, "Institutionalizing HIPAA compliance: Organizations and competing logics in US health care," *Journal of Health and Social Behavior*, vol. 55, no. 1, pp. 108–124, 2014.

[9] A. Arora, R. Telang, and H. Xu, "Optimal policy for software vulnerability disclosure," *Management Science*, vol. 54, no. 4, pp. 642–656, 2008.

[10] H. Assal and S. Chiasson, "Motivations and amotivations for software security," in *SOUPS Workshop on Security Information Workers (WSIW). USENIX Association*, 2018.

[11] ——, "Security in the software development lifecycle," in *Symposium on Usable Privacy and Security (SOUPS)*, 2018, pp. 281–296.

[12] D. Austen-Smith and J. S. Banks, "Information aggregation, rationality, and the condorcet jury theorem," *American Political Science Review*, vol. 90, no. 1, pp. 34–45, 1996.

[13] R. Bernard, "Information lifecycle security risk assessment: A tool for closing security gaps," *Computers & Security*, vol. 26, no. 1, pp. 26–30, 2007.

[14] D. Botta, R. Werlinger, A. Gagné, K. Beznosov, L. Iverson, S. Fels, and B. Fisher, "Towards understanding IT security professionals and their tools," in *Symposium on Usable Privacy and Security (SOUPS)*, 2007.

[15] T. D. Breaux and A. I. Antón, "Mining rule semantics to understand legislative compliance," in *ACM Workshop on Privacy in the Electronic Society*, 2005.

[16] ——, "Analyzing regulatory rules for privacy and security requirements," *IEEE Transactions on Software Engineering*, vol. 34, no. 1, pp. 5–20, 2008.

[17] T. D. Breaux and D. G. Gordon, "Regulatory requirements traceability and analysis using semi-formal specifications," in *International Requirements Engineering Conference (RE)*, 2013.

[18] T. D. Breaux, M. W. Vail, and A. I. Anton, "Towards regulatory compliance: Extracting rights and obligations to align requirements with regulations," in *International Requirements Engineering Conference (RE)*, 2006.

[19] K. Caine, "Local standards for sample size at CHI," in *Conference on Human Factors in Computing Systems (CHI)*, 2016.

[20] Center for Internet Security Controls, "Center for Internet Security Controls Downloads," 2021. [Online]. Available: https://learn.cisecurity.org/cis-controls-download

[21] K. Charmaz, "Constructing grounded theory: A practical guide through qualitative analysis," Sage Publications, 2006.

[22] R. H. B. Christensen and P. B. Brockhoff, "Analysis of sensory ratings data with cumulative link models," *Journal de la Société Française de Statistique*, vol. 154, no. 3, pp. 58–79, 2013.

[23] D. Christopoulos, "Peer esteem snowballing: A methodology for expert surveys," in *Eurostat conference for new techniques and technologies for statistics*, 2009, pp. 171–179.

[24] R. Clark, "Compliance != security (except when it might be)," in *Enigma*. USENIX Association, 2018. [Online]. Available: https://www.usenix.org/node/208142

[25] C. Colwill, "Human factors in information security: The insider threat–who can you trust these days?" *Information Security Technical Report*, vol. 14, no. 4, pp. 186–196, 2009.

[26] CrowdStrike, "Crowdstrike global threat report: Adversary tradecraft and the importance of speed," 2019. [Online]. Available: https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2019GlobalThreatReport.pdf

[27] L. de la Torre, "A guide to the california consumer privacy act of 2018," *SSRN 3275571*, 2018.

[28] C. Dietrich, K. Krombholz, K. Borgolte, and T. Fiebig, "Investigating system operators' perspective on security misconfigurations," in *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2018.

[29] H. Dorussen, H. Lenz, and S. Blavoukos, "Assessing the reliability and validity of expert interviews," *European Union Politics*, 2005.

[30] J. Dykstra and C. L. Paul, "Cyber operations stress survey (COSS): Studying fatigue, frustration, and cognitive workload in cybersecurity operations," in *USENIX Workshop on Cyber Security Experimentation and Test (CSET)*, 2018.

