Beyond Deterrence: A Systematic Review of the Role of Autonomous Motivation in Organizational Security Behavior Studies

Xiaowei Chen
University of Luxembourg
Esch-sur-Alzette, Luxembourg
xiaowei.chen@uni.lu

Lorin Schöni
ETH Zurich
Zurich, Switzerland
lorin.schoeni@gess.ethz.ch

Verena Distler*
Aalto University
Espoo, Finland
verena.distler@aalto.fi

Verena Zimmermann*
ETH Zurich
Zurich, Switzerland
verena.zimmermann@gess.ethz.ch

Abstract

What drives employees to ensure security when handling information assets in organizations? There is growing interest from the security behavior community in how autonomous motivators shape employees' security-related behaviors. To reconcile the scattered viewpoints on *autonomous motivation* and synthesize findings from studies utilizing various theoretical frameworks, we systematically reviewed relevant publications. We present a preregistered literature review that investigated (a) what forms of autonomous motivation have been examined in organizational security contexts, (b) which behaviors/behavioral intentions are related to autonomous motivators, and (c) how autonomous motivation affects employees' security behaviors. Based on an initial set of 432 papers, filtered down to 45 studies, we identified 17 unique autonomous motivators and three types of related security behaviors. This review not only develops a refined taxonomy of autonomous motivation related to security behaviors but also charts a path forward for future research on autonomous motivation in human-centered security.

CCS Concepts

• **Security and privacy → Human and societal aspects of security and privacy**; • **Human-centered computing → HCI theory, concepts and models**.

Keywords

Information security behavior, Autonomous motivation, Motivation theory, Intrinsic motivation, Self-Determination Theory, Systematic review, Expectancy-Value Theory, Human-centered security

*Both authors contributed equally to this research.

CHI '25, Yokohama, Japan

ACM ISBN 979-8-4007-1394-1/25/04
https://doi.org/10.1145/3706598.3713122

ACM Reference Format:
Xiaowei Chen, Lorin Schöni, Verena Distler, and Verena Zimmermann. 2025. Beyond Deterrence: A Systematic Review of the Role of Autonomous Motivation in Organizational Security Behavior Studies. In *CHI Conference on Human Factors in Computing Systems (CHI '25), April 26-May 1, 2025, Yokohama, Japan.* ACM, New York, NY, USA, 28 pages. https://doi.org/10.1145/3706598.3713122

1 Introduction

Organizations face the critical challenge of securing their information systems against cyber threats that target humans. Various lenses can be applied to improve our understanding of why people behave the way they do. Prior work has highlighted important obstacles to information security such as prescribed security policies not being feasible and too cumbersome [74], inappropriate cost-benefit trade-offs of complex security advice [65], or situational factors making secure responses challenging [45]. Recent conceptualizations of security behavior change [66, 121] highlight that security behaviors need to be met with low friction and to be within the compliance budget. People need to understand the behaviors, agree that these behaviors matter, believe that they are able to implement them, acquire the skills to implement the behavior, and then embed them in their everyday life. Hence, promoting secure behaviors in an organization is a challenging, multi-step process, involving various stakeholders [46].

The majority of security behavior studies focused on the roles of deterrence and sanctions in guiding employees' security behaviors [6, 38]. A recent review [38] found that out of 49 studies concerned with cybersecurity behavior, 36 measured compliance exclusively. While compliance is crucial for maintaining organizational information security, attacks are becoming increasingly sophisticated. Employees need to flexibly cope with new threats that are not yet prescribed by existing information security policies (**ISP**s), thus going beyond compliance when necessary. Recently, there has been a shift of focus from "threats and sanctions" approaches, which do not always lead to the desired security behaviors [27], toward exploring employees' motivation to engage in "self-driven" protective security behaviors [30, 51, 92]. Correspondingly, a growing number of recent publications have investigated how employees' autonomous motivation shapes their security behaviors [38, 71, 103].

"What is autonomous motivation?" In the framework of Self-Determination Theory (**SDT**), human motivation can be categorized into three types [41, 118]: *amotivation* (lack of intention and motivation), *controlled motivation* (driven by external reward/punishment and pressure), and *autonomous motivation*. **Autonomous motivation** comprises both *intrinsic motivation* (including interest, enjoyment, and satisfaction) and the internalized extrinsic motivation in which people have identified with an activity's value and integrated it into their sense of self (including values, commitment, and ethics) [41]. Satisfying an individual's psychological needs for competence, autonomy, and relatedness creates autonomous motivation [137]. When performing tasks autonomously, employees experience a sense of choice and enjoyment; they do not feel compelled by outside forces [42]. Autonomous motivation is enduring and sustainable in driving employee performance [137].

Security-related research shows that autonomous motivators are positively correlated with certain security behaviors in the workplace [51, 133] and might make compelling contributions to explain and foster employees' protective cybersecurity behaviors [6, 92]. Despite this potential, autonomous motivation is a construct derived from psychology which necessitates adaptation and empirical validation in the context of security behaviors. It is worth noting that in a widely cited taxonomy of security behavior grounded in SDT [105], autonomous motivators have been categorized as intrinsic motivation. Moreover, researchers have applied constructs from other theories to investigate autonomous motivators, frequently without clarifying their theoretical foundation [79, 127] or the definition of "autonomous/intrinsic" [89, 133]. These inconsistencies in the conceptualization and application of autonomous motivation (e.g.,[79, 105]) pose challenges for future research, particularly in terms of synthesizing prior findings from studies that examined autonomous motivation in relation to security behaviors.

To consolidate the theoretical foundation and reconcile scattered findings on autonomous motivation, we conducted a preregistered literature review using the Scopus and ACM Digital Library databases to investigate (a) what forms of autonomous motivation have been examined in organizational security contexts, (b) the behaviors/behavioral intentions that are related to autonomous motivators, and (c) how autonomous motivation affects security behaviors in the workplace. The contributions of our review are three-fold:

- We developed a refined taxonomy of autonomous motivation including 17 motivators clustered into five categories by reviewing theoretical frameworks and comparing measurements of autonomous motivators in the security domain. The taxonomy and the accompanying toolbox of existing measurements provide relevant and timely support for researchers and practitioners who aim to examine and develop user-centered security policies and interventions.
- While previous studies aiming to explain security behavior understood as compliance often made use of theories focusing on *threats* and *deterrence*, our review suggests that there is a shift towards Self-Determination Theory as the most frequently applied theory in studies that focused on what *motivates* employees to ensure security. This shift in theory mirrors a paradigm shift in the security domain from viewing the human as the weakest link towards viewing the human as a valuable resource that can be enabled and motivated to contribute to security.
- We provide an overview of suitable avenues to extend the study of autonomous motivation in the domain of organizational information security and provide practical suggestions for researchers who want to conduct theory-informed studies on autonomous motivation in human-centered security.

2 Background

2.1 Motivation in security behavior studies

The interdependent relationship and distinctive contributions of emotion, cognition, and motivation to human behavior have sparked extensive discussions in psychology [86]. In the security context, emotions influence the degree of attention individuals direct toward cybersecurity tasks and their adherence to guidelines [150]. Cognitive processes such as perception, attention, and elaboration affect how a person interprets and responds to cyber attacks [26]. Motivation is critical in both initiating and maintaining behaviors [85]. Whereas initial changes are often driven by the expectation of long-term benefits, maintaining these changes relies more on the regular satisfaction derived from the behavior itself [85]. While we acknowledge the critical roles of emotion, cognition, and other factors in behavior change, this review narrows its scope to autonomous motivation.

A prevalent approach for studying employees' security behaviors involves deductive methodology [87], where motivation is often included as one of the independent variables, and security behaviors are the dependent variables in research models. In this approach, researchers examine motivational factors alongside other variables to explain or influence employees' compliance intentions [64, 90]. Established theories from other disciplines have been frequently introduced into security behavior research [87] to explain the relationships between motivational factors and behaviors. Theory-based literature reviews [7, 88] indicate that the Theory of Planned Behavior [132], Protection Motivation Theory [59], and Deterrence Theory [84] have been the most frequently utilized to examine employees' security behaviors. Below, we describe how each of these theories conceptualizes the role of motivation in changing security behaviors.

The Theory of Planned Behavior proposes that an individual's behavioral intentions are determined by their *attitudes toward the behavior*, *subjective norm* (e.g., perception of others' expectations), and *perceived behavioral control* (e.g., one's ability to perform the behavior) [2]. Individuals' beliefs in their ability to perform a behavior are crucial in determining their choice of action [97]. Thus, an individual's motivation to perform a security behavior is influenced by their attitude and social influences, but their ability (perceived behavioral control) determines whether they can successfully carry it out [97]. Though the Theory of Planned Behavior has frequently been applied to examine employees' compliance behaviors, researchers have raised concerns about missing variables in the framework [132]. Kranz and Haeussinger [83] proposed integrating the Theory of Planned Behavior and the Organismic Integration Theory — a subtheory of SDT. They empirically tested their research model in a sample of 444 employees [83]. They found

that when employees' personal values and principles aligned with their employer's information security prescriptions and goals, employees' intentions to comply increased significantly [83]. This finding suggests that autonomous motivation is a relevant factor in fostering information security compliance.

Protection Motivation Theory, initially developed in the health management domain [114], posits that individuals' protective behaviors are influenced by their evaluations of the *severity* and *certainty* of a threat and assessments of the efficacy and their ability to perform protective behavior. In the framework of Protection Motivation Theory, situations involving threats (e.g., health, intrapersonal and interpersonal, economic [59]) motivate people to choose protective solutions. In the context of information security, threats represent events with potentially harmful consequences [59]. A review of 67 studies applying Protection Motivation Theory showed that most studies examined threats and coping appraisal constructs, specifically *self-efficacy* (91.0%), severity (89.6%), *vulnerability* (88.1%), and *response efficacy* (83.6%) [59]. Menard et al. [92] argued that if a threat is perceived as irrelevant, the appeal will not evoke fear and will fail to connect with the individual. After comparing three competing research models in their study [92], they suggested that intrinsic motivators could be a powerful factor that influences organizational security behaviors.

Deterrence Theory, rooted in criminology, proposes that "certain controls can serve as deterrent mechanisms by increasing the perceived threat of punishment for information system misuse" [37, p.1]. It has frequently been applied to understand employees' ISP compliance and violation behaviors [138]. According to Deterrence Theory, motivation is linked to an individual's perception of the certainty, swiftness, and severity of the sanctions that may result from their actions [138]. In a survey study of 602 U.S. employees, Son compared the intrinsic and extrinsic motivation models integrated into the framework of Deterrence Theory [133]. Their study revealed that "intrinsic" motivators (*perceived legitimacy* and *value congruence*) played a more substantial role in explaining employee compliance than extrinsic motivations (*perceived deterrent certainty* and *severity*) [133]. Son [133] suggested that exploring intrinsic motivation-based approaches, rather than only sanction-based methods, is likely to enhance employees' compliance with ISPs.

To summarize, research involving the most frequently used theories suggested that autonomous motivation provides an alternative approach for explaining and fostering security behaviors. However, systematic examinations of how autonomous motivation is related to organizational security behaviors are lacking. This research gap thus led us to our first research question:

> **RQ1**. What forms of autonomous motivation have been found to influence employees' information security behaviors?

2.2 Paradigm shift from compliance to extra-role security behavior

Maintaining information security in organizations is not only a technical challenge but also needs to consider human actions [91]. The complexity of human behavior positions individuals as key influencers in securing information systems, and research on behavioral factors in cybersecurity is critical [91]. Lahcen et al. [91] analyzed **insider threats** (risks caused by an employee or any other individual with authorized access to the information system) in the workplace and categorized them into three types: unintentional, intentional, or malicious. Unintentional errors are caused by a lack of knowledge or skill (e.g., accessing confidential information through public Wi-Fi), while intentional errors arise from knowingly risky behavior (e.g., leaving passwords on a sticky note), and malicious actions are deliberate with the intent to cause significant harm (e.g., stealing confidential data) [91]. Most organizations have an information security policy (ISP) that describes insiders' responsibilities and prescribes actions to protect the organization [133].

Different taxonomies have been proposed for understanding employees' **security compliance**, focusing on factors such as intentionality, technical expertise, and intrinsic/extrinsic motivation [105, 136]. Via interviews (n = 110) and surveys (n = 1167), Stanton et al. [136] categorized employees' behaviors into six categories with two parameters: intentionality (including malicious, neutral, and benevolent intentions) and technical expertise (including novice and expert). They suggested that employees might exhibit behaviors from different categories at different points in time [136]. Organizations can enhance their security status through motivational interventions that promote benevolent intent among employees [136], including effective security management, strong leadership, clear role designations, and training programs. In another taxonomy, Padayachee [105] categorized research findings on security compliance and deterrent control into a taxonomy predicated on SDT. They linked motivational factors with security-compliant behaviors and suggested that organizations apply the framework to understand employees' motivations, thereby assessing and promoting security compliance [105].

Recent research has highlighted a proactive approach towards employees that extends beyond mere compliance with ISP guidelines. Posey et al. [109] proposed a taxonomy of protection-motivated behaviors that indicates which protection-motivated behaviors are critical, which are difficult to promote, and which are considered common sense, allowing for direct comparisons across individual behaviors. Posey et al. [111] suggested that employees can be guardians of organizational information security. This is aligned with a recent interview study where cybersecurity professionals posited that empowering employees, rather than inhibiting their behaviors, can enable them as the last line of defense in organizations [143]. An increasing number of security behavior studies have examined employees' extra-role security behaviors [25, 51], beyond mere compliance. These studies investigated a wide range of security-related behaviors and tasks in the workplace, such as employees' self-driven security literacy learning [130], crowdsourced approaches to defending against phishing attacks [25], and security knowledge sharing in the workplace [120].

Understanding what drives employees to perform these **extra-role security** tasks can enhance organizational information security [39]. Extra-role information security tasks describe "security-related citizenship behaviors that go beyond prescription but nonetheless contribute to the organisational, social, and psychological InfoSec environment" [38, p.198]. In a focus group study,

Chen et al. [30] found that various intrinsic factors influenced employees' intentions to report phishing emails. These motivators, deeply embedded in employees' psychological needs, include enjoyment, satisfaction, empowerment, and sense of belonging [30]. Recently, Frank and Kohn [51] proposed a taxonomy of motivation for extra-role security behaviors (**SDT-ER taxonomy**), based on SDT, in which motivators of extra-role behaviors are arranged along a continuum from extrinsic to intrinsic motivation. They [51] linked six out of nine dimensions of extra-role security behaviors with autonomous motivators (including usefulness-driven, value-driven, and interest-driven). However, further research is needed to investigate other types of security behaviors related to autonomous motivation:

> **RQ2**. Which employee security behaviors (or behavioral intentions) related to autonomous motivation have been examined in the surveyed literature?

2.3 The fragmentation and heterogeneity of applying diverse theoretical frameworks

Sutton and Staw [139] discussed how references, data, variables, diagrams, and hypotheses can be mistaken for theory and shared their definition of **theory**:

> Theory is about the connections among phenomena, a story about why acts, events, structure, and thoughts occur. Theory emphasizes the nature of causal relationships, identifying what comes first as well as the timing of such events. [139, p.378]

In this review, we adopted Sutton and Staw's definition and emphasize the three characteristics of theory: (a) It consists of interrelated propositions and constructs; (b) it establishes clear relationships between constructs; and (c) it explains or predicts the occurrence of events [73]. We refer to a **theoretical framework** as the application of a theory or set of interrelated constructs derived from an established theory to guide the research [73]. By contrast, a **research model** involves synthesizing concepts, ideas, and constructs from multiple sources, including empirical findings and different theories, to create a unique model to address research problems [73]. We adopted Liehr and Smith's definition of **concept**: "an image or symbolic representation of an abstract idea" [73, p.188]. We conceptualize a **construct** as "a label for a cluster or domain of covarying behaviours" [19, para.2]. Constructs are key components of theories [146].

In the security behavior community, researchers have argued that theory is essential for the field [44]. Theory provides a structure for understanding complex behaviors and their underlying motivations [92] and for identifying intangible psychological factors that influence users' security-related choices. Moreover, theory guides the development of measurements [49] and interventions [130, 162], thus enhancing the rigor and validity of research outputs. For example, Faklaris et al. [49] created and empirically validated the Security Attitudes (SA-6) measurement with the guidance of the Theory of Reasoned Action. Zou et al. [162] developed and evaluated the effectiveness of two interventions grounded in Protection Motivation Theory, and Silic and Lowry [130] integrated intrinsic motivation into their security training to create an immersive learning experience for employees. Furthermore, a strong theoretical foundation helps to avoid the pitfalls of an "atheoretical black box" [44], ensuring that research contributions are meaningful. Given the interdisciplinary nature of security behavior research [80], theories from **psychology, criminology**, and **organizational behavior** have been introduced to study security behaviors [88]. This integration of various theories has facilitated the exploration of diverse factors that influence security behaviors [35, 97], ranging from fear, desire, and self-efficacy to organization culture and societal influences, which offer numerous insights for understanding and promoting security behaviors [88]. However, this blossoming of adopted theories has also presented new challenges and raised new questions for researchers. For example, "How can we synthesize findings from varied and even competing theoretical frameworks?" This disparity and fragmentation of knowledge requires ongoing effort from researchers to synthesize findings from studies that have utilized different theoretical frameworks.

There are two common approaches for integrating existing findings from different theories, namely, theory-driven and empirical-data-driven approaches [97]. The theory-driven approach [88] can highlight important factors that are not visible in the empirical data of a specific case, whereas the empirical-data approach can find relevant constructs from a phenomenon and compare constructs from different theories [97]. Lebek et al. [88] conducted a literature review (n = 113) of theories related to security awareness in behavioral research. They proposed a meta-model by assembling the core constructs from the four most commonly applied theories in reviewed papers [88]. Moody et al. [97] empirically compared 11 theories with employees (n = 274), then they proposed and tested a unified model of ISP compliance (including constructs such as response efficacy, role values, and reactance) with 393 employees. To address the fragmentation and heterogeneity of research on cybersecurity self-efficacy, Borgert et al. [22] conducted a systematic literature review (n = 174). They made suggestions for standard and transparent self-efficacy measures and called for the pursuit of parsimony and falsifiability in self-efficacy theories, noting that inconsistencies often arise from deviations from the original theory and differing assumptions [22]. However, to the best of our knowledge, no systematic research has synthesized the role of autonomous motivation in organizational security behaviors.

