

# A Taxonomy of Positive Incentives to Motivate Cybersecurity Behaviors

Tobias Reittinger  
 University of Regensburg  
[tobias.reittinger@ur.de](mailto:tobias.reittinger@ur.de)

Günther Pernul  
 University of Regensburg  
[guenther.pernul@ur.de](mailto:guenther.pernul@ur.de)

## Abstract

*Cyberattacks pose a significant risk for organizations. As employees are often the primary target of cyberattacks, they are an organization's last line of defense. Incentives can be used to motivate employees to engage in cybersecurity. However, the lack of a consolidated framework for positive cybersecurity incentives, such as rewards, hinders decision-makers from identifying suitable incentives and adapting them to their organizational needs. This can lead to limited motivational effects, inefficient resource use, and inconsistent outcomes. To address this research gap, we developed a taxonomy of positive cybersecurity incentives from a systematic review of 46 papers and insights from 15 cybersecurity decision-makers. This taxonomy provides a comprehensive knowledge base and structured framework for categorizing and designing cybersecurity incentives, aiming to increase their effectiveness. The 15 cybersecurity decision-makers evaluated the taxonomy and showed very high inter-rater agreement, and we created an interactive version to enhance its applicability.*

**Keywords:** Cybersecurity, Incentives, Human Behavior, Taxonomy, Literature Review, Information Systems.

## 1. Introduction

As digitization advances and new technologies emerge, organizations face significant threats from cyberattacks. Despite increased investments in cybersecurity, attackers often remain one step ahead, as the effectiveness of cyberattacks has increased (Mair & Schwon-dra, 2023). The consequences are severe: In 2023, the financial impact of cyberattacks reached 8.15 billion US dollars, a figure projected to rise by nearly 70% to over 13 billion US dollars by 2028 (Statista, 2024).

Employees are often the primary targets of cyberattacks, mainly through stolen credentials or phishing (Verizon, 2024), highlighting their crucial role as the *last line of defense* in cybersecurity (Kirsch & Boss, 2007). While education and awareness are founda-

tional (Kävrestad et al., 2024), they may not necessarily lead to behavioral change. Thus, motivating employees to actively engage in cybersecurity practices is essential. Positive incentives, such as rewards, can help address this challenge by fostering motivation and encouraging desired behaviors (Ryan & Deci, 2017). In short, organizations can sustain employees' cybersecurity commitment by combining education, awareness, and incentives (Reittinger et al., 2024).

However, cybersecurity incentives require further research. Decision-makers lack a comprehensive knowledge base about positive cybersecurity incentives, which hinders their ability to identify and tailor suitable options to their specific needs, thereby limiting their impact on cybersecurity posture. Furthermore, the absence of a structured framework for designing cybersecurity incentives can lead to limited motivational effects, inefficient resource utilization, and inconsistent outcomes. In this paper, we facilitate this research gap by addressing the following research questions:

**RQ.** *How can positive incentives be categorized and designed to motivate cybersecurity behaviors?*

To tackle this research question, we developed a taxonomy of cybersecurity incentives using the methodology of Kundisch et al. (2021). We conducted a systematic literature review (SLR) of 46 papers from five databases and interviewed 15 cybersecurity decision-makers from diverse backgrounds. These decision-makers evaluated the taxonomy by categorizing incentives from 10 illustrative scenarios, allowing us to measure reliability through their level of agreement. We also gathered feedback on the taxonomy's completeness, comprehensibility, and applicability. Beyond the practical implications for decision-makers, these insights could advance the understanding of cybersecurity incentives in research, aiding their optimization and enhancing organizational cybersecurity posture. In summary, this paper offers the following contributions:

- We developed a taxonomy of cybersecurity incentives, including five dimensions, eight layers, and

32 characteristics. This taxonomy covers incentives inside organizations (e.g., for employees), outside organizations (e.g., for bug bounties), and between organizations (e.g., for threat intelligence sharing). It serves as a comprehensive knowledge base and a structured framework to help decision-makers design and categorize cybersecurity incentives, aiming to enhance their effectiveness.

- We evaluated the taxonomy with 15 cybersecurity decision-makers and found a very high inter-rater agreement (Fleiss, 1971; Landis & Koch, 1977). We developed an interactive open-source tool with illustrative examples to enhance comprehensibility and applicability.