[31] J. E. Edwards, T. Edwards, M. D. Thomas, P. Rosenfeld, and S. Booth-Kewley, "How to conduct organizational surveys: A step-by-step guide," Sage Publications, 1997.

[32] Food and Drug Administration, "FDA guidance documents," October 2020. [Online]. Available: https://www.fda.gov/regulatory-information/search-fda-guidance-documents

[33] B. G. Fry, M. Therese, B. Weckmueller *et al.*, "The family educational rights and privacy act of 1974," *Student records management: A handbook*, 1997.

[34] S. M. Furnell, N. Clarke, R. Werlinger, K. Muldner, K. Hawkey, and K. Beznosov, "Preparation, detection, and analysis: The diagnostic work of it security incident response," *Information Management & Computer Security*, vol. 18, no. 1, pp. 26–42, 2010.

[35] M. Galesic and M. Bosnjak, "Effects of questionnaire length on participation and indicators of response quality in a web survey," *Public Opinion Quarterly*, vol. 73, no. 2, pp. 349–360, 2009.

[36] General Services Administration, "FedRAMP moderate security controls." [Online]. Available: https://www.fedramp.gov/assets/resources/documents/FedRAMP_Moderate_Security_Controls.xlsx

[37] C. F. Goodwin and J. P. Nicholas, "Developing a national strategy for cybersecurity," *Foundation for Security Growth and Innovation*, 2013.

[38] V. Grover, "From business reengineering to business process change management: A longitudinal study of trends and practices," *IEEE Transactions on Engineering Management*, vol. 46, no. 1, pp. 36–46, 1999.

[39] J. Harmening, "Security management systems," in *Computer and Information Security Handbook*. Elsevier, 2017.

[40] W. U. Hassan, S. Guo, D. Li, Z. Chen, K. Jee, Z. Li, and A. Bates, "NoDoze: Combatting threat alert fatigue with automated provenance triage," in *Network and Distributed Systems Security Symposium (NDSS)*, 2019.

[41] A. F. Hayes and K. Krippendorff, "Answering the call for a standard reliability measure for coding data," *Communication Methods and Measures*, 2007. [Online]. Available: http://dx.doi.org/10.1080/19312450709336664

[42] Q. Hu, T. Dinev, P. Hart, and D. Cooke, "Managing employee compliance with information security policies: The critical role of top management and organizational culture," *Decision Sciences*, vol. 43, no. 4, pp. 615–660, 2012.

[43] C. D. Huang and R. S. Behara, "Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints," *International Journal of Production Economics*, vol. 141, no. 1, pp. 255–268, 2013.

[44] L. Hugick and J. Best, "Questionnaire length," *Encyclopedia of Survey Research Methods*, vol. 10, 2008.

[45] K.-L. Hui, W. Hui, and W. T. Yue, "Information security outsourcing with system interdependency and mandatory security requirement," *Journal of Management Information Systems*, vol. 29, no. 3, pp. 117–156, 2012.

[46] J. Humble, "Continuous delivery sounds great, but will it work here?" *Communications of the ACM*, vol. 61, no. 4, pp. 34–39, 2018.

[47] J. Hunker and C. W. Probst, "Insiders and insider threats- An overview of definitions and mitigation techniques." *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, vol. 2, no. 1, pp. 4–27, 2011.

[48] C. Insiders, "Crowd research partners," *Insider Threat*, 2018.

[49] Internal Revenue Service, "Publication 1075: Tax Information Security Guidelines For Federal, State and Local Agencies," 2016. [Online]. Available: https://www.irs.gov/pub/irs-pdf/p1075.pdf

[50] International Organization for Standardization, "Are you safe online? New ISO standard for cybersecurity," 2012. [Online]. Available: https://www.iso.org/news/2012/10/Ref1667.html

[51] F. D. János and N. H. P. Dai, "Security concerns towards security operations centers," in *IEEE International Symposium on Applied Computational Intelligence and Informatics (SACI)*, 2018.