To conclude, a plethora of theoretical frameworks have been utilized to study autonomous motivation and security behaviors. However, due to the distinctiveness of theoretical frameworks and a lack of synthesization of findings on the topic, it is still unclear how autonomous motivation influences employees' security behaviors. Consequently, we formulated the following research question:

> **RQ3**. Which theoretical frameworks have been employed to explore autonomous motivation in the domain of organizational information security, and how do these theoretical frameworks further our understanding of organizational information security?

Additionally, previous studies have indicated that study context, cultural background, and other various roles might influence the interpretation of study results [62, 122]. We propose that authors' reflections on their study limitations and future opportunities from their work can provide information on how to further advance the field. Thus, our last two research questions are:

RQ4. What are the characteristics of the study contexts in terms of geographical location, industry sectors, and participants' job roles in the surveyed literature?
RQ5. What are promising avenues for studying autonomous motivation in the domain of organizational information security?

3 Systematic Literature Review

3.1 Preparation phase

In the preparation phase, we tested our search terms, verified whether the extracted papers were relevant, and refined the research questions and search terms. We began by identifying 77 papers that mentioned "intrinsic motivation," "security," and "employee" in their abstracts from the Scopus database. Of those, 22 were evaluated as relevant for defining the scope of our review and generating our research questions. These studies were conducted in the workplace or specifically mentioned that their study goal was to examine employees' motivation to engage in security behaviors.

3.2 Literature search

To cover the wide and interdisciplinary landscape of security behavior, we chose the ACM Digital Library (The ACM guide to computing literature) and the Scopus database as the initial data sources. The ACM Digital Library covers relevant computer science and IT-security-related publications. To complement the results with publications from related disciplines, Scopus indexes a wide range of peer-reviewed publications from different disciplines and is considered one of the most comprehensive databases [124]. Our review captures literature from fields such as usable security, information security management, and security behavior studies. These two databases cover most of the respective influential venues.

To address our research questions, we collected previous literature by conducting searches that combined the terms "autonomous motivators," "security behavior," and "workplace." We had to vary the terms slightly for each search engine. We provide all the searches as supplemental material. Here, we give an example search that we used in Scopus:

```
TITLE-ABS-KEY ( "autonomous" OR "intrinsic" OR "endogenous" ) AND TITLE-ABS-KEY ( motivation ) AND TITLE-ABS-KEY ( "security behavior" OR "security behaviour" OR "cybersecurity" OR "information security" OR "information technology security" OR "IT security" OR "information system security" ) AND TITLE-ABS-KEY ( "employee" OR "workplace" OR "organization" OR "organisation" OR "company" OR "corporation" )
```

3.3 Preregistration

After conducting an initial screening of the resulting hits, we preregistered our review on the OSF to enhance the transparency of our process and facilitate the replication of the work by other researchers [32]. We follow the Generalized Systematic Review Registration Form proposed by Van den Akker et al. [147] for registration and documentation. In addition, we report our screening process, which adheres to the PRISMA guidelines [61, 96] for transparency and meta-analyses.

3.4 Study selection

We manually searched and identified 432 publications of interest from the two databases on February 18, 2024. Subsequently, we downloaded their bibliographic information (including title, authors, abstract, and publication venues) and imported all of them into Rayyan, an online tool for systematic reviews [1]. Through Rayyan, automatic duplication identification, and manual confirmation, we removed 61 duplicates, and thus, 371 publications moved on to the screening process.

Two authors independently screened the same 26% of papers (95 out of 371) on the basis of our inclusion and exclusion criteria without being able to see the other coder's decisions. Of the 95 papers, the two authors agreed to include 13 publications and to exclude 78. The first author recommended the inclusion of one additional paper, whereas the second author recommended three other papers. Thus, to avoid potentially overlooking any relevant publications, 17 publications from this collection were included for further evaluation. The authors achieved 95.79% agreement (almost perfect agreement), with a Cohen's kappa of .84. The first author then screened the rest of the publications with the following inclusion and exclusion criteria and a total of 46 out of 371 publications moved on to further evaluation.

- **Inclusion**: The study examined employees' autonomous motivation related to their cybersecurity behavior or intentions in the workplace as indicated by a screening of the title, abstract, and keywords.
- Relevant **autonomous motivators** that were in line with the inclusion criteria comprised interest, curiosity, enjoyment, desire, satisfaction, empowerment, commitment, value, contribution, responsibility, fairness, moral belief, justice, ethics, legitimacy, endogenous motivation, autonomous motivation, intrinsic motivation, or fulfilling basic psychological needs (e.g., autonomy, competence, and relatedness).
- **Exclusion**: The study was not peer-reviewed (e.g., doctoral dissertation), was not an empirical study focusing on employees (i.e., no participants were included or a student sample was used), or gave no indication of the data analytic methods or respective findings (e.g., it was a work in progress that lacked findings).

We used Zotero to screen the full text of retrieved publications. Eight publications were excluded for the following reasons: not an empirical study (n = 3), not related to employees' motivation (n = 2), student sample (n = 1), prestudy of another paper that was already included (n = 1), and concerns about quality[2] (n = 1). We applied forward and backward snowballing to the papers we retrieved in May 2024 and identified an additional seven papers that met our inclusion criteria. A total of 45 papers were included for our review (see Figure 2 number of papers by year). 32 were published in journals, addressing topics in information systems, security, and interdisciplinary fields. High-impact journals include *MIS Quarterly*, *Information & Management*, *European Journal of Information Systems*, *Computers & Security*, and *Computers in Human Behavior*. The remaining 13 papers appeared as conference proceedings at venues

[1] https://www.rayyan.ai/.
[2] The journal was de-listed from Scopus due to quality concerns in 2020. The paper was published in the same year of de-listing and does not match the journal's scope.

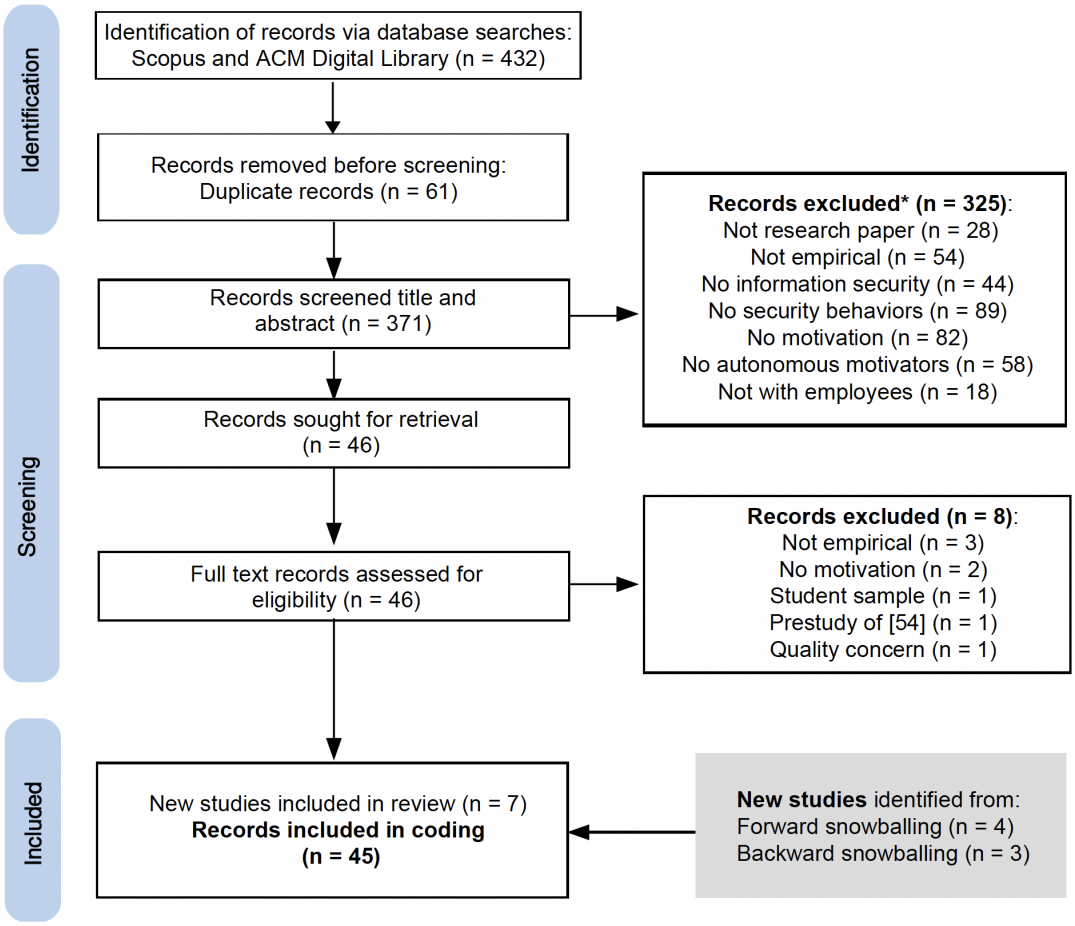

Figure 1: PRISMA flow diagram of study selection (Note: *Multiple reasons may apply).

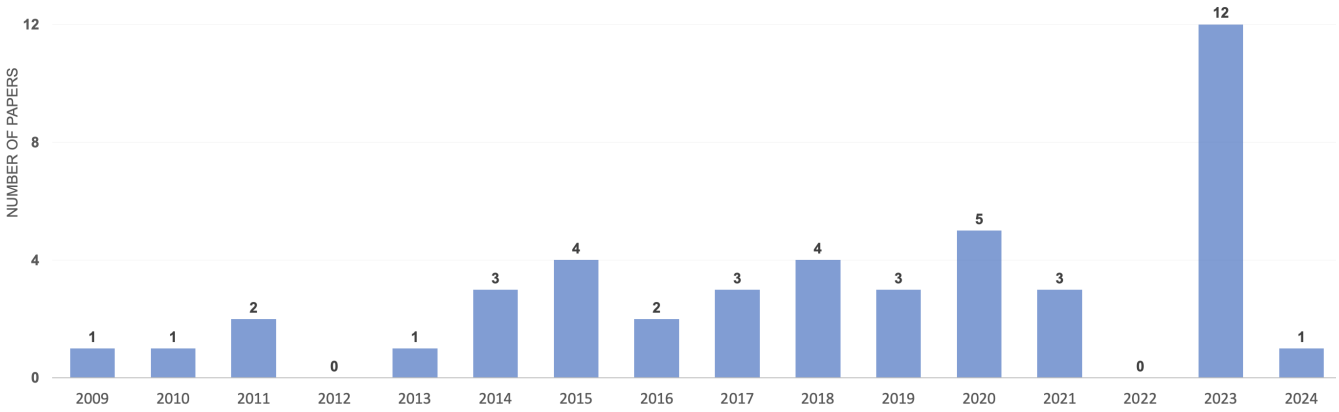

Figure 2: Number of papers by year.

including the *Symposium on Usable Privacy and Security (SOUPS)*, the *Hawaii International Conference on System Sciences*, and the *AIS International Conference on Information Systems*. Appendix B contains a table of publication venues.

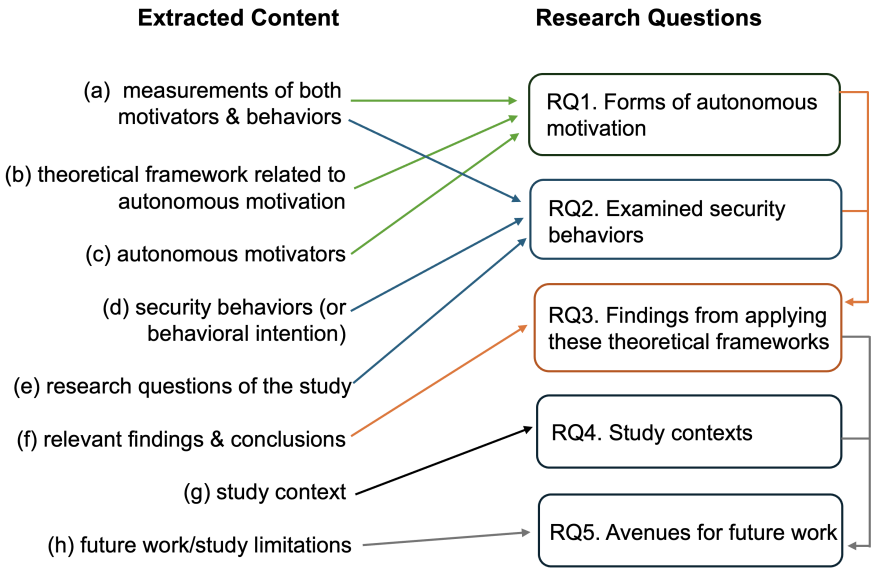

Figure 3: Matching extracted content with the research questions.

3.5 Paper extraction

To address our research questions, we used Microsoft Excel to extract and code (a) measurements of both motivators and behaviors, (b) theoretical framework related to autonomous motivation, (c) autonomous motivators, (d) security behaviors (or behavioral intentions), (e) research questions of the study, (f) relevant findings and conclusions, (g) study context, and (h) future work/study limitations. To standardize the coding process, the first author developed a detailed extraction manual to facilitate a systematic and consistent extraction that was jointly discussed and tested by all authors. Figure 3 illustrates the connection between the extracted content and our research questions.

First, all authors coded the same three papers to ensure a joint understanding. We resolved some ambiguities encountered during the process via discussion (e.g., when a paper mentioned multiple theoretical frameworks, we coded only the theoretical framework that was related to the autonomous motivators). Then, we extracted data from all papers. The data that each author extracted was independently reviewed by another author to ensure accuracy and consistency. For transparency, the extraction manual is provided in the Supplementary Material along with all the extracted data.

3.6 Measurement extraction

During the extraction process, we observed that some references to the original sources that the authors borrowed or adapted their measurements from were quite vague. To ensure scientific rigor and to provide a useful toolbox of existing measurements for other researchers, we thus conducted a second iteration of the extraction phase with a specific focus on measurement extraction of autonomous motivators and security behaviors to identify all original references and also to describe the ways in which the original measures were adapted.

We also contacted the authors of 10 papers that did not include the complete measurements of either autonomous motivators or security behaviors to request the missing measurements. Four authors provided the requested measurements; however, for the remaining six papers, we were unable to obtain access to their full measurements. Consequently, our descriptions of their measurement and adaptation process are based on the information provided in their publications.

4 Results

4.1 Autonomous motivators examined in security behavior studies

Thirty-eight of the reviewed papers employed scales for measuring autonomous motivators in their study design. Among them, six papers' complete measurements were inaccessible. Thus, we extracted 97 measurements comprising 392 items from the remaining 32 papers. Additionally, there were four qualitative studies [21, 51, 63, 129] and three studies that used alternative measurements (i.e., Analytic Hierarchy Process questionnaires, a popular method for decision-making) [10], a single-item measure [54], and autonomous motivators as design principles [4]).

By analyzing the definitions, measurements (when provided), and references of all autonomous motivators, we identified 17 unique autonomous motivators that have been investigated in security behavior studies. We found that these motivators were driven by an individual's *interest*, the *intrinsic values* of engaging in the activity, or *personal values* and *expectations* associated with the activity. Additionally, a group of motivators was driven by *fulfilling psychological needs*, such as autonomy or relatedness. Table 1 provides an overview of all motivators, their definitions, and how often they have been studied. The category was developed from the SDT-ER taxonomy suggested by Frank and Kohn [51] but extended

with insights from the empirical studies included in our review, thus resulting in five groups of motivators (refer to Table 1). We marked our proposed new categories with asterisks in Table 1.

To provide a useful toolbox for researchers or practitioners interested in measuring autonomous motivation in the security domain, we also extracted and categorized all provided measurements from the reviewed articles, their original sources where applicable, and whether they were adapted. Table 2 provides an exemplary excerpt of the complete overview table provided in the supplementary material.

4.1.1 Interest-driven motivators (n = 4). Joy, curiosity, and satisfaction are intrinsic and interest-driven motivators [51]. In the SDT framework, these motivators are termed intrinsic motivation [116]. In the studies we reviewed, interest-driven motivators were either examined with specified terms such as joy (e.g., technophilia [51], interest [63], or satisfaction [120]) or applied as principles (e.g., joy and curiosity [130]) for training design. Compared with the other motivators associated with a specific task or values/expectations associated with engaging in an activity, intrinsic motivators emerge when an individual is internally driven.

4.1.2 Task-driven motivators (n = 11). *Intrinsic task value* describes the positive experiences derived directly from a task that motivate individuals to engage with it [144]. Researchers sometimes intermix the terms intrinsic value and intrinsic motivation [70]. However, Eccles and Wigfield argued that it is necessary to differentiate the "internal origin of the desire to engage in an activity" (intrinsic motivation) from "the enjoyment of the task itself" (intrinsic value) [48]. We thus propose that intrinsic value[48] should be renamed intrinsic task value to make this term more distinguishable from intrinsic motivation. For example, Silic and Lowery surveyed employees' perceptions of feeling rejuvenated, lowering their stress, and passing the time more enjoyably when using a web system [130]. Other tasks have also been examined for the intrinsic value related to performing the task of protecting one's mobile identity [5] and complying with ISPs [5, 12, 24, 89]. These studies explored how employees' feelings of accomplishment, fulfillment, contentment [12, 24, 28], importance [43], and pleasantness [89] were associated with compliance. In addition, four of the studies we reviewed [71, 109, 110, 148] examined the relationship between *job satisfaction* and ISP compliance.