In this paper, we focus on *positive incentives*, which we define as those incentives that reward behavior, as opposed to penalties and punishments. This term does not imply that the recipients perceive these incentives positively, e.g., winners may appreciate a competition reward, but losing participants may not.

The structure of this paper is as follows: Section 2 covers the background and related work. Section 3 outlines the study's methodology. Section 4 details the taxonomy development process, while Section 5 presents the taxonomy and its application. We evaluate the taxonomy in Section 6, discuss findings and future work in Section 7, and conclude in Section 8.

## 2. Background and Related Work

We outline the background and related work below.

### 2.1. Background

Incentives are based on the principles of human motivation. Self-Determination Theory (SDT) (Ryan & Deci, 2017), a well-known motivational theory, identifies two types of motivation: *Intrinsic motivation*, which comes from the inherent enjoyment of an activity, and *extrinsic motivation*, driven by external factors like rewards and punishments. While intrinsic motivation supports long-term engagement, extrinsic motivation can prompt immediate action (Deci & Ryan, 2014). Thus, combining both forms of motivation can lead to a more comprehensive motivational cybersecurity strategy.

Most organizations aim to enhance intrinsic motivation in cybersecurity through education and awareness campaigns (L. Li et al., 2019). However, extrinsic motivation is currently underutilized in the industry (Reitinger et al., 2024), leaving substantial potential untapped. Relying solely on intrinsic motivation may not ensure comprehensive cybersecurity engagement. To

boost extrinsic motivation, incentives can be strategically integrated into the approach (Goel et al., 2021).

One way organizations can integrate extrinsic motivators is security policies, which specify actions and behaviors employees must follow to ensure a secure work environment (Reeves et al., 2021). Compliance with these policies could be linked to tangible rewards, such as performance bonuses for employees who adhere to security protocols and report phishing emails. This connection between following policies and receiving rewards can enhance employees' motivation for cybersecurity efforts (Goel et al., 2020; Ryan & Deci, 2017).

### 2.2. Related Work

Research on incentives was initially developed outside the cybersecurity domain. Holmstrom and Milgrom (1994) provide a foundational framework by examining how organizations design incentives to align employee behavior with organizational goals. This framework is expanded by Gibbons and Roberts (2013), who explore the complexity and implications of incentive systems across various organizational contexts, synthesizing economic theories to explain how incentives influence behavior within firms. However, Boss et al. (2009) suggest that incentives in cybersecurity may differ from other domains, as employees often view rewards as incentives to exceed expectations—a strategy not typically feasible in cybersecurity (Luft, 1994). These insights highlight the need for a more nuanced investigation.

Recently, research has increasingly emphasized the importance of human factors in cybersecurity. Zimmermann and Renaud (2019) advocate for shifting the perspective from viewing humans as problems to recognizing them as essential solutions in cybersecurity. This view is echoed by Sharma and Warkentin (2019), who argue that the organizational context is critical for effective cybersecurity, and by Warkentin and Willison (2009), who highlight the need for a deeper understanding of human factors in information security. In summary, while incentives are crucial in cybersecurity, they must be analyzed separately from other domains to address the unique challenges inherent in cybersecurity.

Thus, incentives in cybersecurity have been increasingly explored. Goel et al. (2020) examine the effectiveness of financial incentives in improving security policy compliance, finding mixed results depending on the context and implementation. Vance et al. (2012) apply protection motivation theory to understand the motivations behind security compliance, which is fundamental to developing effective incentives. Additionally, specific incentives, such as gamification, have been studied, with Friedl et al. (2024a, 2024b) suggesting it could be an ef-

fective tool for increasing cybersecurity knowledge.

To summarize findings on cybersecurity incentives, several taxonomies have been developed. Alkalabi et al. (2021) conduct an SLR to create an overview of incentives for threat information sharing within a specific geographical region. Similarly, Gelhaar et al. (2021) develop a taxonomy of incentive mechanisms for data sharing, offering a detailed classification of the components of incentive mechanisms and their application in data ecosystems. Additionally, Wessels et al. (2021) create a typology for cybersecurity investments, exploring how incentives influence stakeholders' decisions. However, no existing paper has developed a holistic taxonomy of positive cybersecurity incentives applicable to motivate cybersecurity behavior. This paper aims to address this research gap.