[52] M. E. Johnson and S. Dynes, "Inadvertent disclosure-information leaks in the extended enterprise." in *Workshop on the Economics of Information Security (WEIS)*, 2007.

[53] K. Julisch, "Security compliance: The next frontier in security research," in *ACM New Security Paradigms Workshop*, 2009.

[54] F. B. Kokulu, A. Soneji, T. Bao, Y. Shoshitaishvili, Z. Zhao, A. Doupé, and G.-J. Ahn, "Matched and mismatched SOCs: A qualitative study on security operations center issues," in *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2019.

[55] E. Kolkowska and G. Dhillon, "Organizational power and information security rule compliance," *Computers & Security*, vol. 33, pp. 3–11, 2013.

[56] B. Kör and B. Metin, "Understanding human aspects for an effective information security management implementation," *International Journal of Applied Decision Sciences*, vol. 14, no. 2, pp. 105–122, 2021.

[57] J. Kosseff, "New York's financial cybersecurity regulation: Tough, fair, and a national model," *New York Department of Financial Services (DFS)*, 2016.

[58] K. Krippendorff, "Reliability in content analysis: Some common misconceptions and recommendations," *Human Communication Research*, vol. 30, no. 3, pp. 411–433, 2004.

[59] D. C. Latham, "Department of Defense trusted computer system evaluation criteria," *Department of Defense (DoD)*, 1986.

[60] N. A. Lawson, J. M. Orr, and D. S. Klar, "The HIPAA privacy rule: An overview of compliance initiatives and regirements," *Def. Counsel. J.*, vol. 70, p. 127, 2003.

[61] V. G. Li, M. Dunn, P. Pearce, D. McCoy, G. M. Voelker, and S. Savage, "Reading the tea leaves: A comparative analysis of threat intelligence," in *USENIX Security Symposium*, 2019.

[62] M. Lombard, J. Snyder-Duch, and C. C. Bracken, "Content analysis in mass communication: Assessment and reporting of intercoder reliability," *Human Communication Research*, vol. 28, no. 4, pp. 587–604, 2002.

[63] O. A. Michalec, D. Van Der Linden, S. Milyaeva, and A. Rashid, "Industry responses to the european directive on security of network and information systems (NIS): Understanding policy implementation practices across critical infrastructures," in *Symposium on Usable Privacy and Security (SOUPS)*, 2020, pp. 301–317.

[64] C. F. Mondschein and C. Monda, "The EU's general data protection regulation (GDPR) in a research context," *Fundamentals of Clinical Data Science*, pp. 55–71, 2019.

[65] National Institute of Standards and Technology (NIST), "NIST cybersecurity framework," 2014. [Online]. Available: https://www.us-cert.gov/ccubedvp/cybersecurity-framework

[66] R. Neware, U. Shrawankar, P. Mangulkar, and S. Khune, "Review on multi-factor authentication (MFA) sources and operation challenges," *International Journal of Smart Security Technologies (IJSST)*, vol. 7, no. 2, pp. 62–76, 2020.

[67] M. Nieles, K. Dempsey, and V. Y. Pillitteri, "An introduction to information security," *NIST Special Publication*, vol. 800, no. 12, p. 101, 2017.

[68] North American Electric Reliability Corporation (NERC), "NERC sanction guidelines," 2012. [Online]. Available: https://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/Appendix_4B_SanctionGuidelines_20121220.pdf

[69] ——, "CIP-007-6 — Cyber security – Systems security management," 2014.

[70] N. Ochoa, "Pass-the-hash toolkit for Windows implementation & use," *CORE Security Technologies*, vol. 1, 2010.

[71] D. of Defense, "Risk management framework (RMF) for DoD information technology (IT)," 2014.

[72] U. N. R. C. O. of Standards Development, *Regulatory Guide*. UNRCO Office, 1979.

[73] M. T. Orne, "On the social psychology of the psychological experiment: With particular reference to demand characteristics and their implications," *American Psychologist*, vol. 17, no. 11, p. 776, 1962.