4.1.3 Motivators fulfilling psychological needs. These motivators specifically address and satisfy individuals' basic psychological needs (e.g., competence, autonomy, relatedness [119], and safety).

Competence-related (n = 24). Competence-related motivators were the most frequently examined motivators in the studies we reviewed. They took the form of self-efficacy (n = 13), *perceived competence* (n = 7), and *perceived behavioral control* (n = 4). Despite different theoretical origins [13], papers in our sample often used self-efficacy and perceived competence interchangeably [43, 83]. SDT posits that the need for competence drives individuals to master significant tasks [113], whereas Social Cognitive Theory defines self-efficacy as the belief in one's ability to achieve specific outcomes [13]. Bulgurcu et al. [24] proposed self-efficacy, along with behavioral beliefs and normative beliefs, as an antecedent of attitudes when introducing the Theory of Planned Behavior. However, Ajzen, who postulated the Theory of Planned Behavior, stated that perceived behavioral control, which is conceptually similar to self-efficacy, captures the extent to which an individual has the ability to perform the behavior and how much the behavior is under their control [3]. Taking this viewpoint into account, we grouped perceived behavior control with self-efficacy and perceived competence.

Autonomy-related (n = 14). Spreitzer defined one dimension of *psychological empowerment* as self-determination to "reflect autonomy in the initiation and continuation of work behaviors and processes" [135]. One of our reviewed papers used the term "choice" to refer to self-determination [43]. Scrutinizing their cited source [135], we included "choice" [43] as one adapted measurement of *autonomy*. Additionally, Gerdenitsch et al. [55] used the measurement of *decision-making autonomy* to capture whether workers are given the autonomy in their work to make their own decisions. Thus, we consider decision-making autonomy as one application of autonomy in the work context.

Perceived relatedness (n = 10). In the studies we reviewed, some scholars used the term perceived relatedness to capture an individual's connection to their digital information and online accounts [92, 104, 160]; whereas others suggest that the *camaraderie* and *enjoyment working with others* are notable motivators for cybersecurity advocates [63].

Protection motivation (n = 4). Protection motivation has been investigated in organizational settings, regarding employees' intention/likelihood of protecting themselves [51] and their organization [103, 109, 110] from security threats.

4.1.4 Value-driven motivators. These motivators are congruent with employees' endorsed goals, values, and ethics that are integrated into their identity [119].

Altruism (n = 1). Altruism was observed as motivating employees to help their colleagues with security-related problems, share their security knowledge, and reduce the workload of IT personnel [51]. Frank and Cohn suggested that altruistic values enhance extra-role security behavior, especially by promoting helpful behaviors, stewardship, civic virtue, and organizational loyalty [51].

Commitment (n = 8). Three studies tested the relationship between *affective commitment* and compliance behavior [109, 148]. Others examined *organizational commitment* more generally and defined it as employees' acceptance of an organization's information security goal and policy, along with a willingness to invest effort in information security [28, 38, 72]. Posey et al. [110] suggested that organizational commitment serves as the mechanism that makes workplace security threats personally relevant to employees.

Perceived value congruence (n = 3). Son [133] introduced the concept of *perceived value congruence* to measure the extent to which an employee and their employer share the same values. Chen and Li [28] used the same measurement items as Son [133], but they renamed the construct perceived value fit.

Organizational justice (n = 4). Li et al. examined organizational justice's role in motivating employees' internet policy compliance intentions [90]. They tested four dimensions of organizational justice (i.e., procedural, distributive, interpersonal, and informational justice [90]). Li et al. [90] hypothesized that the four dimensions of justice beliefs, when enforced within an organization, influence

Table 1: The taxonomy of autonomous motivation related to organizational security behaviors (N = number of reviewed studies that examined the motivator. *new categories proposed on the basis of the outcomes of the study).

Driver	Motivator and definition	N	Section
Interest-driven	• *Joy, Satisfaction, Curiosity (Intrinsic Motivation)*: employees engaging with an activity because they like the activity, enjoy doing the activity, or derive satisfaction from performing the task [130].	4	4.1.1
Task-driven*	• *Intrinsic Task Value*: the anticipated or actual enjoyment derived from engaging in a specific task (e.g., feeling rejuvenated or content) [48].	11	4.1.2
	• *Job Satisfaction*: satisfaction or positive emotions derived from one's job [148].	4	
Psychological Needs Fulfillment*	• *Competence-related*: includes (a) self-efficacy, which refers to the belief in one's ability to achieve specific outcomes [13], (b) perceived competence, and (c) perceived behavioral control.	24	4.1.3
	• *Autonomy-related*: an individual's perception of the extent to which they are engaging in an activity of their own choice [92, 95].	14	
	• *Perceived relatedness*: "the degree of connectedness an individual feels toward others when interacting in a specific context" [92, p.1212].	10	
	• *Protection motivation*: employees' intention/likelihood of protecting themselves and their organization from security threats [51, 109].	4	
Value-driven	• *Altruism*: people perceiving "the act of helping as enjoyable and interesting" [51, p.4].	1	4.1.4
	• *Commitment*: "an affective attachment to the organization" [94, p.539] and "a willingness to exert effort on behalf of the organization" [72, p.71].	8	
	• *Perceived Value Congruence*: the extent to which an employee and their employer share the same values [133].	3	
	• *Organizational Justice*: employees' perceptions of fairness in the processes and outcomes of organizational decisions [90].	4	
	• *Personal Responsibility*: employees' willingness to be accountable for their work-related choices, behaviors, and outcomes [71].	12	
	• *IS Identity*: a person's self-concept of their roles, responsibilities, and importance of complying with information security policies [103].	2	
	• *Normative Beliefs*: an individual's beliefs about whether important others or groups approve or disapprove of a specific behavior [2].	3	
	• *Employee Involvement*: personal norms [72], peer involvement [72], user-IS exchange [38], and management support [143] in the workplace.	5	
Expectation*	• *Perceived Benefits*: an individual's expectations of the benefits of performing a task, including saving time, convenience, increasing productivity [76], demonstrating impact [43], and making a difference [64].	4	4.1.5
	• *Response Efficacy*: an individual's belief in the effectiveness of a prescribed solution in mitigating the threat [92, 130].	12	

employees' workplace ethics and subsequently enhance their intentions to comply. Another two studies measured whether perceived fairness positively affected employees' attitudes toward ISP compliance [11, 89]. Son [133] introduced a similar concept, *perceived legitimacy*, which measures the extent to which employees view the ISP as appropriate, desirable, and just.

Personal responsibility (n = 12). When employees consider security actions to be more their responsibility than their employers', they are more likely to perform security actions [21, 51, 71], such as installing software updates [20]. We identified some constructs that are closely related to responsibility, including locus of control [72] and ownership [76]. Ifinedo [72] measured *locus of control* (which refers to the extent to which people believe they have control over the course of events [134]); however, the items involved the concept of responsibility, such as "the primary responsibility for protecting my organization's information belongs to others and not me" [72]. In a security context, psychological ownership can be defined as a feeling of possessiveness an individual develops for a security task [76]. Psychological ownership has been empirically tested to confirm its relationship with ISP compliance [76] and updating software [20]. Additionally, three studies investigated how *perceived excessive responsibility* influences employees' compliance [76, 78, 79], that is, employees' sense of going beyond their regular work duties [79].

Table 2: Excerpt of the overview of the applied measurements for autonomous motivation for all reviewed articles. (Note: DT = Deterrence Theory, EVT = Expectancy Value Theory, SDT = Self-Determination Theory, na = not available.)

Authors	Theoretical framework	Motivator	Measurement	Example	Source	Adaption
Alahmari et al. [4]	SDT	Psychological Needs Fulfillment	autonomy, competence, relatedness	na	na	na
Alhelaly et al. [5]	EVT	Interest-driven	Intrinsic Interest Value	In general, I find protecting my mobile identity is (extremely boring -extremely interesting).	[47]	yes
Alzahrani & Johnson [10]	SDT	Psychological Needs Fulfillment	autonomy, competence, relatedness (relation of needs to each other)	scale from 9-1 and 1-9 with competence and autonomy as end points	na	na
Alzahrani et al. [11]	SDT & DT	Psychological Needs Fulfillment, Value-driven	perceived autonomy/ relatedness/competence; perceived legitimacy; perceived value congruence;	na	na	na
...	...	...	...	...	...	...

Information security identity (n = 2). Employees' information security identity (IS identity) may be a driver of their compliance-based and voluntary security behaviors [103]. Two related constructs are *internalization of information security policies* (e.g., "I contribute to the organization by complying with its information security policy." [106]) and *internal perceived locus of causality* (e.g., "I comply with the requirements of the ISP because I want to find out how to ensure information system security." [83]).

Normative beliefs (n = 3) and *employee involvement (n = 5).* Normative beliefs and employee involvement have been examined as motivators of ISP compliance in the studies we reviewed. [24, 72, 83] examined the relationship between normative beliefs and ISP compliance intentions. In addition to being influenced by others, employees might be motivated to comply with ISPs for their own reasons. We put these motivators together with employee involvement, which includes *personal norms* [72] (personal belief in the relevance of complying), *peer involvement* [72] (actively involving oneself in information security), *user-IS exchange* [38] (employees' perceptions of and interactions with the information security department), and *management support* [28, 109, 143] (peer/higher management/technical support for information security).

4.1.5 Expectation motivators. Expectation motivators are related to the expected outcome and the perceived benefits of performing an activity.

Perceived benefits (n = 4). Even though the following concepts were labeled "intrinsic" and "satisfaction," when we scrutinized the measurement items, they focused on expectations of a certain reputation and better cooperation (*intrinsic outcome expectations*, [50]) and whether the solution would be efficient (cost/benefits) or effective in protecting the organization (*self-worth satisfaction*, [120]).

Response efficacy (n = 12). Response efficacy is one of the most frequently studied Protection Motivation Theory components [59]. Employees might evaluate the efficacy of following an organization's ISPs or performing preventive measures. Perceived high response efficacy motivates individuals to comply with ISPs [154] and engage in security behaviors [92].

4.2 Security behaviors related to autonomous motivation

All 45 of the papers we reviewed examined security behaviors or behavioral intentions as outcomes of autonomous motivation, along with other factors of influence. Except for four qualitative studies [21, 51, 63, 129], the remaining 41 studies used single questions, items, or log data to evaluate participants' security behaviors. We found that general ISP compliance and specific security tasks were often examined separately [20, 33, 51]. When switching from one security task to another, employees' intentions to perform a task can vary significantly [20]. Therefore, we present our findings of various security behaviors related to autonomous motivation in three categories: *information security compliance*, *extra-role security*, and *ISP violation behaviors*. See the overview of security behaviors related to autonomous motivation in Table 3. Similar to the excerpt provided in Table 2, we also provide an overview of the security behaviors and their measurements in the Supplementary Material to provide a useful toolbox for future research.

4.2.1 ISP compliance behaviors. ISPs prescribe employees' responses for securing corporate information [133]. Employees' compliance with the organization's ISP is the key to enhancing information security [24]. All our reviewed ISP compliance studies (n = 24) examined either respondents' self-reported behavioral intentions/attitudes or likelihood of performing specific tasks.

Intention to comply with the ISP (n = 16). Nine studies utilized the measurement proposed by Bulgurcu et al. [24] that includes three statements referring to complying with the ISP requirements, protecting information and technology resources, and carrying out the responsibilities prescribed by the ISP. Four studies used Herath and Rao's measurements [64] to indicate their likelihood and certainty of following the organization's ISP [64]. Hong and Xu [71] used a

Table 3: Security behaviors related to autonomous motivation. (Note: [38, 55, 77, 103] examined two types of behaviors in their study.)

Type of behavior	Behavior/Intention examined	Count
ISP compliance (n = 24)	Intentions to comply with ISPs	16
	Attitude toward ISP compliance	2
	Performance of specific compliance tasks	6
Extra-role (ER) security behaviors (n = 22)	ER behavioral intentions	1
	ER volunteering intentions	1
	Participation in ER behaviors	5
	Protection-motivated behaviors	2
	Security knowledge sharing	4
	Actions not prescribed in the ISP	7
	Cybersecurity advocates	1
	Attack-focused tasks	1
ISP violation behaviors (n = 3)	Insider computer abuse	1
	Instrumental policy abuse	1
	Infringing ERM rules	1

scenario-based scale to survey respondents' intentions to comply with the ISP. They adapted the scenarios from the four scenarios (user authentication and access control, hardware, software, and the network) created by Guo et al. [57]. Two studies [10, 11] did not specify their ISP measurement items.

Attitude toward ISP compliance (n = 2). Awudu and Terzis [12] examined respondents' evaluative judgments of the importance, necessity, benefit, and usefulness of complying with the ISP. Tejay and Mohammed [143] surveyed employees' perceived value and the effectiveness of the information security program in protecting critical information. Additionally, employees were asked to indicate their views on whether the security program balances risks with security controls [143].

Performance of specific compliance tasks (n = 6). Son [133] surveyed employees' compliance with tasks such as (a) accessing information assets, (b) communicating via email, (c) handling internet and network resources, (d) performing antivirus actions, and (e) preventing unauthorized access. Li et al. [90] investigated whether employees followed their organization's internet use policy, whereas Jeon et al. [77] examined employees' use of enterprise rights management (**ERM**) systems in their organizations. Two studies [54, 103] assessed employees' adherence to the organization's ISP, regarding protecting sensitive information, changing passwords as per policy, and securing workstations when unattended. Interestingly, Vedadi et al. [148] expanded the role of management in their data collection and instructed supervisors to rate their employees' security practices with respect to the discussion of sensitive information, compliance with security procedures, and adherence to information security rules.

4.2.2 Extra-role security behaviors. These behaviors comprise "spontaneous security actions that are not defined by organizational rules or policies" [51, p.2]. Examples include voluntarily helping others, actively intervening, accepting obstacles without complaint, and actively participating in improving security measures [51]. Twenty-two of the studies we reviewed examined such security behaviors that employees may view as extra-role security behaviors.

Extra-role behavioral intentions and participation (n = 7). Chen and Li [28] introduced *extra-role behavioral intentions* to assess employees' intentions to perform extra-role security behaviors in the workplace. They examined the extent to which employees promoted the information security program, put forth extra effort to enhance security, and voluntarily engaged in activities such as reporting risks or proposing new strategies [28]. Similarly, Davis et al. [38] used the concept *extra-role volunteering intentions* to survey employees' general intentions to engage in voluntary and proactive efforts to enhance information security. Furthermore, five studies asked employees to self-report their participation in extra-role security behaviors [55]. These self-reported questions were related to different aspects of organizational information security, such as helping colleagues/new employees learn about the ISP [103], evaluating the effectiveness of the system [127, 129], and reporting when suspicious emails had been received [106].

Protection-motivated behaviors (n = 2). Posey et al. [109] introduced protection-motivated behaviors (PMBs) to emphasize the critical role of employees' safe computing practices in organizational security. PMBs are defined as voluntary actions by insiders aimed at safeguarding both organizational information and the information systems that manage security threats [109]. In a multidimensional scaling study [108], Posey et al. categorized 67 PMBs into 14 clusters on the basis of levels of improvement needed, standardization and application, and reasonableness. These clusters include employees' behaviors, such as email handling, data protection, security training, software use, and account protection [108].

Information security knowledge sharing (n = 4). Information security knowledge sharing refers to sharing knowledge about information security to increase security awareness and mitigate security risks [51, 120]. Alahmari et al. [4] elaborated on the idea that security knowledge sharing implies a collaborative approach to cybersecurity, which is a powerful and efficient solution for mitigating cyber attacks. Frank and Ament [50] investigated the

motivational factors influencing employees' intentions to share their information security incident experience. They argued that communicating incident experiences in the workplace can act as a social learning strategy that allows employees to learn from their colleagues' security incidents [50].

Security actions not prescribed in the ISP (n = 7). Researchers investigated a range of security actions that might enhance organizational information security, even though these actions were not outlined in the ISP [21, 54]. Blythe and Coventry [20] examined employees' intentions to *scan USB sticks* with anti-malware software and *install software updates promptly*. Alhelaly et al. looked into the motivational aspects of *mobile identity protection* due to the significant amount of important data stored on these devices [5]. Ogbanufe et al. [104] examined factors that motivate employees to voluntarily *adopt multifactor authentication*. Finally, Menard et al. [92] and Yang et al. [160] explored the application of security messages that appeal to individuals' psychological needs as a method for encouraging people to *adopt password managers*.

Roles of cybersecurity professionals (n = 2). Haney and Lutters [63] examined the work motivation of *cybersecurity advocates*. These security professionals promote, educate, and motivate workers to adopt the best practices for security in the workplace [63]. Hodges and Buckley [70] examined differences in motivation and self-efficacy between two cybersecurity behaviors: *attack-focused tasks* (e.g., red-teaming and exploit development) and defense-focused tasks (e.g., network design and policy writing). They asked security professionals to estimate the ratio between the amount of defense-focused work and attack-focused work they performed [70].

4.2.3 ISP violation behaviors. Three studies examined employees' organizational ISP violation behaviors. These behaviors include insider computer abuse [27], instrumental policy abuse [151], and infringing ERM rules [77]. *Insider computer abuse* refers to unauthorized and deliberate employee behaviors that harm organizational information assets [27]. Welck et al. [151] argued that enterprises rely on information technology to facilitate work tasks, and merely prohibiting harmful use through security policies often leads to employees' *policy abuses*. Similarly, Jeon et al. [77] examined employees' behaviors with respect to *infringing ERM rules*, for example, accessing information through a borrowed account.

4.3 Applied theoretical frameworks and key findings

Among the 45 reviewed papers, 24 different theoretical frameworks related to autonomous motivators were mentioned. We include a glossary of these frameworks in **Appendix A**. SDT was the most frequently cited (n = 16), followed by Protection Motivation Theory (n = 7), Theory of Planned Behavior (n = 6), and Deterrence Theory (n = 3). In the following subsections, we summarize the key findings from the reviewed papers on the basis of the approaches the studies used to engage the theoretical frameworks, that is, deductive, inductive, and design approaches [44]. Two papers [79, 127] did not indicate a specific theory in their research; thus, we exclude them from this subsection leading to 43 papers.