### 3. Methodology

We explain the research methodology in this section.

#### 3.1. Taxonomy Development

We methodically developed the taxonomy using the extended taxonomy design process (ETDP) by Kundisch et al. (2021). The ETDP consists of 18 steps and enhances the well-known methodology of Nickerson et al. (2013) by incorporating evaluation guidelines. We conducted a *systematic literature review (SLR)* of 46 papers from five databases and 15 *semi-structured interviews*<sup>1</sup> with cybersecurity decision-makers, allowing us to integrate multiple sources and leverage industry experience (Kundisch et al., 2021). For the SLR, we followed the guidelines of Okoli and Schabram (2015), and for the expert interviews, we used the cognitive interviewing methodology by Willis (2004).

#### 3.2. Evaluation

We evaluated the taxonomy through another round of semi-structured interviews<sup>1</sup> with the same 15 cybersecurity decision-makers, using cognitive interviewing methodology (Willis, 2004). First, we inquired about the taxonomy's *completeness* and *comprehensibility*. To assess its *reliability*, the cybersecurity decision-makers categorized incentives from 10 illustrative scenarios (five each from the literature and the industry) using the taxonomy. We calculated the inter-rater agreement using Fleiss' Kappa (Fleiss, 1971). After the taxonomy's use, we collected feedback on its *applicability*.

<sup>1</sup>Questionnaires and codebooks for the taxonomy development and evaluation: <https://github.com/IncentiveTaxonomy/Availability>

**Table 1. Participating cybersecurity decision-makers**

ID	Position	Sector	Employees	Exp.	Country
E1	CISO	Technology	100-999	5	Germany
E2	Security manager	Consulting	100-999	3	US
E3	Security engineer	Manufacturing	1,000-9,999	3	Germany
E4	CEO	Law firm	100-999	7	Germany
E5	Project manager	Pharmaceuticals	+10,000	13	Switzerland
E6	Security consultant	IT services	1-9	10	Germany
E7	CEO	Healthcare	10-99	22	Austria
E8	Security consultant	Retail	1-9	1	Germany
E9	ISO	Energy	1,000-9,999	2	Switzerland
E10	CISO	Finance	100-999	8	Austria
E11	Cyber risk manager	IT services	100-999	1	US
E12	CEO	Retail	10-99	35	Germany
E13	Security advisor	Finance	100-999	17	Germany
E14	Security manager	Government	+10,000	7	Germany
E15	CEO	Manufacturing	10-99	12	Germany

### 3.3. Participants

The study targeted cybersecurity decision-makers to ensure the relevance of insights for designing and implementing cybersecurity incentive programs. Participants were recruited through purposive sampling using the authors' professional networks and were incentivized with a free cybersecurity incentive workshop based on the research results. We recruited 15 participants with extensive experience across various positions, sectors, organization sizes, and countries, as described in Table 1. These 15 cybersecurity decision-makers participated in both the taxonomy development and its evaluation.

### 3.4. Coding and Analysis

The semi-structured interviews were transcribed using Whisper Transcription. Following the flexible coding approach (Deterding & Waters, 2021), one researcher conducted the initial coding, and a second researcher co-interpreted the codes. Any coding conflicts were resolved through multiple rounds of discussion, resulting in the final codebooks.<sup>1</sup>

## 4. Taxonomy Development Process

In the present section, we develop the taxonomy following the 18 ETDP steps by Kundisch et al. (2021).

### 4.1. Objective Definition

In Section 1, we emphasized the need for a taxonomy of cybersecurity incentives. Building on this, we established the meta-characteristic: *Characteristics of positive incentives to motivate cybersecurity behaviors*, forming our taxonomy's foundation. Following the guidelines of Nickerson et al. (2013), the objective ending conditions were: *i)* examining all objects, *ii)* identifying at least one object for each characteristic in every dimension, *iii)* ensuring no merging or split-