[74] PCI Security Standards Council, "Payment card industry data security standard: Requirements and security assessment procedures v3.2," 2016. [Online]. Available: https://www.pcisecuritystandards.org/pci_security/

[75] A. Peterson, "Cracking security misconceptions: Untangling common myths about modern information security," O'Reilly Media, 2016.

[76] P. Puhakainen and M. Siponen, "Improving employees' compliance through information systems security training: an action research study," *MIS Quarterly*, pp. 757–778, 2010.

[77] S. Rabe-Hesketh, A. Skrondal, and A. Pickles, "Reliable estimation of generalized linear mixed models using adaptive quadrature," *The Stata Journal*, vol. 2, no. 1, pp. 1–21, 2002.

[78] S. Rahaman, G. Wang, and D. Yao, "Security certification in payment card industry: Testbeds, measurements, and recommendations," in *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2019.

[79] M. Revilla and J. K. Höhne, "How long do respondents think online surveys should be? New evidence from two online panels in Germany," *International Journal of Market Research*, vol. 62, no. 5, pp. 538–545, 2020.

[80] K. B. Rosati, "HIPAA privacy: The compliance challenges ahead." *Journal of Health Law*, vol. 35, no. 1, pp. 45–82, 2002.

[81] W. Sonnenreich, J. Albanese, and B. Stout, "Return on security investment (ROSI)- A practical quantitative model," *Journal of Research and Practice in Information Technology*, vol. 38, no. 1, pp. 45–56, 2006.

[82] R. Stevens, C. Ahern, D. Votipka, E. Redmiles, P. Sweeney, and M. L. Mazurek, "The battle for New York: A case study of applied digital threat modeling at the enterprise level," in *USENIX Security Symposium*, 2018.

[83] R. Stevens, J. Dykstra, W. K. Everette, J. Chapman, G. Bladow, A. Farmer, K. Halliday, and M. L. Mazurek, "Compliance cautions: Investigating security issues associated with US digital-security standards," in *Network and Distributed System Security Symposium (NDSS)*, 2020.

[84] R. Stevens, J. Dykstra, W. K. Everette, and M. L. Mazurek, "It lurks within: A look at the unexpected security implications of compliance programs," *IEEE Security & Privacy*, vol. 18, no. 6, pp. 51–58, 2020.

[85] A. Strauss and J. Corbin, "Basics of qualitative research techniques," Sage Publications, 1998.

[86] S. C. Sundaramurthy, A. G. Bardas, J. Case, X. Ou, M. Wesch, J. McHugh, and S. R. Rajagopalan, "A human capital model for mitigating security analyst burnout," in *Symposium on Usable Privacy and Security (SOUPS)*, 2015.

[87] S. C. Sundaramurthy, J. McHugh, X. Ou, M. Wesch, A. G. Bardas, and S. R. Rajagopalan, "Turning contradictions into innovations or: How we learned to stop whining and improve security operations," in *Symposium on Usable Privacy and Security (SOUPS)*, 2016.

[88] P. P. Swire, "A model for when disclosure helps security: What is different about computer and network security," *J. on Telecomm. & High Tech. L.*, vol. 3, p. 163, 2004.

[89] The MITRE Corporation, "MITRE attack mitigations," 2020. [Online]. Available: https://attack.mitre.org/mitigations/enterprise/

[90] M. Theoharidou, S. Kokolakis, M. Karyda, and E. Kiountouzis, "The insider threat to information systems and the effectiveness of ISO17799," *Computers & Security*, vol. 24, no. 6, pp. 472–484, 2005.

[91] J. S. Tiffany, "Respondent-driven sampling in participatory research contexts: Participant-driven recruitment," *Journal of Urban Health*, vol. 83, no. 1, pp. 113–124, 2006.

[92] U.S. Congress, "Federal information security management act of 2002," *Title III of the E-Government Act of 2002*, 2002.