4.3.1 Deductive approach (n = 35). The deductive approach refers to papers that test predefined hypotheses or research models. Online surveys were used most frequently in the reviewed papers. Most authors chose this methodology to test the assumed relationships between the constructs from their conceptualized research models. This process included (a) verifying whether a theoretical framework from other disciplines was useful for interpreting IS topics [38]; (b) comparing two theoretical frameworks to examine which one provided more explanations about IS phenomena [92]; and (c) extending an established theory with constructs from another theory [72] or factors of influence identified in prior studies [20]. We apply our proposed taxonomy to summarize the findings from the reviewed studies (deductive approach) and provide an overview in Table 4.

Intentions to comply with/attitude toward ISPs. From studies examining the antecedents of employees' ISP compliance, we found that some autonomous motivators were consistently related to employees' intentions to comply/attitude toward compliance, whereas others demonstrated non-significant or mixed results:

- **Significant antecedents**: Intrinsic task value [89], Job satisfaction [71, 148], Autonomy-related [11], Perceived relatedness [11], Personal responsibility [71, 72, 76, 78], Perceived value congruence [11], Normative beliefs [24, 83, 148], Commitment [148], Perceived benefit [76], and Response efficacy [154].
- **Mixed results**: Competence-related [11, 24, 72, 78, 154].
- **No significant effects**: Organizational justice [89].

Compliance with specific security tasks. Li et al. [90] found that personal responsibility (work-related ethical beliefs) had a positive impact on employees' internet use policy compliance than the sanction-based approach (sanction severity and certainty). Organizational justice (procedural and distributive justice) had a positive impact on compliance intentions directly and indirectly by fostering work ethics [90]. Similarly, the autonomous motivators (perceived legitimacy and value congruence) contributed significantly more to the explained variance in employees' compliance than extrinsic motivators (deterrent certainty and severity) [133]. Furthermore, Ogbanufe and Ge [103] revealed that whereas protection motivation and IS role identity were positively related to compliance behaviors, intrinsic task value did not demonstrate a significant relationship with in-role compliance. Empowerment-based ERM can enhance employees' perceived responsibility and benefits; however, this empowerment does not lead to increased compliance with ERM regulations [77].

Extra-role and protection-motivated behaviors/intentions. Employees who internalized information security policies self-reported more security practices compared with those who merely complied with the policies [106]. Perceived control, IT competence, and user-IS exchange are positively associated with information security commitment [38]. Information security commitment [28, 38] promoted employee participation in extra-role behaviors. Organizational commitment made information security threats personally relevant to employees [110]. Whereas intrinsic task value and IS identity were positively related to extra-role security behaviors, protection motivation was negatively related to extra-role security

Table 4: Security behavior/intentions and autonomous motivation matrix from the studies we reviewed utilizing the deductive approach. (Note: n = the number of security behaviors that have been examined more than once; non-sig = the motivator did not demonstrate statistical significance, otherwise, the motivator was found to be significant; mixed = the motivator had mixed results regarding significance from different studies on the behavior type; inversely = the motivator is inversely related to employees' intentions to perform the behavior; otherwise, the motivator was found to be positively related to employees' intentions to perform the behavior. Motivators related to security behavior or intentions via a moderator are not included in this table.)

	Expectation	Value	Needs fulfillment	Task	Interest
Intention/attitude to comply with ISPs	Perceived benefit; Response efficacy	Organizational justice (non-sig); Commitment; Personal responsibility (4); Perceived value congruence; Normative beliefs (3)	Autonomy-related; Competence-related (mixed, 5); Perceived relatedness	Intrinsic task value; Job satisfaction (2)	
Compliance with specific security tasks	Perceived benefits (non-sig)	Organizational justice (2); Personal responsibility (mixed, 2); Perceived value congruence; IS identity	Protection motivation	Intrinsic task value (non-sig)	
Extra-role and Protection-motivated behaviors/intentions	Response efficacy; Perceived benefits	Perceived value congruence; IS identity (2); Normative belief (2); Commitment (mixed, 2)	Competence-related; Protection motivation (mixed, 2)	Intrinsic task value (2); Job satisfaction (non-sig)	
Security knowledge sharing	Perceived benefits	Normative beliefs	Competence-related		Intrinsic motivation
Actions not prescribed in the ISP	Response efficacy (4)	Personal responsibility (mixed, 4)	Competence-related (mixed, 5); Autonomy-related (3); Perceived relatedness (mixed, 2)	Intrinsic task value	
Attack-focused tasks			Competence-related	Intrinsic task value	
Insider computer abuse		Personal responsibility (inversely)			
Instrumental policy abuse	Response efficacy (inversely)		Autonomy-related (inversely)		
Infringing ERM rules	Perceived benefits (inversely)	Personal responsibility (inversely)			

behaviors [103]. Response efficacy showed a strong positive correlation with both protection motivation and self-reported engagement in protection-motivated behaviors [110]. While management support had a significant effect on insiders' protection motivation [110], increased job satisfaction did not significantly impact their protection motivation [109]. Intrinsic task value and perceived benefits significantly influenced an individual's intention to protect their mobile identity [5].

Security knowledge sharing. Perceived benefits (e.g., reputation and sense of accomplishment) were more effective at encouraging the sharing of incident experiences than external rewards such as incentives [50]. Perceived behavioral control and normative beliefs also significantly influenced employees' sharing intentions [120]. Additionally, intentions to share and trust had significant effects on security knowledge-sharing behavior within organizations [120]. Satisfaction of curiosity positively influenced employees' intentions to share knowledge within information systems, mediated through their attitudes [120].

Actions not prescribed in the ISP. Response efficacy significantly facilitated anti-malware behaviors [20]. Employees with a stronger sense of personal responsibility for security had greater intention to engage in anti-malware software and software updates [20]. Self-efficacy emerged as the strongest predictor of both anti-malware software use and email security behavior but had no impact on software update behavior [20]. In another study, Blythe et al. [21] found that whereas employees accepted some responsibilities, they diffused others onto their organization [21]; additionally, low response efficacy, driven by a lack of feedback on the effectiveness of employees' responses, was identified as a potential barrier to certain security practices [21]. Furthermore, Ogbanufe et al. [104] revealed that autonomy and relatedness exhibited significant correlations with intrinsic task value, whereas competence did not. Subsequently, intrinsic task value was significantly associated with

the voluntary use of multifactor authentication [104]. Perceived autonomy, competence, and relatedness were significantly related to home users' intention to install a password manager [92]. However, in a replication study with organizational users, Yang et al. [160] found that only autonomy demonstrated significant correlations. Lastly, in a survey with 137 cybersecurity professionals, Hodges and Buckley [70] found that individuals who chose to focus more on *attack tasks* were more internally motivated, with a higher intrinsic task value and higher self-efficacy than those focused on defensive tasks.

ISP violation behaviors. The reviewed studies suggested that empowering employees and fostering their sense of responsibility can serve as remedies for curbing behaviors that violate rules in organizations [27, 77]. Jeon et al. [77] indicated that granting employees the autonomy to access information within a defined set of rules leads to greater perceived benefits and an added sense of responsibility compared with those using control-based systems, which reduce users' intentions to circumvent access rules [77]. In an online vignette experiment, Welck et al. [151] found that two dimensions of psychological empowerment, self-determination (autonomy) and impact (response efficacy), had a significant negative effect on employees' intentions to abuse the rules [151]. Burns et al. found that employees' perceptions of maladaptive financial benefits and psychological contract violations were positively related to insider computer abuse [27]. Employees' personal responsibility (self-control) was found to negatively moderate the relationship between their abuse motives and insider computer abuse.

4.3.2 Inductive approach (n = 3). We categorize papers as inductive if their approach was to derive theoretically cohesive abstractions from observations. Frank and Kohn [51] examined various types of extra-role security behaviors and their motivators by conducting in-depth interviews (n = 29). They found that interest, competence, autonomy, and a sense of connection influence these behaviors. Employees exhibited different extra-role security behaviors based on distinct motivational factors, suggesting the need for targeted interventions. Organizations should also identify highly motivated employees and clarify the boundaries of acceptable extra-role security behaviors. Through interviews with cybersecurity professionals (n = 28), Haney and Lutters [63] identified several intrinsic drivers of cybersecurity advocacy, including interest, a sense of duty, self-efficacy, evidence of impact, camaraderie, and, to a lesser extent, awards and monetary compensation [63].

In a case study of Ghanaian government employees, Awudu and Terzis [12] explored attitudes toward ISP compliance and perceptions of intrinsic and extrinsic rewards. Their findings indicate that, despite the absence of a formal ISP and related training, a positive information security culture existed within the organization [12]. Employees recognized the necessity, benefits, and importance of the ISP, and they felt content, satisfied, accomplished, and fulfilled when they adhered to it. However, perceptions of extrinsic rewards were less clear. Whereas experienced staff reported that they generally believed that extrinsic rewards do not motivate compliance, the viewpoints of inexperienced staff were uncertain [12].

4.3.3 Design approach (n = 5). Here, we refer to papers that adopt theories to inform the design of a tool, intervention, or product. Silic and Lowry [130] tested a **gamified security training** versus an email-based training in the field. Their longitudinal findings suggested that the gamified training inherently motivated employees to learn and adhere to security policies, and perceived intrinsic usefulness and curiosity increased employees' behavioral intentions to follow security policies [130]. Similarly, Alahmari et al. [4] designed a **mobile intervention** by using elements such as badges and a leaderboard to encourage sharing of security knowledge in the workplace. The intervention, designed to address employees' basic psychological needs, improved their knowledge of and their responses to security incidents, in comparison with the control group [4].

Shojaifar et al. [129] introduced CYSEC, an automated cybersecurity **communication tool** designed to promote cybersecurity practices in the workplace. The tool leverages SDT constructs to guide and motivate companies toward adopting effective cybersecurity measures. Their observations indicated that enhancing self-efficacy positively influenced users' self-motivation, whereas providing choices supported both autonomy and self-motivation [129]. Lastly, two studies combined constructs of SDT with established **assessment methods**. Alzahrani and Johnson [10] developed a questionnaire, using the Analytic Hierarchy Process method, to survey the weights for autonomy, competence, relatedness, and behavioral intentions to comply with ISP. Gangire et al. [54] created an information-security-compliant behavior questionnaire with questions related to competence, relatedness, and autonomy based on the Human Aspects of Information Security Questionnaire (**HAIS-Q**).

4.4 Study contexts and control variables

We analyzed the context-related and control variables of all 45 papers. Below, we highlight the more widely reported and impactful contextual factors. A complete overview of the demographic and contextual factors can be found in the Supplementary Material.

4.4.1 Study context: Demographic information. The number of participants in the papers varied, ranging from 15 to 993 participants. Naturally, quantitative papers tended toward a larger sample size with a median of 289. For qualitative papers, the median number of participants was 25.

Ten papers did not report participants' ages, and two more provided only very vague information. However, of those 12 that reported, the median mean age was 38.43. The remaining papers provided age ranges, where 16 reported the largest proportions for groups between 25 and 49 years of age. Overall, only few papers investigated very young or older participants as a primary target population, with two papers reporting a large proportion of participants below 25 [5, 12] and three papers reporting a large proportion of participants above 50 years old [89, 90, 154]. None of the papers reported any age-based recruitment criteria.

Nine papers did not report participants' gender. The majority of the remaining papers reported a balanced distribution of genders, whereas 12 papers had a skewed proportion where any gender took up more than 60% of the entire sample. Of these, seven were skewed toward a male population, whereas five were skewed toward a female population.

Geographical location. The majority of studies took place in Western countries, with a particular focus on the United States. Seven

online studies did not specify the location or geographic composition of its sample. Geographical locations are summarized in Table 5.

Table 5: Geographical areas of studies.

Region	Count
North America	17
Europe	7
Other Western	1
Middle East	4
East Asia	7
Africa	2
Not specified	7

Industry. The studies collected data from people who were actively employed, although industry was not always explicitly stated. There were a broad variety of sectors, and education, finance, government, and healthcare were prominent in the reviewed studies.

Job roles. Most papers investigated employees in general, irrespective of their exact job role. Whereas some papers investigated specialized groups, such as cybersecurity specialists [63, 70] or security managers [10], the studies did not explore differences between these groups and other employees or roles.

4.4.2 Control variables in the studies and their findings. Of the 40 papers employing quantitative analyses, 20 reported the use of control variables. We provide an overview of the frequencies of these control variables and their impacts in Table 6. In all cases, age was used as a control variable. Gender and education were used in 18 and 12 papers, respectively. We grouped together control variables that determined the degree of experience an employee might have, such as tenure with an organization, general job market experience, or amount of experience with specific systems. 12 papers controlled for these factors. Finally, 12 papers also controlled for factors indicating either job role or job status, such as whether an employee was a specialist or was working in a managerial position. A few papers also controlled for various other factors such as organization size [11, 38, 64, 83], self-efficacy [154], or security-related awareness [38].

A total of 18 papers reported on the effects of control variables. Of these, three found no significant influence of any variable. In the following, we detail any control variables for which significant effects were reported in more than one case. Age appeared to have a positive influence on compliance intentions and behavior in some cases, with ten papers reporting no significant effect and five papers finding that older individuals showed more security intentions and behavior [11, 78, 79, 90, 154]. Gender seemed to have minor influence overall, with no significant effect reported in 11 papers but women demonstrating higher compliance intentions in two cases [64, 72]. The effects of other variables were less clear. Education was reported as not significant nine times, whereas significant effects were reported three times, with one paper stating a positive relationship between education and extra-role behavioral intentions [28], and two showing that it decreased information security engagement intentions [11, 38].

Although several studies investigated job role or managerial status, the variables were not consistently applied or measured. However, the three papers that reported on their effects noted positive influences of higher specialization or managerial status, such as increasing protection motivation [110] or perceptions of success [143]. Computer self-efficacy showed mixed effects, in two cases decreasing security compliance intentions [78, 79] and in one case increasing compliance behavior [133]. Finally, a variety of general security awareness or knowledge of specialized systems were positively associated with security engagement and behavioral intentions (e.g., [38, 78]).

4.5 Future study opportunities suggested in the reviewed papers

We systematically analyzed the future work and study limitations discussed by the authors of our reviewed papers. We coded and categorized the extracted 130 suggestions into the following four themes:

4.5.1 Theoretical framework refinement, integration, and testing (n = 33). Testing and refining theoretical frameworks (both established theories and conceptual models) is essential for advancing cybersecurity research [64, 92]. Existing models, such as SDT and Protection Motivation Theory [92, 109], require ongoing refinement to maintain their relevance in security behavioral research. Researchers should integrate meaningful constructs [64, 92] into their research models to increase the explanatory power. Furthermore, researchers have called for new paradigms in security behavioral research [92, 133]. For instance, Burns et al. [27] advocated for a paradigm shift from Deterrence Theory to theories that emphasize self-control and motivation. Similarly, authors have recommended investigating how organizational commitment [110], autonomy [78], emotion [43], and psychological empowerment [142] are related to security behaviors, as well as the antecedents of these psychological constructs [43, 154]. Additionally, the authors proposed interdisciplinary perspectives for enriching human-centered security research. Tejay and Mohammed [143] argued for the incorporation of theories from anthropology, which could introduce new perspectives to cybersecurity culture that are currently underexplored. Finally, it is crucial to test and apply research models to different types of behaviors to validate their robustness and explainability [109], ensuring that these theories can be utilized to address different cybersecurity challenges.

4.5.2 Methodology improvement (n = 54). A total of 54 recommendations focused on improving research design, measurement, and data collection. First, many authors advocated for the use of longitudinal research designs to capture changes in behavior over time [38, 64, 89, 103] and to unveil causal relationships between motivators and security behavior. Some authors proposed that qualitative methods should be utilized, such as case studies [24], observation [63], and focus groups [72], to investigate psychological constructs and behaviors in more depth. Several authors emphasized the need to incorporate additional control variables, such as geography [5], education [5], and social desirability [64], to improve the accuracy of research findings. Second, a significant number of authors

Table 6: Control variables and their impact.

Attribute	Count	Impact
Age	20	Higher age can increase compliance intentions and behavior.
Gender	18	Women can demonstrate higher compliance intentions.
Education	12	Mixed effects.
Experience	12	No statistically significant effect reported.
Job role/Status	12	Generally positive influences of more specialized and hierarchical positions.

suggested future work to improve the measurements of motivators [83] and security behaviors [90], including developing more valid scales [83] and triangulating self-reported data with objective logs [92, 104], as self-reports can induce biases [89]. Third, randomized sampling [54] and the inclusion of diverse participants from different organizations [11] and various job roles (e.g., management, external stakeholders [12]) are recommended to ensure the robustness of the findings. Fourth, to enhance the generalizability of research findings, several authors proposed that studies should be replicated across different organizations [77] and that the research models should be tested with specific ISPs [24]. These suggestions call for rigorous methods, data collection, and the use of both qualitative and quantitative approaches to improve research on information security behaviors.

4.5.3 Examining personal, organizational, industrial, cultural, and contextual differences (n = 21). To mitigate potential biases in cybersecurity, it is essential to study underinvestigated sectors and demographics to extend beyond heavily regulated industries and traditional geographic regions [10, 148]. More diverse research samples should be used across industries, departments, and occupations to improve the validity of findings [79]. Future research should also explore cultural influences on security behaviors, as factors such as national culture [143] and individualism [109] may significantly impact employees' security decisions. Conducting cross-cultural studies can further illuminate how security behaviors vary across different social environments [50, 143]. Moreover, examining individual differences [27], such as personality traits [43, 90], is crucial for developing a better understanding of employee security behaviors; for example, personality differences might vary their acceptance of intrinsic and extrinsic appeals [90]. Finally, organizational contexts, including policies [55], security task characteristics [43], and leadership dynamics [55], also play a vital role in shaping employee behaviors.

4.5.4 Intervention design and practical application (n = 22). Many authors suggested that organizations should promote organizational culture and foster an ethical climate that is aligned with personal values [28], create interventions based on specific industry needs [77], and embed security responsibilities within the organizational culture [21]. Encouraging creativity [70] and collaboration [120] in cybersecurity practices might enhance their effectiveness. Several authors proposed that employees' needs for autonomy, competence, and relatedness should be fostered in the workplace to improve their security behaviors [71, 92]. Employees should be provided with the freedom to control their tasks, which can reduce negative emotions and increase compliance intentions [79]. Additionally, some authors suggested that gamification and innovative media should be incorporated into security training to engage employees [130]. The gap between static training and evolving threats was noted, with recommendations for more iterative and dynamic training approaches [4]. Furthermore, the authors highlighted the role of empowerment in promoting cybersecurity compliance. Empowering employees to participate in decision-making and feel more autonomous was also seen as crucial for enhancing job satisfaction and organizational commitment [43, 71]. These suggestions call for a shift toward more culturally aligned, autonomous, and empowerment-focused approaches in cybersecurity.

5 Discussion

We provide an overview of the key findings in Table 7. Next, we discuss the development of our taxonomy, practical implications of our review, and suggestions for future studies.

5.1 A taxonomy of autonomous motivation related to organizational security behaviors

Reflection on the role of theories in our work: We began with the definition of autonomous motivation proposed in the SDT framework [41]. After analyzing the reviewed papers, we found that neither the SDT motivation continuum [116] nor the SDT-ER taxonomy [51] could accommodate the five groups of autonomous motivators identified in the reviewed empirical studies. Therefore, we introduced two core constructs — intrinsic (task) value and expectation, from Expectancy-Value Theory [48] — into the SDT-ER taxonomy and integrated psychological needs fulfillment as an additional reason for behavior. See the taxonomy of autonomous motivation related to organizational security behaviors in Figure 4. The following rationales support our adaptation:

- The reviewed studies [71, 148] suggested that job satisfaction has a positive association with ISP compliance behavior. [71, 148] defined job satisfaction as the pleasurable or positive emotional state resulting from one's job or job experience. Job satisfaction cannot readily be categorized into the three categories in the SDT-ER taxonomy, i.e., usefulness-driven, value-driven, and interest-driven motivators. We propose a new category "task-driven" to accommodate job satisfaction because it emphasizes the enjoyment individuals derive from an activity [48]. Thus, job satisfaction and *intrinsic task value* were incorporated into the taxonomy under the task-driven category.
- In the SDT framework, "satisfying human needs for competence, relatedness, and autonomy creates sustainable (i.e., enduring) motivation" [137, p.77], namely, autonomous motivation. However, multiple reviewed studies have suggested

Table 7: Summary of key results.

Research Questions (RQs)	Key results
RQ1. Forms of autonomous motivation (section 4.1)	We developed a refined **taxonomy of autonomous motivation** related to security behaviors and categorized 17 unique motivators into five groups: interest-driven, task-driven, psychological needs fulfillment, value-driven, and expectation.
RQ2. Related security behaviors (section 4.2)	The most examined security behavior in the reviewed studies were ISP compliance behavior/intention (n = 24), followed by extra-role security behaviors (n = 22). Additionally, three studies investigated employees' ISP violation behaviors.
RQ3. Applied theoretical frameworks and findings (section 4.3)	**24 theoretical frameworks** have been applied to study autonomous motivators. The most frequently applied theories were Self-Determination Theory (n = 16), Protection Motivation Theory (n = 7), and Theory of Planned Behavior (n = 6). The most frequently examined autonomous motivators were competence and personal responsibility, with mixed results (some studies found statistically significant effects, while others did not). **Commitment, perceived value congruence, information security identity, perceived benefit,** and **intrinsic task value** were less studied but seem to be positively related to several security behaviors. Autonomous motivators have **positive relationship** with ISP compliance behavior/intention and extra-role security behaviors, and some motivators (i.e., response efficacy, personal responsibility, and autonomy) **are inversely related to** ISP violation behaviors. The majority of studies in our review adopted deductive approaches (n = 37), with only **three** employing inductive methods and **five** using design-based approaches. Among the 45 papers reviewed, we found only **one** longitudinal study (six months) and **one** replication study.
RQ4. Study contexts (section 4.4)	**Most examined regions** were: North America (n = 17), Europe (n = 7), and East Asia (n = 7). Education, finance, government, and healthcare were the most studied **sectors**. Of the 40 papers employing quantitative analyses, **only 20** reported the use of control variables. Age, gender, education, and job roles might influence employees' security behaviors.
RQ5. Promising avenues (section 4.5)	Theoretical framework refinement, integration, and testing. Methodology improvement: longitudinal designs, more qualitative studies, better measurements and sampling, inclusion of control variables, and replication studies. Examining personal, organizational, industrial, cultural, and contextual differences. Intervention design and practical application.

that these motivators and protection motivation are *directly* related to employees' security behavioral intentions, not necessarily through moderators [11, 110, 160]. Thus, we created the new category in our taxonomy: "psychological needs fulfillment."

- We proposed to use "expectation," instead of usefulness-driven, to categorize response efficacy and perceived benefits to express their future-oriented nuance. According to Expectation-Value Theory, *expectation of success* is one of the core constructs that directly influence individuals' choice of performing an activity [30, 48]. The measures of response efficacy and perceived benefits assess employees' anticipated outcomes (e.g., securing the workplace network [20]) of the recommended security actions using future-oriented language. These outcomes are neither static nor aligned with the concept of "usefulness" in relation to employees' job roles. For this reason, we integrated expectation into our taxonomy.

This review makes a theoretical contribution by clarifying a construct emphasized by multiple theories and carefully aligning the findings from reviewed empirical studies with established theories. This approach resulted in a theoretically robust and practically relevant taxonomy, demonstrating the potential for fostering autonomous motivation and promoting security behaviors in organizations. Behavioral security scholars can draw inspiration from studies that employ relevant theoretical frameworks. For example, through the lens of SDT, the **social condition and process** that provide rationale for the activity, acknowledge individuals' perspective and feelings, and support their experience of choice (while minimize the use of pressure) foster autonomous motivation [40]. In practice, interventions targeting management stakeholders have been carried out to change organizational climate, with the goal of improving employees' satisfaction and trust in the organization [131]. Further, task challenges **at moderate levels** strengthens employees' autonomous motivation, hence, simulating their work-related well-being [140]. These findings could be leveraged to improve cybersecurity management and security task design at the workplace.

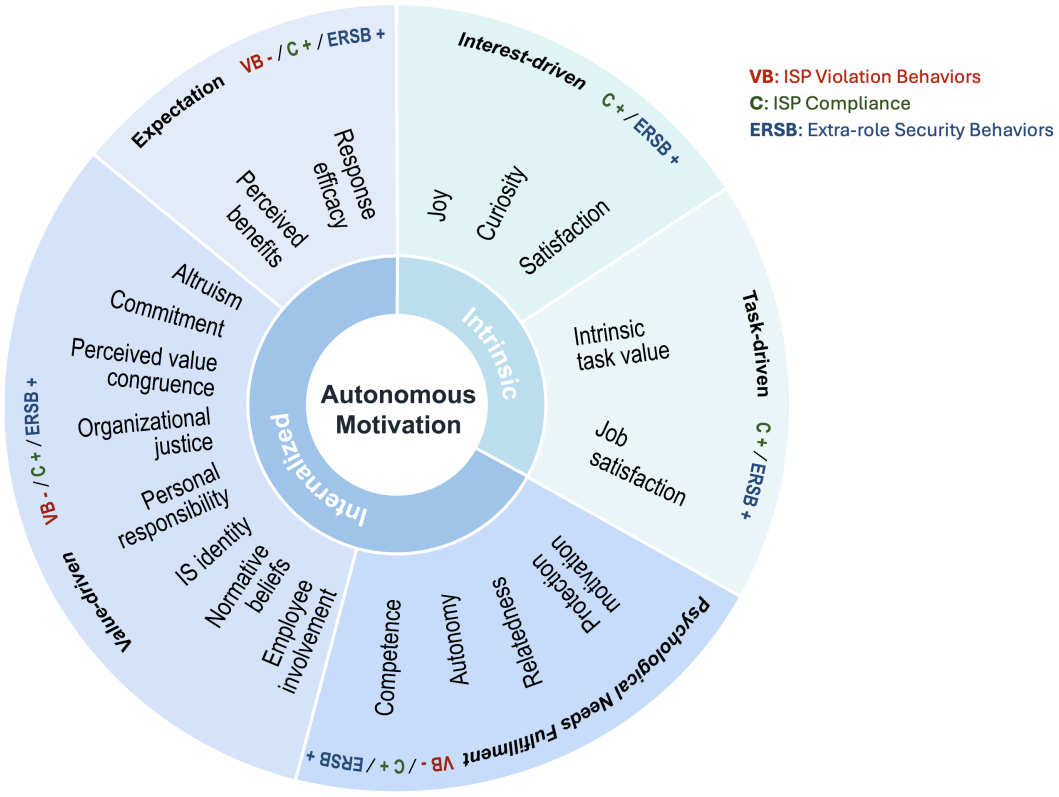

Figure 4: The taxonomy of autonomous motivation related to organizational security behaviors (based on the work of [41, 51]; -/+ indicates that at least one motivator from the located category is negatively (-)/positively (+) related to the behavior).

How autonomous motivators influence employees' organizational security behaviors: Applying our taxonomy to analyze the findings from reviewed studies, we found that all five categories of autonomous motivation demonstrated positive statistically significant relationships with employees' intentions to comply with ISPs (see Table 4). [130] achieved a significant result with a design-based approach (not included in Table 4). This suggests that all categories of autonomous motivators might positively influence employees' intentions to comply with ISP in organizations.

Among all the motivators, personal responsibility and competence-related motivators were examined the most, with mixed results (some studies demonstrated significance, whereas others did not; see Table 4). Given the diverse demographics and contexts of the papers we reviewed, this result requires further scrutiny. Other motivators, such as commitment, perceived value congruence, IS identity, perceived benefit, and intrinsic task value were less studied but were positively associated with several security behaviors.

Autonomous motivators were not only positively associated with compliance behaviors and extra-role security behaviors but also inversely related to violation behaviors. Specifically, personal responsibility, response efficacy, autonomy, and perceived benefits were found to be negatively associated with employees' violation behaviors (see Table 4). Only three studies investigated employees' violation behaviors, partly due to a scarcity of research on employees' risky cybersecurity behavior [7]. These previous findings suggest that autonomous motivation may help reduce employees' violation behaviors.

5.2 Practical implications

5.2.1 Human-centered security and autonomous motivation. Autonomous motivation is instrumental to design user-centric security policy and interventions. One prominent theme of human-centered security is the user-centered design of security mechanisms. *User needs* have long been emphasized as a primary design goal when developing usable and secure systems [163]. Security mechanisms and policies that fail to consider employees' job contexts, the feasibility of organizational strategies, and usability issues reduce employees' *motivation to engage* with security measures [1]. Nevertheless, studies show that security measures still cause frictions [15] and security officers "regularly shift responsibility either to the management (by demanding more support) or to the employees (by blaming them)" [67, p.2311]. Other streams of research within the community examined the behavioral aspects of organizational security, such as the learning curve of security behavior [66, 121], designing tools to aid security tasks [18], and creating engaging experiences for security learning [52]. The autonomous motivation reviewed in this study can influence an employee's decisions on

whether to perform a security behavior when they are capable and to engage with non-mandatory security tasks. When security mechanisms align with employees' interests, tasks, psychological needs, values, and expectations, the associated behaviors are more likely to be accepted and maintained.

5.2.2 Empowering employees. Multiple authors [43, 151, 161] have suggested empowerment as a complementary measure to technical measures and sanctions in promoting compliance and preventing ISP violations. **The empowerment approach** emphasizes that people's strengths and abilities should be identified and built upon, rather than blaming them for their difficulties [107]. Empowerment can influence employees' security behaviors through different approaches [30, 43, 77]. First, psychological empowerment positively influences employees' ISP compliance intentions [142]. Second, empowerment also informs the design of management tools [77]. For example, an empowerment-based management system has demonstrated the potential to minimize the circumvention of access rules [77]. Finally, when an employee feels empowered, they are more likely to engage in proactive security behaviors, such as becoming security champions, i.e., proactive security advocates who often have a good knowledge of security practices and can promote security culture among employees [53, 58, 93, 141]. While research showed that this promising approach faced certain challenges in the past, such as the selection of appropriate people [16, 53] and difficulties arising based on a lack of management support [58], our findings might inform criteria for the successful implementation of a security champion program. For example, people with high autonomous motivation might be good candidates for becoming security champions. To foster or maintain that motivation, security champions should not only be appointed without further rights, but also be enabled to act and be included in the development and discussion of security measures.

Security training programs, access to security strategies, and inclusion in decision-making have been shown to enhance employees' psychological empowerment, as highlighted by [142]. Moreover, employees' perceptions of managerial practices, workplace support, leadership, and work design characteristics significantly impact their sense of empowerment [126]. Building on these findings, our taxonomy of autonomous motivation could be a useful tool for organizations aiming to enhance the perceived fairness of their information security policies, align work environments with employees' internal values, and foster a stronger information security identity. By integrating autonomous motivation into these efforts, organizations can not only empower their employees but can also promote employees' engagement in security practices. In the following subsection, we use the designing of security training programs as an example to illustrate how the taxonomy of autonomous motivation can be applied in practice.

5.2.3 Evaluating and improving security training programs. Security managers deploy "a combination of tangible activities, material delivery, and ongoing engagement" with the goal of raising employees' security awareness [68]. Employees often perceive these activities as a burden and disengage with security training [30]. Some researchers [14, 123] suggest using tools such as scenario-based surveys, HAIS-Q, or Security Attitude Inventory (SA-13) to differentiate employees and deliver targeted interventions for specific employee groups, to avoid burdening employees with unnecessary interventions. Others propose to improve the training design to engage employees with intrinsic motivation being frequently applied as a guiding principle in designing awareness campaigns [29], particularly in gamified training [130, 145]. This approach often integrates intrinsic motivators such as joy, curiosity, and satisfaction, into the learning experience and has demonstrated its effectiveness [130, 155]. As noted by Bennett and Mekler, in the Human-Computer Interaction (**HCI**) and user experience (**UX**) communities, "very little attention has been paid to motivational factors related to the outcomes of the activity, and how these relate to the values and goals users bring to the interaction" [17, p.26]. Which opportunities exist for organizations to apply autonomous motivators to evaluate and improve security training?

Security managers can apply the constructs from the taxonomy of autonomous motivation to audit the training (e.g., perceived benefits: "How well does the training benefit employees and enhance their knowledge in protecting against attacks?"). They can utilize motivators to collect employees' feedback on the training (e.g., competence: "To what extent do you feel the training has improved your ability to identify incoming threats?"). Involving employees in the training design process and ensuring organizational transparency and fairness can improve their engagement. Additionally, management can support employees by addressing technology-related frustrations (leading to higher job satisfaction) and encouraging self-development in technology use (e.g., enhancing personal competence and fulfilling curiosity). Moving forward, organizations should consider conducting regular evaluations of their security awareness campaigns to ensure ongoing relevance and effectiveness [68].

5.3 Looking into the future of autonomous motivation in human-centered security

5.3.1 Recommendations for conducting theory-informed studies. Throughout our review, we encountered the following challenges at least once (see Table 8). However, we deliberately avoid pointing out individual papers to maintain a focus on providing constructive and future-oriented recommendations for avoiding pitfalls and enhancing the transparency and replicability of research.

5.3.2 Future avenues. Our analysis of suggestions in the reviewed papers identified four future directions for security behavior studies (see section 4.5). Regarding publication venues, information system journals seem to be in favor of deductive methodology and studies with clear theoretical contributions. Much of the reviewed design-based and inductive studies were published in interdisciplinary journals, as well as security and privacy venues that commonly accept HCI studies. Only three of the reviewed studies examined beyond general roles, that is, cybersecurity specialists [63, 70] and security managers [10]. Stakeholders that design cybersecurity policy and manage cybersecurity tasks (e.g., CISOs and system administrators) are under-represented in our review. Ensuring organizational security is their primary task, unlike most employees for whom security is usually a secondary task [156]. Security professionals usually have higher cybersecurity expertise as compared to general employees. Based on these differences, it would be highly

Table 8: Observed challenges and our recommendations in conducting theory-informed studies.

Observed challenges	Recommendations
Theories	
• Naming theories with terms different from those used in cited sources.	• Maintain consistency in terminology by using the same names for theories as those found in cited sources.
• Introducing one theory in the related work section while using another theory for measurement.	• Ensure consistency by clearly explaining the choice of theory in both the related work and measurement sections.
• Categorizing autonomous motivators under terms that differ from the theoretical framework, such as classifying them as intrinsic motivation when based on SDT.	• Use terminology that accurately reflects the theoretical framework and definitions of the constructs.
• Stating theoretical propositions without correct or sufficient citations.	• Provide accurate citations to support all theoretical propositions, ensuring the relevance and quality of the sources.
• Lack of linkage between the introduced theory and the proposed research model.	• Clearly present the research model and state how the theory informs the model.
Measurement	
• Using the same measurement as the cited source, but giving it a different name.	• Standardize measurement terms across studies and provide clear explanations to avoid confusion.
• Names of the concepts/constructs do not intuitively match items used for their measurement.	• Define concepts and constructs clearly to match the items used for their measurement.
• Removing or adding items to measurements without providing a reason.	• Justify any changes to measurement items with clear reasoning and documentation.
• Cited sources cannot be retrieved, and items were not included.	• Include all items used in the Appendix of the study to maintain transparency and reproducibility.

relevant to compare security professionals' and general employees' motivation toward security tasks. However, professionals are much more limited in numbers as compared to general employees and hence harder to reach. For example, previous research on security professionals sometimes relied on computer science students as an alternative (e.g., [99]), involved high payment for professional work included in the studies (e.g., [100]), or had limited sample sizes (e.g., [36, 69]). Despite these challenges, insights from this comparison could guide the design of security measures that reduce the conflicts between primary and secondary tasks.