[93] ——, "The public company accounting reform and investor protection act of 2002 (Sarbanes-Oxley)," in *The Public Company Accounting*

Reform and Investor Protection Act. Washington DC: US Congress, 2002, p. 55.
[94] U.S. National Security Agency, "NSA's Top Ten Cybersecurity Mitigation Strategies," 2018. [Online]. Available: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/nsas-top-ten-cybersecurity-mitigation-strategies.cfm
[95] M. Vaismoradi, H. Turunen, and T. Bondas, "Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study," *Nursing & Health Sciences*, vol. 15, no. 3, pp. 398–405, 2013.
[96] V. Verendel, "Quantified security is a weak hypothesis: A critical survey of results and assumptions," in *Workshop on New Security Paradigms*, 2009, pp. 37–50.
[97] D. Votipka, R. Stevens, E. Redmiles, J. Hu, and M. Mazurek, "Hackers vs. testers: A comparison of software vulnerability discovery processes," in *IEEE Symposium on Security and Privacy (SP)*, 2018.
[98] C. Vroom and R. Von Solms, "Towards information security behavioural compliance," *Computers & Security*, vol. 23, no. 3, pp. 191–198, 2004.
[99] F. Wolf, A. J. Aviv, and R. Kuber, "Security obstacles and motivations for small businesses from a CISO's perspective," in *USENIX Security Symposium*, 2021.
[100] X. Zhang, "Critical success factors for public–private partnerships in infrastructure development," *Journal of Construction Engineering and Management*, vol. 131, no. 1, pp. 3–14, 2005.

APPENDIX A
SURVEY QUESTIONNAIRE

- Does your organization adhere to any form of mandatory compliance standard or regulatory controls?
- Which compliance standards does your organization deal with?
- Does your organization believe compliance is sufficient to protect your systems and data? (Yes, maybe no)
- Does your organization employ proactive security controls to address threats not covered by compliance programs?
- If yes, please describe unaddressed threats.
- Please select which of the following proactive controls your organization uses to complement (in addition to) compliance programs. Please do not select controls required by compliance programs that your organization follows. (Multiple selection options: Vulnerability disclosure or bug bounty programs Machine learning and other statistical analysis, Threat modeling, Tabletop security training exercises, Live security training exercises, Threat intelligence, Threat hunting (regular searches to ascertain the presence of a previously undetected adversary or compromise), Endpoint Threat Detection and Response solutions, Change control reviews/panels, Sandboxing, Zero clients/one-time-use systems, Integrity review of data and application updates, Periodic access review, Multi-factor authentication, Multi-factor physical access, Hands-on training, On-the-job mentorship security training, On-the-job peer partnering training, Others: (fill-in-the-blank), None of the above)
- Enter loop for each item:
  - Is this security control required by compliance?
  - Why did you / your organization decide to implement this control?
  - On a scale from 1 to 5, with 5 being the highest rating, how well has this control worked out for your organization? (1-5)
  - What worked (or did not work) well about this control?
  - How do you ensure this measure is compatible with compliance controls (or if not, why not)?
  - How often do you reassess this control's effectiveness? (Daily, Once a week, One a month, Every few months, Yearly, Never)
- How does your organization prioritize which proactive measures you are going to invest in? What are the key factors?
- Demographics
  - What is the highest level of school you have completed or the highest degree you have received?
  - Please select the option that best categorizes your organization (Government/Defense, Entertainment, Financial services (payments, credit cards), Consumer services (hotels, retail, sales), Critical services (power, water, etc), Healthcare, Agriculture/mining, Information technology, Education/Research)
  - Please specify the job role that most closely reflects your employment position (Security Engineer, Security Analyst, Management, Compliance/Governance SME, Developer)
  - Please estimate the number of years experience you have in the compliance and information technology fields.
  - Please specify the estimated size of your organization.
  - Please specify the estimated size of your constituency or clientele.
  - How many organizations do you support?

APPENDIX B
DEMOGRAPHICS AND CODEBOOK

The demographics and codebook are available at https://gist.github.com/beyond-compliance-study/d124de07b3ac1739cc9bd28622e57c28

The demographics table details the collected demographics of each participant. Clientele size (C/S) indicates the number of supported customers, whereas the number of reported supported organizations (S/O) indicates how many *external* organizations that the company supports.