Our systematic review also allowed us to make methodological recommendations for future research. Most of our reviewed studies employed surveys and only five studies used design approaches (including one longitudinal intervention study [130]), three exploratory studies, and one replication study among 45 papers. We encourage future research to include more qualitative studies, intervention studies, longitudinal designs, and the development of tools (e.g., [129]) to support organizational security practices. Whereas subjective measurements from self-assessment questionnaires remain the most commonly used method [81], incorporating objective assessment methods could offer valuable insights. For instance, eye gaze data might provide an objective measure to complement others [8, 75, 102]. However, as eye gaze data are often challenging to interpret on their own, researchers commonly supplement eye-tracking data with methods such as Retrospective Think Aloud [56]. These methods often require manual and labor-intensive segmentation and labeling of the data, which can be especially daunting for large or complex datasets [153]. While automating such processes shows promise, they still lack in precision and contextual understanding [102, 149]. Scenario-based assessments [57] and the triangulation of data from multiple sources—such as management evaluations [148], self-reports, and system log data [130]—show promise in providing a more complete understanding of security behaviors. However, there are noteworthy challenges regarding both data collection and analysis of behavioral data in the field. Accessing organizational log data often requires researchers to collaborate closely with the organization's security officers [31, 159]. Additionally, the sensitivity of behavioral data demands rigorous processing protocols that comply with local data protection laws. Coordination among the legal team (e.g., for non-disclosure agreements), the data protection office, and the Ethical Review Panel at the research institute can take months.

Previous reviews [7, 88] have indicated that the Theory of Planned Behavior, Protection Motivation Theory, and Deterrence Theory are the ones that have been examined most extensively in security behavior research, primarily focusing on competence, threat appraisal, and deterrence (see section 2.1). However, our review on autonomous motivation highlights the increasing relevance of SDT. This shift in theoretical frameworks reflects how different theories are driven by specific perspectives, demonstrating the adage, "What you look for is what you find." When research is limited to exploring how threat appraisal leads to protection motivation, it inevitably reinforces those findings, leaving little room to explore the influence of psychological needs and other motivational

factors. Future research should further evaluate other frameworks, such as SDT and Expectancy-Value Theory, in the security context, to continue moving beyond deterrence. Additionally, there is the potential to integrate autonomous motivation with 20 other less-explored theories (Appendix A) in the security domain. The application of these theories could further capture the complexities of organizational security behaviors.

5.4 Limitations

Our review converges with recent security behavior studies within the HCI community, such as "self-efficacy and security behavior" [22], "cognition in social engineering empirical research" [26], and "emotions in cybersecurity" [150]. However, due to the scope of this review, we did not investigate the relationship between autonomous motivation and other influencing factors examined in [22, 26, 150]. Future studies can synthesize findings from these recent studies and this review and comprehensively examine these factors with specific security behaviors. While we proposed a refined taxonomy, the SDT framework's definition still captures the essence of autonomous motivation. Our taxonomy is not exhaustive, as it builds on previous taxonomies and the findings of reviewed papers. We encourage future research to validate our taxonomy and examine the interactions among motivators through empirical studies.

6 Conclusion

Scholars have suggested that autonomous motivators hold untapped potential in promoting security behaviors without relying on controlled motivation alone [92, 133]. Prior work has used a variety of theoretical frameworks from various disciplines to study autonomous motivators, leading to fragmented and heterogeneous literature. It is unclear how autonomous motivators connect with security behaviors.

To reconcile scattered findings, we systematically reviewed and analyzed 45 empirical studies examining autonomous motivation in organizational security contexts. We propose a refined taxonomy of autonomous motivation related to organizational security behaviors. We identify three types of security behaviors that have been examined in relation to autonomous motivation, synthesize findings and suggestions from the reviewed studies, and chart a path for conducting theory-informed studies on autonomous motivation in human-centered security.

7 Data Availability Statement

We have included the anonymized preregistration for peer review [32]. The data supporting the findings of this paper, including the preparation phase extraction, search query results, extraction manual, and the extraction table, are available as supplemental material.

Acknowledgments

Author 1 acknowledges the financial support of the Institute for Advanced Studies at the University of Luxembourg through a Young Academic Grant (2021). The Doctoral School in Humanities and Social Sciences at the University of Luxembourg supported the project with the Research Support Grants for 2024 and 2025. We thank Sophie Doublet and Muriel Frank for their support in discussing and visualizing autonomous motivation. We thank the ACs and reviewers for their constructive feedback.

References

[1] Anne Adams and Martina Angela Sasse. 1999. Users are not the enemy. *Commun. ACM* 42, 12 (1999), 40–46.
[2] Icek Ajzen. 1991. The theory of planned behavior. *Organizational behavior and human decision processes* 50, 2 (1991), 179–211.
[3] Icek Ajzen. 2020. The theory of planned behavior: Frequently asked questions. *Human behavior and emerging technologies* 2, 4 (2020), 314–324.
[4] Saad Alahmari, Karen Renaud, and Inah Omoronyia. 2023. Moving beyond cyber security awareness and training to engendering security knowledge sharing. *Information Systems and e-Business Management* 21, 1 (2023), 123–158.
[5] Yasser Alhelaly, Gurpreet Dhillon, and Tiago Oliveira. 2023. When expectation fails and motivation prevails: the mediating role of awareness in bridging the expectancy-capability gap in mobile identity protection. *Computers & Security* 134 (2023), 103470.
[6] Rao Faizan Ali, PDD Dominic, Syed Emad Azhar Ali, Mobashar Rehman, and Abid Sohail. 2021. Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. *Applied Sciences* 11, 8 (2021), 3383.
[7] Rawan A Alsharida, Bander Ali Saleh Al-rimy, Mostafa Al-Emran, and Anazida Zainal. 2023. A systematic review of multi perspectives on human cybersecurity behavior. *Technology in society* 73 (2023), 102258.
[8] Florian Alt, Mariam Hassib, and Verena Distler. 2023. Human-centered Behavioral and Physiological Security. In *New Security Paradigms Workshop*. ACM, Segovia Spain, 48–61. doi:10.1145/3633500.3633504
[9] Steven Alter. 2014. Theory of Workarounds. *Communications of the Association for Information Systems* 34, 1 (2014), 55. http://aisel.aisnet.org/cais/vol34/iss1/55
[10] Ahmed Alzahrani and Christopher Johnson. 2019. AHP-based Security decision making: How intention and intrinsic motivation affect policy compliance. *International Journal of Advanced Computer Science and Applications* 10, 6 (2019), 1–8.
[11] Ahmed Alzahrani, Chris Johnson, and Saad Altamimi. 2018. Information security policy compliance: Investigating the role of intrinsic motivation towards policy compliance in the organisation. In *2018 4th international conference on information management (ICIM)*. IEEE, New York, NY, USA, 125–132.
[12] Salim Awudu and Sotirios Terzis. 2023. Investigating Staff Information Security Policy Compliance in Electronic Identity Systems: The Ghanaian National Identity System. In *International Conference for International Association for Development of the Information Society (IADIS): Proceedings of International Conferences e-society and Mobile Learning*. ERIC, USA, 68–75.
[13] Albert Bandura and Dale H Schunk. 1981. Cultivating competence, self-efficacy, and intrinsic interest through proximal self-motivation. *Journal of personality and social psychology* 41, 3 (1981), 586.
[14] Adam Beautement, Ingolf Becker, Simon Parkin, Kat Krol, and M. Angela Sasse. 2016. Productive security: a scalable methodology for analysing employee security behaviours. In *Proceedings of the Twelfth USENIX Conference on Usable Privacy and Security* (Denver, CO, USA) *(SOUPS '16)*. USENIX Association, USA, 253–270.
[15] Adam Beautement, M. Angela Sasse, and Mike Wonham. 2008. The compliance budget: managing security behaviour in organisations. In *Proceedings of the 2008 New Security Paradigms Workshop* (Lake Tahoe, California, USA) *(NSPW '08)*. Association for Computing Machinery, New York, NY, USA, 47–58. doi:10.1145/1595676.1595684
[16] Ingolf Becker, Simon Parkin, and M Angela Sasse. 2017. Finding security champions in blends of organisational culture. In *Proceedings of the 2nd European Workshop on Usable Security*, Vol. 11. Internet Society, Paris, France, 124.
[17] Daniel Bennett and Elisa Mekler. January 2024. Beyond Intrinsic Motivation: The Role of Autonomous Motivation in User Experience. *ACM Transactions on Computer-Human Interaction* 1, 1 (January 2024), 1–44.
[18] Benjamin Maximilian Berens, Florian Schaub, Mattia Mossano, and Melanie Volkamer. 2024. Better Together: The Interplay Between a Phishing Awareness Video and a Link-centric Phishing Support Tool. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 826, 60 pages. doi:10.1145/3613904.3642843
[19] John F. Binning. 2016. Construct. https://www.britannica.com/science/construct. Encyclopedia Britannica.
[20] John M Blythe and Lynne Coventry. 2018. Costly but effective: Comparing the factors that influence employee anti-malware behaviours. *Computers in Human Behavior* 87 (2018), 87–97.
[21] John M Blythe, Lynne Coventry, and Linda Little. 2015. Unpacking security policy compliance: The motivators and barriers of employees' security behaviors. In *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*. Usenix,

Berkeley, CA, USA, 103–122.
[22] Nele Borgert, Luisa Jansen, Imke Böse, Jennifer Friedauer, M Angela Sasse, and Malte Elson. 2024. Self-Efficacy and Security Behavior: Results from a Systematic Review of Research Methods. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, Honolulu, USA, 1–32.
[23] Sharon S Brehm and Jack W Brehm. 2013. *Psychological reactance: A theory of freedom and control*. Academic Press, New York, USA.
[24] Burcu Bulgurcu, Hasan Cavusoglu, and Izak Benbasat. 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly* 34, 3 (2010), 523–548.
[25] Pavlo Burda, Luca Allodi, and Nicola Zannone. 2020. Don't forget the human: a crowdsourced approach to automate response and containment against spear phishing attacks. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, New York, NY, USA, 471–476.
[26] Pavlo Burda, Luca Allodi, and Nicola Zannone. 2024. Cognition in social engineering empirical research: a systematic literature review. *ACM Transactions on Computer-Human Interaction* 31, 2 (2024), 1–55.
[27] AJ Burns, Tom L Roberts, Clay Posey, Paul Benjamin Lowry, and Bryan Fuller. 2023. Going beyond deterrence: A middle-range theory of motives and controls for insider computer abuse. *Information Systems Research* 34, 1 (2023), 342–362.
[28] Hao Chen and Wenli Li. 2019. Understanding commitment and apathy in is security extra-role behavior from a person-organization fit perspective. *Behaviour & Information Technology* 38, 5 (2019), 454–468.
[29] Xiaowei Chen, Sophie Doublet, and Verena Distler. 2024. Making Motivation Theories Accessible: Introducing Motivation Cards to Map Motivators for Security and Privacy Education. In *S&PEI Workshop of the Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*.
[30] Xiaowei Chen, Sophie Doublet, Anastasia Sergeeva, Gabriele Lenzini, Vincent Koenig, and Verena Distler. 2024. What Motivates and Discourages Employees in Phishing Interventions: An Exploration of Expectancy-Value Theory. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*. Usenix, Berkely, CA, USA, 487–506.
[31] Xiaowei Chen, Margault Sacré, Gabriele Lenzini, Samuel Greiff, Verena Distler, and Anastasia Sergeeva. 2024. The Effects of Group Discussion and Role-playing Training on Self-efficacy, Support-seeking, and Reporting Phishing Emails: Evidence from a Mixed-design Experiment. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 829, 21 pages. doi:10.1145/3613904.3641943
[32] Xiaowei Chen, Verena Zimmermann, Lorin Schöni, and Verena Distler. 2024. Systematic literature review on autonomous motivation in organizational cybersecurity behaviors. https://osf.io/jxtk9.
[33] W Alec Cram, John D'arcy, and Jeffrey G Proudfoot. 2019. Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance. *MIS quarterly* 43, 2 (2019), 525–554.
[34] Russell Cropanzano and Marie S Mitchell. 2005. Social exchange theory: An interdisciplinary review. *Journal of management* 31, 6 (2005), 874–900.
[35] Robert E Crossler, Allen C Johnston, Paul Benjamin Lowry, Qing Hu, Merrill Warkentin, and Richard Baskerville. 2013. Future directions for behavioral information security research. *computers & security* 32 (2013), 90–101.
[36] Joseph Da Silva and Rikke Bjerg Jensen. 2022. " Cyber security is a dark art": The CISO as Soothsayer. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2 (2022), 1–31.
[37] John D'Arcy, Anat Hovav, and Dennis Galletta. 2009. User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information systems research* 20, 1 (2009), 79–98.
[38] Joshua Davis, Deepti Agrawal, and Xiang Guo. 2023. Enhancing users' security engagement through cultivating commitment: the role of psychological needs fulfilment. *European Journal of Information Systems* 32, 2 (2023), 195–206.
[39] Joshua M Davis, Deepti Agrawal, and Obi Ogbanufe. 2025. Shaping extra-role security behaviors through employee-agent relations: A dual-channel motivational perspective. *International Journal of Information Management* 80 (2025), 102833.
[40] Edward L Deci and Richard M Ryan. 2008. Facilitating optimal motivation and psychological well-being across life's domains. *Canadian psychology/Psychologie canadienne* 49, 1 (2008), 14.
[41] Edward L Deci and Richard M Ryan. 2008. Self-determination theory: A macrotheory of human motivation, development, and health. *Canadian psychology/Psychologie canadienne* 49, 3 (2008), 182.
[42] Edward L Deci and Richard M Ryan. 2014. The importance of universal psychological needs for understanding motivation in the workplace. *The Oxford handbook of work engagement, motivation, and self-determination theory* 13 (2014), 13–32.
[43] Gurpreet Dhillon, Yurita Yakimini Abdul Talib, and Winnie Ng Picoto. 2020. The mediating role of psychological empowerment in information security compliance intentions. *Journal of the Association for Information Systems* 21, 1 (2020), 5.
[44] Antonio Díaz Andrade, Monideepa Tarafdar, Robert M Davison, Andrew Hardin, Angsana A Techatassanasoontorn, Paul Benjamin Lowry, Sutirtha Chatterjee, and Gerhard Schwabe. 2023. The importance of theory at the Information Systems Journal. *Information Systems Journal* 33 (2023), 693–702.
[45] Verena Distler. 2023. The Influence of Context on Response to Spear-Phishing Attacks: an In-Situ Deception Study. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. ACM, Hamburg Germany, 1–18. doi:10.1145/3544548.3581170
[46] P Drogkaris and A Bourka. 2019. Cybersecurity culture guidelines: Behavioural aspects of cybersecurity. *European Union Agency for Network and Information Security (ENISA)* (2019).
[47] Jacquelynne S Eccles and Allan Wigfield. 1995. In the mind of the actor: The structure of adolescents' achievement task values and expectancy-related beliefs. *Personality and social psychology bulletin* 21, 3 (1995), 215–225.
[48] Jacquelynne S Eccles and Allan Wigfield. 2020. From expectancy-value theory to situated expectancy-value theory: A developmental, social cognitive, and sociocultural perspective on motivation. *Contemporary educational psychology* 61 (2020), 101859.
[49] Cori Faklaris, Laura A Dabbish, and Jason I Hong. 2019. A self-report measure of end-user security attitudes (SA-6). In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX, Santa Clara, USA, 61–77.
[50] Muriel Frank and Clara Ament. 2021. How motivation shapes the sharing of information security incident experience. In *Proceedings of the 54th Hawaii International Conference on System Sciences*. ScholarSpace, Hawaii, USA, 4528–4537.
[51] Muriel Frank and Vanessa Kohn. 2023. Understanding extra-role security behaviors: An integration of self-determination theory and construal level theory. *Computers & Security* 132 (2023), 103386.
[52] Anjuli Franz, Verena Zimmermann, Gregor Albrecht, Katrin Hartwig, Christian Reuter, Alexander Benlian, and Joachim Vogt. 2021. SoK: still plenty of phish in the sea—a taxonomy of user-oriented phishing interventions and avenues for future research. In *Proceedings of the Seventeenth USENIX Conference on Usable Privacy and Security (SOUPS'21)*. USENIX Association, USA, Article 18, 19 pages.
[53] Trevor Gabriel and Steven Furnell. 2011. Selecting security champions. *Computer Fraud & Security* 2011, 8 (2011), 8–12.
[54] Yotamu Gangire, Adéle Da Veiga, and Marlien Herselman. 2021. Assessing information security behaviour: A self-determination theory perspective. *Information & Computer Security* 29, 4 (2021), 625–646.
[55] Cornelia Gerdenitsch, Daniela Wurhofer, and Manfred Tscheligi. 2023. Working conditions and cybersecurity: Time pressure, autonomy and threat appraisal shaping employees' security behavior. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 17, 4 (2023), 19.
[56] Zhiwei Guan, Shirley Lee, Elisabeth Cuddihy, and Judith Ramey. 2006. The validity of the stimulated retrospective think-aloud method as measured by eye tracking. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Montréal, Québec, Canada) *(CHI '06)*. Association for Computing Machinery, New York, NY, USA, 1253–1262. doi:10.1145/1124772.1124961
[57] Ken H Guo, Yufei Yuan, Norman P Archer, and Catherine E Connelly. 2011. Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of management information systems* 28, 2 (2011), 203–236.
[58] Marco Gutfleisch, Markus Schöps, Stefan Albert Horstmann, Daniel Wichmann, and M. Angela Sasse. 2023. Security Champions Without Support: Results from a Case Study with OWASP SAMM in a Large-Scale E-Commerce Enterprise. In *Proceedings of the 2023 European Symposium on Usable Security* (Copenhagen, Denmark) *(EuroUSEC '23)*. Association for Computing Machinery, New York, NY, USA, 260–276. doi:10.1145/3617072.3617115
[59] Steffi Haag, Mikko Siponen, and Fufan Liu. 2021. Protection motivation theory in information systems security research: A review of the past and a road map for the future. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems* 52, 2 (2021), 25–67.
[60] JR Hackman. 1976. Motivation through the design work: Test of the theory. *Organizational Behavior and Human Performance* 16 (1976), 250–279.
[61] Neal R Haddaway, Matthew J Page, Chris C Pritchard, and Luke A McGuinness. 2022. PRISMA2020: An R package and Shiny app for producing PRISMA 2020-compliant flow diagrams, with interactivity for optimised digital transparency and Open Synthesis. *Campbell systematic reviews* 18, 2 (2022), e1230.
[62] Felix Haeussinger and Johann Kranz. 2013. Information security awareness: Its antecedents and mediating effects on security compliant behavior. In *Thirty Fourth International Conference on Information Systems*. Citeseer, Milan, 1–16.
[63] Julie M Haney and Wayne G Lutters. 2019. Motivating cybersecurity advocates: Implications for recruitment and retention. In *Proceedings of the 2019 on Computers and People Research Conference*. Association for Computing Machinery, New York, NY, USA, 109–117.
[64] Tejaswini Herath and H Raghav Rao. 2009. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision support systems* 47, 2 (2009), 154–165.

[65] Cormac Herley. 2009. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 Workshop on New Security Paradigms Workshop* (Oxford, United Kingdom) *(NSPW '09)*. Association for Computing Machinery, New York, NY, USA, 133–144. doi:10.1145/1719030.1719050

[66] Jonas Hielscher, Annette Kluge, Uta Menges, and M Angela Sasse. 2021. "taking out the trash": Why security behavior change requires intentional forgetting. In *Proceedings of the 2021 New Security Paradigms Workshop*. Association for Computing Machinery, Virtual Event, USA, 108–122.

[67] Jonas Hielscher, Uta Menges, Simon Parkin, Annette Kluge, and M. Angela Sasse. 2023. "Employees who don't accept the time security takes are not aware enough": the CISO view of human-centred security. In *Proceedings of the 32nd USENIX Conference on Security Symposium* (Anaheim, CA, USA) *(SEC '23)*. USENIX Association, USA, Article 130, 18 pages.

[68] Jonas Hielscher and Simon Parkin. 2024. " What Keeps People Secure is That They Met The Security Team": Deconstructing Drivers And Goals of Organizational Security Awareness. In *33nd USENIX Security Symposium (USENIX Security 23)*. USENIX, Philadephia, USA, 3295–3312.

[69] Jonas Hielscher, Markus Schöps, Uta Menges, Marco Gutfleisch, Mirko Helbling, and M. Angela Sasse. 2023. Lacking the tools and support to fix friction: results from an interview study with security managers. In *Proceedings of the Nineteenth USENIX Conference on Usable Privacy and Security* (Anaheim, CA, USA) *(SOUPS '23)*. USENIX Association, USA, Article 8, 20 pages.

[70] Duncan Hodges and Oliver Buckley. 2017. Its not all about the money: Self-efficacy and motivation in defensive and offensive cyber security professionals. In *Human Aspects of Information Security, Privacy and Trust: 5th International Conference, HAS 2017, Held as Part of HCI International 2017, Vancouver, BC, Canada, July 9-14, 2017, Proceedings 5*. Springer, Berlin/Heidelberg, Germany, 494–506.

[71] Yuxiang Hong and Mengyi Xu. 2021. Autonomous motivation and information security policy compliance: role of job satisfaction, responsibility, and deterrence. *Journal of Organizational and End User Computing (JOEUC)* 33, 6 (2021), 1–17.

[72] Princely Ifinedo. 2014. Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management* 51, 1 (2014), 69–79.

[73] Sitwala Imenda. 2014. Is there a conceptual difference between theoretical and conceptual frameworks? *Journal of social sciences* 38, 2 (2014), 185–195.

[74] Philip G. Inglesant and M. Angela Sasse. 2010. The true cost of unusable password policies: password use in the wild. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Atlanta, Georgia, USA) *(CHI '10)*. Association for Computing Machinery, New York, NY, USA, 383–392. doi:10.1145/1753326.1753384

[75] Lennart Jaeger and Andreas Eckhardt. 2021. Eyes wide open: The role of situational information security awareness for security-related behaviour. *Information Systems Journal* 31, 3 (2021), 429–472.

[76] Soohyun Jeon and Anat Hovav. 2015. Empowerment or control: Reconsidering employee security policy compliance in terms of authorization. In *2015 48th Hawaii International Conference on System Sciences*. IEEE, New York, NY, USA, 3473–3482.

[77] Soohyun Jeon, Anat Hovav, Jinyoung Han, and Steven Alter. 2018. Rethinking the prevailing security paradigm: can user empowerment with traceability reduce the rate of security policy circumvention? *ACM SIGMIS Database: the DATABASE for Advances in Information Systems* 49, 3 (2018), 54–77.

[78] Soohyun Jeon, Insoo Son, and Jinyoung Han. 2020. Exploring the role of intrinsic motivation in ISSP compliance: enterprise digital rights management system case. *Information Technology & People* 34, 2 (2020), 599–616.

[79] Soohyun Jeon, Insoo Son, and Jinyoung Han. 2023. Understanding employee's emotional reactions to ISSP compliance: focus on frustration from security requirements. *Behaviour & Information Technology* 42, 13 (2023), 2093–2110.

[80] Heidi Julien, Jen JL Pecoskie, and Kathleen Reed. 2011. Trends in information behavior research, 1999–2008: A content analysis. *Library & Information Science Research* 33, 1 (2011), 19–24.

[81] Kristian Kannelønning and Sokratis K Katsikas. 2023. A systematic literature review of how cybersecurity-related behavior has been assessed. *Information & Computer Security* 31, 4 (2023), 463–477.

[82] Herbert C Kelman. 1958. Compliance, identification, and internalization three processes of attitude change. *Journal of conflict resolution* 2, 1 (1958), 51–60.

[83] Johann Kranz and Felix Haeussinger. 2014. Why deterrence is not enough: The role of endogenous motivations on employees' information security behavior. In *Thirty Fifth International Conference on Information Systems*. Association for Information Systems, Atlanta, GA, USA, 1–14.

[84] Kuang-Ming Kuo, Paul C Talley, and Chi-Hsien Huang. 2020. A meta-analysis of the deterrence theory in security-compliant and security-risk behaviors. *Computers & Security* 96 (2020), 101928.

[85] Dominika Kwasnicka, Stephan U Dombrowski, Martin White, and Falko Sniehotta. 2016. Theoretical explanations for maintenance of behaviour change: a systematic review of behaviour theories. *Health psychology review* 10, 3 (2016), 277–296.

[86] Richard S Lazarus. 1991. Cognition and motivation in emotion. *American psychologist* 46, 4 (1991), 352.

[87] Benedikt Lebek, Jörg Uffen, Michael H Breitner, Markus Neumann, and Bernd Hohler. 2013. Employees' information security awareness and behavior: A literature review. In *2013 46th Hawaii International Conference on System Sciences*. IEEE, Hawaii, USA, 2978–2987.

[88] Benedikt Lebek, Jörg Uffen, Markus Neumann, Bernd Hohler, and Michael H. Breitner. 2014. Information security awareness and behavior: a theory-based literature review. *Management Research Review* 37, 12 (2014), 1049–1092.

[89] Daeun Lee, Harjinder Singh Lallie, and Nadine Michaelides. 2023. The impact of an employee's psychological contract breach on compliance with information security policies: intrinsic and extrinsic motivation. *Cognition, Technology & Work* 25, 2 (2023), 273–289.

[90] Han Li, Rathindra Sarathy, Jie Zhang, and Xin Luo. 2014. Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance. *Information Systems Journal* 24, 6 (2014), 479–502.

[91] Rachid Ait Maalem Lahcen, Bruce Caulkins, Ram Mohapatra, and Manish Kumar. 2020. Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity* 3 (2020), 1–18.

[92] Philip Menard, Gregory J Bott, and Robert E Crossler. 2017. User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems* 34, 4 (2017), 1203–1230.

[93] Uta Menges, Jonas Hielscher, Laura Kocksch, Annette Kluge, and M. Angela Sasse. 2023. Caring Not Scaring - An Evaluation of a Workshop to Train Apprentices as Security Champions. In *Proceedings of the 2023 European Symposium on Usable Security* (Copenhagen, Denmark) *(EuroUSEC '23)*. Association for Computing Machinery, New York, NY, USA, 237–252. doi:10.1145/3617072.3617099

[94] John P Meyer, Natalie J Allen, and Catherine A Smith. 1993. Commitment to organizations and occupations: Extension and test of a three-component conceptualization. *Journal of applied psychology* 78, 4 (1993), 538.

[95] Marianne Miserandino. 1996. Children who do well in school: Individual differences in perceived competence and autonomy in above-average children. *Journal of educational psychology* 88, 2 (1996), 203.

[96] David Moher, Alessandro Liberati, Jennifer Tetzlaff, Douglas G Altman, Prisma Group, et al. 2010. Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *International journal of surgery* 8, 5 (2010), 336–341.

[97] Gregory D Moody, Mikko Siponen, and Seppo Pahnila. 2018. Toward a unified model of information security policy compliance. *MIS quarterly* 42, 1 (2018), 285–A22.

[98] Frederick P Morgeson and Stephen E Humphrey. 2006. The Work Design Questionnaire (WDQ): developing and validating a comprehensive measure for assessing job design and the nature of work. *Journal of applied psychology* 91, 6 (2006), 1321.

[99] Alena Naiakshina, Anastasia Danilova, Eva Gerlitz, and Matthew Smith. 2020. On Conducting Security Developer Studies with CS Students: Examining a Password-Storage Study with CS Students, Freelancers, and Company Developers. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. doi:10.1145/3313831.3376791

[100] Alena Naiakshina, Anastasia Danilova, Eva Gerlitz, Emanuel von Zezschwitz, and Matthew Smith. 2019. "If you want, I can store the encrypted password": A Password-Storage Field Study with Freelance Developers. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–12. doi:10.1145/3290605.3300370

[101] Jeanne Nakamura, Mihaly Csikszentmihalyi, et al. 2009. Flow theory and research. *Handbook of positive psychology* 195 (2009), 206.

[102] Jakub Štěpán Novák, Jan Masner, Petr Benda, Pavel Šimek, and Vojtěch Merunka. 2024. Eye Tracking, Usability, and User Experience: A Systematic Review. *International Journal of Human–Computer Interaction* 40, 17 (Sept. 2024), 4484–4500. doi:10.1080/10447318.2023.2221600

[103] Obi Ogbanufe and Ling Ge. 2023. A comparative evaluation of behavioral security motives: Protection, intrinsic, and identity motivations. *Computers & Security* 128 (2023), 103136.

[104] Obi Ogbanufe, Russell Torres, and Katia Guerra. 2023. BYOA and Security: Examining Perspective-Taking and Self-Determination. *Journal of Computer Information Systems* 2023 (2023), 1–17.

[105] Keshnee Padayachee. 2012. Taxonomy of compliant information security behavior. *Computers & Security* 31, 5 (2012), 673–680.

[106] Minjung Park and Sangmi Chai. 2018. Internalization of information security policy and information security practice: A comparison with compliance. In *51st Hawaii International Conference on System Sciences*. University of Hawai'i, Hawai'i, USA, 4723–4731.

[107] Douglas D Perkins and Marc A Zimmerman. 1995. Empowerment theory, research, and application. *American journal of community psychology* 23 (1995),

569–579.
[108] Clay Posey, Tom Roberts, Paul Benjamin Lowry, Becky Bennett, and James Courtney. 2010. Insiders' Protection of Organizational Information Assets: A Multidimensional Scaling Study of Protection-Motivated Behaviors. In *Roode Workshop on IS Security Research*. SSRN, Boston, MA, USA, 233–277.
[109] Clay Posey, Tom Roberts, Paul Benjamin Lowry, James Courtney, and Becky Bennett. 2011. Motivating the insider to protect organizational information assets: Evidence from protection motivation theory and rival explanations. In *The Dewald Roode workshop in information systems security*. SSRN, Kennesaw, GA, 1–51.
[110] Clay Posey, Tom L Roberts, and Paul Benjamin Lowry. 2015. The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems* 32, 4 (2015), 179–214.
[111] Clay Posey, Tom L Roberts, Paul Benjamin Lowry, Rebecca J Bennett, and James F Courtney. 2013. Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *Mis Quarterly* 37, 4 (2013), 1189–1210.
[112] Travis C Pratt, Francis T Cullen, Kristie R Blevins, Leah E Daigle, and Tamara D Madensen. 2006. The empirical status of deterrence theory: A meta-analysis. In *Taking stock: The status of criminological theory*. Transaction Publishers, New Jersey, USA, 367–395.
[113] Johnmarshall Reeve, Edward L Deci, and Richard M Ryan. 2004. Self-determination theory: a dialectical framework for understanding sociocultural influences on student. *Big theories revisited* 4 (2004), 31.
[114] Ronald W Rogers. 1975. A protection motivation theory of fear appeals and attitude change1. *The journal of psychology* 91, 1 (1975), 93–114.
[115] Benjamin D Rosenberg and Jason T Siegel. 2018. A 50-year review of psychological reactance theory: Do not read this article. *Motivation Science* 4, 4 (2018), 281.
[116] Richard M Ryan and Edward L Deci. 2000. Intrinsic and extrinsic motivations: Classic definitions and new directions. *Contemporary educational psychology* 25, 1 (2000), 54–67.
[117] Richard M Ryan and Edward L Deci. 2017. *Self-determination theory: Basic psychological needs in motivation, development, and wellness*. Guilford Press, New York, USA.
[118] Richard M Ryan and Edward L Deci. 2020. Intrinsic and extrinsic motivation from a self-determination theory perspective: Definitions, theory, practices, and future directions. *Contemporary educational psychology* 61 (2020), 101860.
[119] Richard M Ryan, Edward L Deci, et al. 2002. Overview of self-determination theory: An organismic dialectical perspective. *Handbook of self-determination research* 2, 3-33 (2002), 36.
[120] Nader Sohrabi Safa and Rossouw Von Solms. 2016. An information security knowledge sharing model in organizations. *Computers in Human Behavior* 57 (2016), 442–451.
[121] M. Angela Sasse, Jonas Hielscher, Jennifer Friedauer, and Annalina Buckmann. 2023. Rebooting IT Security Awareness – How Organisations Can Encourage and Sustain Secure Behaviours. In *Computer Security. ESORICS 2022 International Workshops: CyberICPS 2022, SECPRE 2022, SPOSE 2022, CPS4CIP 2022, CDT&SECOMANE 2022, EIS 2022, and SecAssure 2022, Copenhagen, Denmark, September 26–30, 2022, Revised Selected Papers* (Copenhagen, Denmark). Springer-Verlag, Berlin, Heidelberg, 248–265. doi:10.1007/978-3-031-25460-4_14
[122] Yukiko Sawaya, Mahmood Sharif, Nicolas Christin, Ayumu Kubota, Akihiro Nakarai, and Akira Yamada. 2017. Self-confidence trumps knowledge: A cross-cultural study of security behavior. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, Denver, USA, 2202–2214.
[123] Lorin Schöni, Victor Carles, Martin Strohmeier, Peter Mayer, and Verena Zimmermann. 2024. You Know What?-Evaluation of a Personalised Phishing Training Based on Users' Phishing Knowledge and Detection Skills. In *The 2024 European Symposium on Usable Security*. Association for Computing Machinery, Karlstad, Sweden, 1–14.
[124] Michiel Schotten, Wim JN Meester, Susanne Steiginga, Cameron A Ross, et al. 2017. A brief history of Scopus: The world's largest abstract and citation database of scientific literature. In *Research analytics*. Auerbach Publications, Boca Raton, FL, USA, 31–58.
[125] Dale H Schunk and Maria K DiBenedetto. 2020. Motivation and social cognitive theory. *Contemporary educational psychology* 60 (2020), 101832.
[126] Scott E Seibert, Gang Wang, and Stephen H Courtright. 2011. Antecedents and consequences of psychological and team empowerment in organizations: a meta-analytic review. *Journal of applied psychology* 96, 5 (2011), 981.
[127] Ahmad Bakhtiyari Shahri, Zuraini Ismail, and Shahram Mohanna. 2016. The impact of the security competency on "self-efficacy in information security" for effective health information security in Iran. *Journal of medical systems* 40 (2016), 1–9.
[128] Susan P Shapiro. 2005. Agency theory. *Annu. Rev. Sociol.* 31, 1 (2005), 263–284.
[129] Alireza Shojaifar, Samuel A Fricker, and Martin Gwerder. 2020. Automating the communication of cybersecurity knowledge: Multi-case study. In *Information Security Education. Information Security in Action. WISE 2020. IFIP Advances in Information and Communication Technology*. Springer, Cham, Switzerland, 110–124.
[130] Mario Silic and Paul Benjamin Lowry. 2020. Using design-science based gamification to improve organizational security training and compliance. *Journal of management information systems* 37, 1 (2020), 129–161.
[131] Gavin R Slemp, Mark A Lee, and Lara H Mossman. 2021. Interventions to support autonomy, competence, and relatedness needs in organizations: A systematic review with recommendations for research and practice. *Journal of Occupational and Organizational Psychology* 94, 2 (2021), 427–457.
[132] Teodor Sommestad, Henrik Karlzén, and Jonas Hallberg. 2019. The theory of planned behavior and information security policy compliance. *Journal of Computer Information Systems* 59:4 (2019), 344–353.
[133] Jai-Yeol Son. 2011. Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management* 48, 7 (2011), 296–302.
[134] Paul E Spector. 1982. Behavior in organizations as a function of employee's locus of control. *Psychological bulletin* 91, 3 (1982), 482.
[135] Gretchen M Spreitzer. 1995. Psychological empowerment in the workplace: Dimensions, measurement, and validation. *Academy of management Journal* 38, 5 (1995), 1442–1465.
[136] Jeffrey M Stanton, Kathryn R Stam, Paul Mastrangelo, and Jeffrey Jolton. 2005. Analysis of end user security behaviors. *Computers & security* 24, 2 (2005), 124–133.
[137] Dan N Stone, Edward L Deci, and Richard M Ryan. 2009. Beyond talk: Creating autonomous motivation through self-determination theory. *Journal of general management* 34, 3 (2009), 75–91.
[138] Noor Suhani Sulaiman, Muhammad Ashraf Fauzi, Walton Wider, Jegatheesan Rajadurai, Suhaidah Hussain, and Siti Aminah Harun. 2022. Cyber–information security compliance and violation behaviour in organisations: A systematic review. *Social Sciences* 11, 9 (2022), 386.
[139] Robert I Sutton and Barry M Staw. 1995. What theory is not. *Administrative science quarterly* 40:3 (1995), 371–384.
[140] Maja Tadić Vujčić, Wido GM Oerlemans, and Arnold B Bakker. 2017. How challenging was your work today? The role of autonomous work motivation. *European Journal of Work and Organizational Psychology* 26, 1 (2017), 81–93.
[141] Mohammad Tahaei, Alisa Frik, and Kami Vaniea. 2021. Privacy champions in software teams: Understanding their motivations, strategies, and challenges. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–15.
[142] Yurita Abdul Talib and Gurpreet Dhillon. 2015. Employee ISP compliance intentions: an empirical test of empowerment. In *Thirty Sixth International Conference of Information Systems,*. Association for Information Systems, Fort Worth, USA, 1–19.
[143] Gurvirender PS Tejay and Zareef A Mohammed. 2023. Cultivating security culture for information security success: A mixed-methods study based on anthropological perspective. *Information & Management* 60, 3 (2023), 103751.
[144] Kenneth W Thomas and Betty A Velthouse. 1990. Cognitive elements of empowerment: An "interpretive" model of intrinsic task motivation. *Academy of management review* 15, 4 (1990), 666–681.
[145] April Tyack and Elisa D. Mekler. 2020. Self-Determination Theory in HCI Games Research: Current Uses and Open Questions. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–22. doi:10.1145/3313831.3376723
[146] Daniel Udo-Akang. 2012. Theoretical constructs, concepts, and applications. *American International Journal of Contemporary Research* 2, 9 (2012), 89–97.
[147] O Van den Akker, GJY Peters, C Bakker, R Carlsson, NA Coles, KS Corker, G Feldman, DT Mellor, D Moreau, T Nordström, et al. 2020. Generalized systematic review registration form.
[148] Ali Vedadi, Merrill Warkentin, Detmar W Straub, and Jordan Shropshire. 2024. Fostering information security compliance as organizational citizenship behavior. *Information & Management* 61, 5 (2024), 103968.
[149] Antje C. Venjakob and Claudia R. Mello-Thoms. 2015. Review of prospects and challenges of eye tracking in volumetric imaging. *Journal of Medical Imaging* 3, 1 (Sept. 2015), 011002. doi:10.1117/1.JMI.3.1.011002 Publisher: SPIE.
[150] Alexandra von Preuschen, Monika C Schuhmacher, and Verena Zimmermann. 2024. Beyond fear and frustration-towards a holistic understanding of emotions in cybersecurity. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*. USENIX Association, Philadephia, USA, 623–642.
[151] Maximilian von Welck, Manuel Trenz, Tina Blegind Jensen, and Daniel Veit. 2017. Empowerment and BYOx: Towards Improved IS Security Compliance. In *38th International Conference on Information Systems: Transforming Society with Digital Innovation, ICIS 2017: Transforming Society with Digital Innovation*. Association for Information Systems, Atlanta, GA, USA, 1–11.
[152] Joan IJ Wagner, Greta Cummings, Donna L Smith, Joanne Olson, Lynn Anderson, and Sharon Warren. 2010. The relationship between structural empowerment and psychological empowerment for nurses: a systematic review. *Journal of*