The codebook contains all the codes with their categories, explanations, and also, related examples from the data.

APPENDIX C
LIST OF REPORTED COMPLIANCE STANDARDS

Table IV details the reported compliance standards used by study participants.

APPENDIX D
REPORTED MEASURES

Table V lists all the complementary measures reported by our participants, organized according to the four high-level categories.

Reported Standard	Count
NIST Cybersecurity Framework [65]	33
HIPAA (Health Insurance Portability and Accountability Act) [60]	17
PCI DSS (Payment Card Industry Data Security Standard) [74]	14
FISMA (Federal Information Security Management Act) [92]	12
ISO (International Organization for Standardization) [50]	12
FedRAMP [36]	10
GDPR (General Data Protection Regulation) [64]	9
CIS Controls (Center for Internet Security Controls) [20]	8
FERPA (The Family Educational Rights and Privacy Act of 1974) [33]	8
CCPA (California Consumer Privacy Act) [27]	4
COPPA (Children's Online Privacy Protection Act) [4]	4
DoD Instruction 8510.01* [71]	4
NERC CIP (Critical Infrastructure Protection) [69]	2
SOX (Sarbanes-Oxley Act) [93]	2
University IT standards*	2
Genome data protection guidelines*	1
IRS Publication 1075 [49]	1
NY Department of Financial Services Regulation* [57]	1
Trusted Computer System Evaluation Criteria "Orange Book"* [59]	1
U.S. Nuclear Regulatory Commission Standards* [72]	1
Other financial regulations*	1

TABLE IV: Reported compliance standards used by our participants. * indicates standards provided in the 'other' survey field.

Measure	Prevalence
Training and exercises	
Hands-on training	19
On-the-job mentoring	16
Tabletop	15
Live security	13
On-the-job peering	11
Internal phishing exercises*	1
Human-focused reviews	
Periodic access reviews	21
Change control	18
Threat modeling	16
Integrity review	14
Incident response playbooks*	1

Measure	Prevalence
Passive defenses	
Multi-factor authentication	32
Zero clients	9
Sandboxing	9
End-to-end encryption*	1
Microsegmentation*	1
Continually evolving defenses	
Endpoint detection and response	26
Threat hunting	20
Threat intelligence	19
Vulnerability disclosure / bug bounty	14
Physical access barriers	13
Machine learning	10
Dogfooding*	1

TABLE V: All complementary measures reported by our participants, organized into four high-level categories. * indicates measures provided by participants in the 'other' field.

APPENDIX E
QUANTITATIVE ANALYSIS

Factor	Type	Description	Baseline
Category	Fixed	Measure groups	Passive Defense
ID	Random	Participant ID	–

TABLE VI: Cumulative Link Mixed Model Factors.

Our Cumulative Link Mixed Model took into account fixed and random effects (Table VI). The fixed effect was the set of all complementary measure categories and the random effect was the participant set, forming the mixed effect input. The random effect includes duplicate identification numbers, since participants chose more than one control to discuss, and multiple participants could choose the same control. We compared each category of complementary measure to the baseline, passive defenses.

Contrast	Estimate	p-value
PD - CED	2.170	<.0001*
PD - TE	1.807	0.0046*
PD - HFR	1.679	0.0068*
CED - TE	-0.363	0.8321
CED - HFR	-0.491	0.6279
TE - HFR	-0.128	0.9934
PD = Passive Defenses	CED = Continually Evolving Defenses	
TE = Training and Exercises	HFR = Human-focused Reviews	
*Statistically significant		

TABLE VII: Contrasts and estimates between combinations of proactive control groups

In Table VII, we provide contrast values between all combinations of control groups that shows the satisfaction level difference estimates between the control groups and the associated p-value that indicates significance.