nursing management 18, 4 (2010), 448–462.
[153] René Walendy, Markus Weber, Jingjie Li, Steffen Becker, Carina Wiesen, Malte Elson, Younghyun Kim, Kassem Fawaz, Nikol Rummel, and Christof Paar. 2024. I see an IC: A Mixed-Methods Approach to Study Human Problem-Solving Processes in Hardware Reverse Engineering. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 831, 20 pages. doi:10.1145/3613904.3642837
[154] Jeffrey D Wall, Prashant Palvia, and Paul Benjamin Lowry. 2013. Control-related motivations and information security policy compliance: The role of autonomy and efficacy. *Journal of Information Privacy and Security* 9, 4 (2013), 52–79.
[155] Zikai Alex Wen, Zhiqiu Lin, Rowena Chen, and Erik Andersen. 2019. What. hack: engaging anti-phishing training through a role-playing phishing simulation game. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, Glasgow, Scotland, Uk, 1–12.
[156] Alma Whitten and J. D. Tygar. 1999. Why Johnny can't encrypt: a usability evaluation of PGP 5.0. In *Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8* (Washington, D.C.) *(SSYM'99)*. USENIX Association, USA, 14.
[157] Allan Wigfield and Jacquelynne S Eccles. 2000. Expectancy–value theory of achievement motivation. *Contemporary educational psychology* 25, 1 (2000), 68–81.
[158] Robert Willison and Merrill Warkentin. 2013. Beyond deterrence: An expanded view of employee computer abuse. *MIS quarterly* 37, 1 (2013), 1–20.
[159] Michael Workman, William H. Bommer, and Detmar Straub. 2008. Security lapses and the omission of information security measures: A threat control model and empirical test. *Comput. Hum. Behav.* 24, 6 (Sept. 2008), 2799–2816. doi:10.1016/j.chb.2008.04.005
[160] Ning Yang, Tripti Singh, and Allen Johnston. 2020. A Replication Study of User Motivation in Protecting Information Security using Protection Motivation Theory and Self Determination Theory. *AIS Transactions on Replication Research* 6, 1 (2020), 10.
[161] Verena Zimmermann, Lorin Schöni, Thierry Schaltegger, Benjamin Ambuehl, Melanie Knieps, and Nico Ebert. 2024. Human-Centered Cybersecurity Revisited: From Enemies to Partners. *Commun. ACM* 67, 11 (Oct. 2024), 72–81. doi:10.1145/3665665
[162] Yixin Zou, Khue Le, Peter Mayer, Alessandro Acquisti, Adam J Aviv, and Florian Schaub. April, 2024. Encouraging Users to Change Breached Passwords Using the Protection Motivation Theory. *ACM Transactions on Computer-Human Interaction* 1, 1 (April, 2024), 1–45.
[163] Mary Ellen Zurko and Richard T. Simon. 1996. User-centered security. In *Proceedings of the 1996 Workshop on New Security Paradigms* (Lake Arrowhead, California, USA) *(NSPW '96)*. Association for Computing Machinery, New York, NY, USA, 27–33. doi:10.1145/304851.304859

A Glossary of Theoretical Frameworks applied in security behavior studies

Agency Theory: Agency Theory "is mainly concerned with the efforts provided by the individual members and of motivating them to obtain the desired effort input. An agency relationship exists whenever one party (principal) entrusts some decision-making authority to another party (agent)" [64, p.155]. Agency theory has been applied in the fields of economics, law, political science, and sociology [128].

Cognitive Model of Empowerment: "Individuals' judgments and behavior regarding tasks also are shaped by cognitions that go beyond verifiable reality. Such interpretive cognitions go beyond the perception of facts to provide additional, needed meaning for an individual" [144, p.669]. Psychological empowerment is formed based on individuals' assessments of a task regarding: impact, competence, meaningfulness, and choice [144]. The original model was published in an organizational science venue. Talib and Dhillon [142] referred to the model as the "intrinsic motivation model" in their work.

Deterrence Theory: "Individuals are less likely to commit a deviant activity when the risks of getting caught and the severity of the punishment increase" [133, p.297]. There are two central constructs in the theory: *Deterrent certainty* refers to the high likelihood of sanctions for violations of policies or rules, whereas *deterrent severity* refers to the harshness of the sanctions. The theory is rooted in the classical school of criminology [112].

Expectancy-Value Theory: "Individuals' choice, persistence, and performance can be explained by their beliefs about how well they will do in the activity and the extent to which they value the activity" [157, p.68]. Expectancy-Value Theory is a popular motivation theory in education contexts, but it has rarely been applied in information security studies [30].

Flow Theory: Flow Theory describes a state of deep immersion and engagement in an activity, where individuals experience intense focus, a sense of control, and intrinsic enjoyment [101, 130]. This state occurs when the challenge of the task is aligned with the individual's skills, leading to a balance between challenge and ability [101]. In flow, individuals lose awareness of time and external distractions, becoming fully absorbed in the task at hand [101].

Gaming "Theory": Gamification involves "applying game-like design artifacts and system processes to strengthen employees' motivations to encourage learning, efficacy, and increased employee compliance with organizational security initiatives" [130, p.131]. Silic and Lowry [130] conducted a design-science research project. Gaming theory and flow theory were used to guide the intervention design in the study.

Kanter's Model of Structural Empowerment: This model posits that power within organizations originates from two key systemic sources: formal and informal power [152]. Formal power is associated with roles that are highly visible, central to the organization's operations, and require autonomous decision-making [152]. By contrast, informal power is derived from relationships and alliances with superiors, peers, and subordinates [152]. These two forms of power facilitate access to job-related empowerment structures [152]: support (feedback and guidance), information (data, technical knowledge, and expertise), resources (time, materials, money, supplies, and equipment), and opportunity (autonomy, growth potential, sense of challenge, and learning opportunities).

Motive-Control Theory of Insider Computer Abuse: This theory "distinguishes between the influences of expressive and instrumental motives on insider computer abuse and explains how intrinsic (i.e., self-control) and extrinsic (i.e., organizational deterrence) controls moderate these relationships" [27, p.3]. Burns et al. [27] proposed this middle-range theory to focus on understanding the inherent tension between insider motivations and organizational controls.

Organizational Justice "Theory": There are four dimensions of employees' perceived fairness/unfairness in organizations or what is interchangeably termed justice/injustice: distributive justice, procedural justice, interpersonal justice, informational justice [158]. Li et al. [90] referred to this theoretical summary as "organizational justice theory." Can we cite a summary of previous findings, in this case the four dimensions of employees' perception of fairness/justice, as a theory? In which condition can we name a conceptual summary as a theory?

Organismic Integration Theory: When an individual internalizes external regulations (e.g., ISP), they will autonomously comply with these regulations [83]. Ryan and Deci examined "what motivates individuals to engage in behaviors and practices that are not necessarily intrinsically interesting" [117, p.179]. They propose that "supports for the basic needs for competence, relatedness, and autonomy facilitate the internalization and integration of non-intrinsically motivated behaviors" [117, p.203]. Organismic Integration Theory is a sub-theory of Self-Determination Theory [117].

Person Organization Fit Theory: An employee's behavior results from interactions between the individual and the organizational environment [28]. Person-Organization fit is achieved when (a) one provides what the other needs—either the individual's abilities meet the organization's demands (demand-ability fit) or the organization satisfies the individual's needs (need-supply fit); (b) they share similar values, attitudes, and goals; or (c) both [28].

Psychological Empowerment: Psychological empowerment was formed on the basis of an individual's assessment of a task in terms of competence, meaning, impact, and self-determination [135]. Empowerment reflects personal perceptions of a task and one's ability to control, shape, or influence that task [135, 144]. Individuals are intrinsically motivated when they experience these cognitions (competence, meaning, impact, and self-determination) in relation to a task [43].

Protection Motivation Theory: This theory was originally proposed by Rogers to understand individuals' health behaviors [114]. The theory posits that when an individual is confronted with a threat, they cognitively assess the threat and possible associated remedies [114]. On the basis of their assessment of the threat (threat susceptibility, threat severity, and rewards) and their coping appraisals (response efficacy, self-efficacy, and response cost), the individual decides to act in either an adaptive or maladaptive way [92, 114].

Rational Choice Theory: This theory "offers a theoretical explanation for how individuals make decisions when faced with choices. Rational Choice Theory argues that an individual determines how he will act by balancing the costs and benefits of his options" [24, p.527]. Whereas Awudu and Terzis [12] did not refer to a specific theory in their study design, Rational Choice Theory was emphasized in their source of measurement items.

Reactance Theory: Reactance Theory suggests that individuals desire freedom and that individuals will strive to restore freedoms that they perceive to be threatened by external control [23]. The attempt to restore freedom is referred to as psychological reactance, "a motivational state that drives freedom restoration" [115, p.1]. Reactance is conceptualized as being a stable personality trait as well as a behavioral response [154].

Self-Determination Theory: Self-Determination Theory proposes that "humans have evolved to be inherently curious, physically active and deeply social beings. Individual human development is characterized by proactive engagement, assimilating information and behavioral regulations, and finding integration within social groups" [117, p.4].

Social Bond Theory: Social Bond Theory posits that "when people build upon social bonds, their urge to indulge in anti-social or anti-establishment behaviors is reduced" [72, p.70]. There are four social bonds that promote socialization and conformity: attachment, commitment, involvement, and personal norms [72].

Social Cognitive Theory: Social Cognitive Theory posits that "individuals are actively engaged in their own development and obtain desired results when they believe that their actions are under their own control" [72, p.70]. Social cognitive theory "emphasizes the critical role played by the social environment on motivation, learning, and self-regulation" [125, p.1].

Social Exchange Theory: Social Exchange Theory posits that "individuals interact with one another when expecting beneficial outcomes, such as social rewards. Social rewards comprise reputation, status, respect, and social image" [50, p.4529]. Social exchanges lead to mutually beneficial transactions and relationships over time [34].

Social Influence theory: Kelman [82] distinguished three different processes of influence: compliance, identification, and internalization. "*Compliance* occurs when an individual accepts social influences in an attempt to receive a certain reward or avoid punishment. *Identification* happens when an individual perceives the importance of an issue and then shows a willingness to conform. *Internalization* takes place when an organization's value systems and norms coincide with those of the individual via the admission of social influences" [106, p.4724].

Theory of Planned Behavior: An individual's intentions to engage in certain behaviors are determined by *attitude*, *subjective norm*, and *perceived behavioral control* [3]. Attitude is an individual's positive or negative feelings toward engaging in a specified behavior, and the formation of attitude can be examined through an expectancy-value formulation [3]. Subjective norms describe an individual's perceptions of others' expectations. Perceived behavioral control, conceptually similar to self-efficacy, captures the extent to which an individual has the ability to perform the behavior and how much the behavior is under their control [3].

Theory of Primary Message Systems: This theory provides a taxonomy of behavioral patterns used to interpret and understand culture [143]. E.T. Hall identified 10 primary systems, each representing a distinct stream of cultural communication that interacts with others to produce the complex patterns of behavior [143]. These systems form the underlying structure through which cultural norms and values are conveyed, often nonverbally, within a society [143].

Theory of Workarounds: This theory describes the idea that established work practices may be adhered to or deviated from based on a variety of factors [9]. These include "the quality and practicality of the work practices, obstacles or anomalies that may be encountered by work system participants, and the monitoring and reward systems governing the work system" [77, p.58]. This theory emphasizes the dynamic nature of work processes, where employees often adapt or bypass formal procedures to achieve their goals under varying conditions [9].

Work Design Theory: Work Design Theory explores the relationships between the characteristics of work and the resulting employee outcomes, such as job satisfaction, motivation, and performance [60]. According to this theory, work can be structured in various ways to influence these outcomes, with a particular emphasis on task characteristics that shape the employee's experience [60]. Morgeson and Humphrey [98] expanded on traditional models by incorporating three key types of autonomy in task characteristics: work scheduling autonomy, decision-making autonomy, and work methods autonomy.

B Publication Venue of reviewed studies

Table 9: Publication venue of reviewed studies.

Type	Scope	Venue	Reviewed study
Journals	Information Systems	*Information & Management*	[72, 133, 143, 148]
		Journal of Management Information Systems	[92, 110, 130]
		MIS Quarterly	[24]
		Information Systems Research	[27]
		European Journal of Information Systems	[38]
		Journal of the Association for Information Systems	[43]
		Decision Support Systems	[64]
		Information Systems Journal	[90]
		Information Systems and e-Business Management	[4]
		ACM The Data Base for Advances in Information Systems	[77]
		AIS Transactions on Replication Research	[160]
	Interdisciplinary	*Computers in Human Behavior*	[20, 120]
		Behaviour & Information Technology	[28, 79]
		Information Technology & People	[78]
		Journal of Medical Systems	[127]
		Journal of Psychosocial Research on Cyberspace	[55]
		Journal of Organizational and End User Computing	[71]
		Journal of Computer Information Systems	[104]
		Cognition, Technology & Work	[89]
		International Journal of Advanced Computer Science and Applications	[10]
	Security-focused	*Computer & Security*	[5, 51, 103]
		Information & Computer Security	[54]
		Journal of Information Privacy and Security	[154]
Conferences	Information Systems	*Hawaii International Conference on System Sciences*	[50, 76, 106]
		AIS International Conference on Information Systems	[83, 142, 151]
		IEEE International Conference on Information Management	[11]
	Security and Privacy	*Symposium on Usable Privacy and Security (SOUPS)*	[21]
		Human Aspects of Information Security, Privacy, and Trust International Conference	[70]
		The Dewald Roode Workshop in Information Systems Security	[109]
	Human aspects of technology use	*International Conferences on e-Society and Mobile Learning*	[12]
		IFIP World Conference on Information Security Education	[129]
		ACM SIGMIS Computers and People Research	[63]