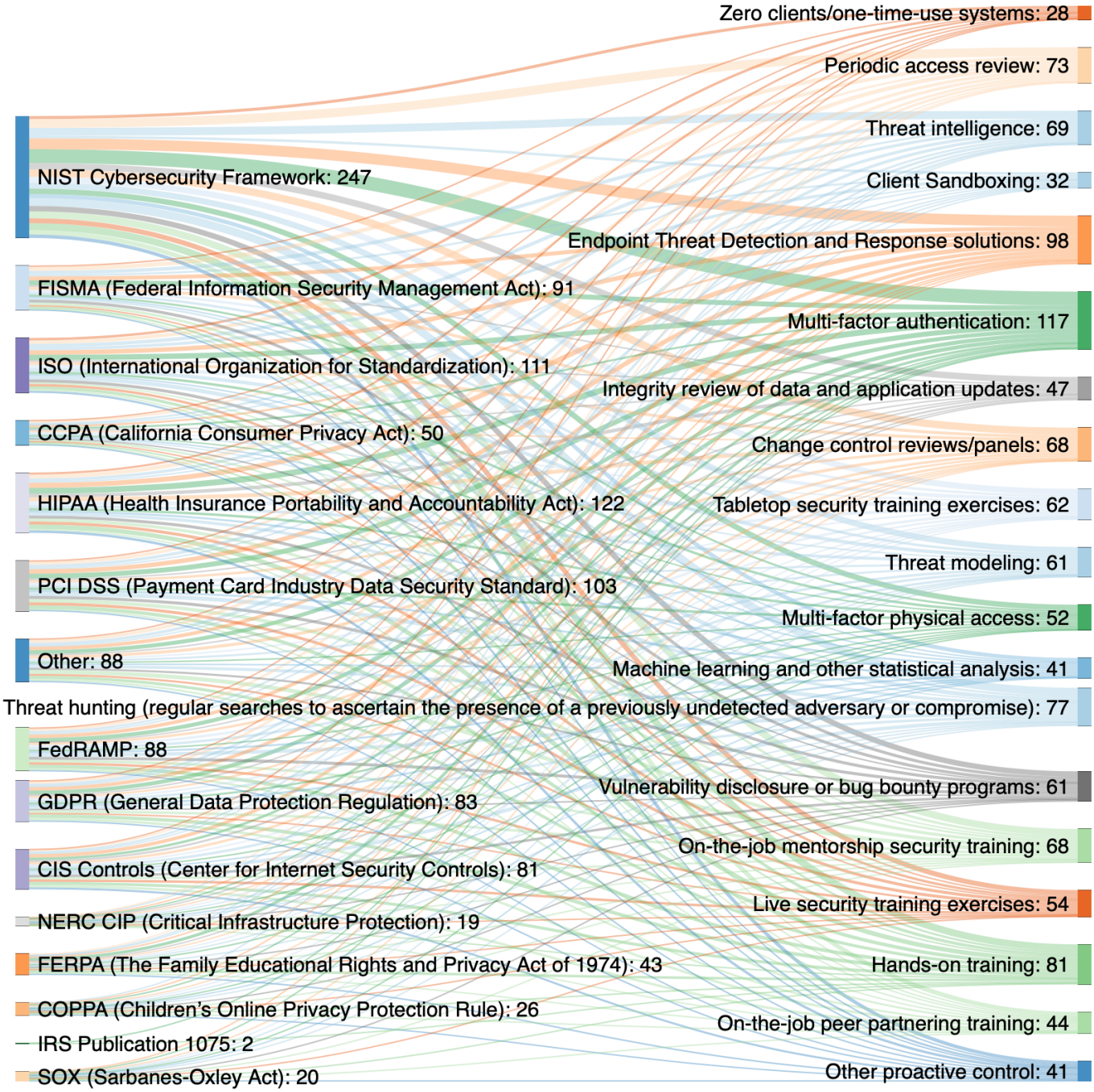

Fig. 4: Sankey diagram demonstrating the relationship between compliance standards and complementary measures. On the left are the compliance standards, and on the right are the complementary measures. The width of the line between the two sides represent the number of times our participants mentioned using the complementary measure when also following the compliance standard. Note that participants could indicate that they require compliance with multiple standards, and therefore any complementary measures that they use would go to all standards that they reported.