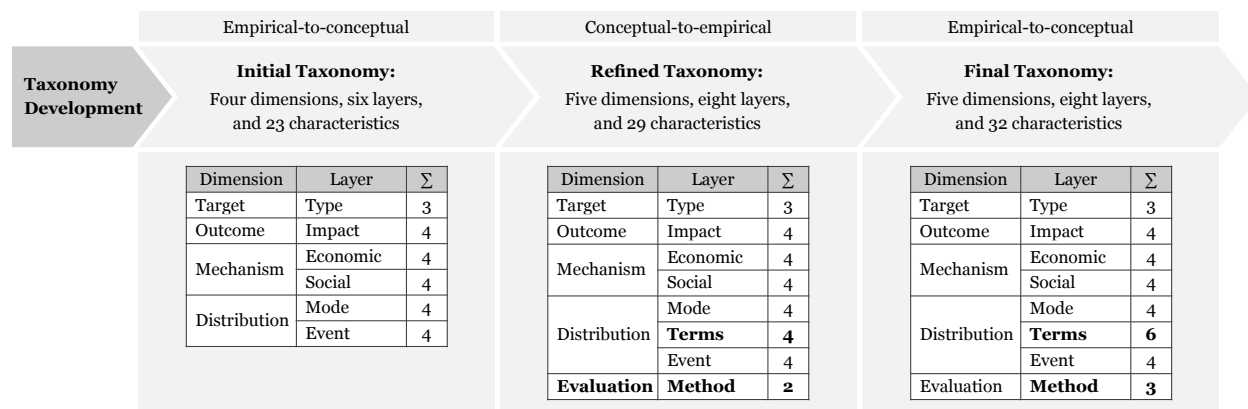


Figure 1. Taxonomy development with corresponding number of characteristics

ting of dimensions in the final iteration, and *iv*) preserving the uniqueness of each dimension and characteristic. To complement these objective criteria, we also defined subjective ending conditions, aiming for the taxonomy to be *i*) concise, *ii*) robust, *iii*) comprehensive, *iv*) extendable, and *v*) explanatory.

Furthermore, we established four evaluation goals to ensure the taxonomy meets its defined objectives. We selected *completeness* and *comprehensibility* to confirm that cybersecurity decision-makers easily understand the taxonomy, and it covers all aspects of positive cybersecurity incentives. Additionally, we chose *reliability* to verify that the taxonomy consistently yields accurate results and *applicability* to ensure it can be practically applied in diverse organizational contexts.

## 4.2. Development and Demonstration

In the taxonomy development, we started with the *empirical-to-conceptual* approach, as significant data on cybersecurity incentives is available from publications (Nickerson et al., 2013). The taxonomy development is visualized in Figure 1, whereas changes to the previous step are highlighted in bold font.

**(1) Initial Taxonomy.** The first iteration of the taxonomy uses an *empirical-to-conceptual* approach, conducting a systematic literature review (SLR) based on the guidelines by Okoli and Schabram (2015), aiming to identify characteristics of positive incentives in cybersecurity. The SLR, covering the period from 01/01/2014 to 04/30/2024, spanned five reputable databases: AIS eLibrary, IEEE Xplore, ACM Digital Library, ScienceDirect, and SpringerLink<sup>2</sup>. We searched the title for the following keyword combinations: *Incentive + Cybersecurity*, *Incentive + Security*, *Reward + Cybersecurity*, and *Reward + Security*. Inclusion criteria required the

<sup>2</sup><http://aisel.aisnet.org>, <http://ieeexplore.ieee.org>, <http://dl.acm.org>, <https://www.sciencedirect.com>, <https://link.springer.com>

literature to be in English, within the cybersecurity domain, and covering incentive characteristics. Initially, 73 publications were found, but after removing duplicates and applying the inclusion criteria, 46 papers remained. The significant reduction was primarily due to the keyword combination *Incentive + Security*, which identified literature outside of cybersecurity. We then extracted 23 characteristics of positive cybersecurity incentives, classifying them through the ETDP into four dimensions with six layers. The initial classification is based on the foundational work of Gibbons and Roberts (2013), Holmstrom and Milgrom (1994), and Ryan and Deci (2017). For full transparency, the selection and classification process is available online.<sup>1</sup>

**(2) Refined Taxonomy.** The second iteration follows a *conceptual-to-empirical* approach, involving 15 expert interviews with cybersecurity decision-makers to explore the characteristics of positive cybersecurity incentives in practice. These interviews provided practical insights that were not initially evident from the SLR and were critical for understanding positive incentives. This process led to the identification of one new dimension and two new layers. The new layer, *Terms*, was added to the existing dimension *Distribution*, reflecting the various ways incentives are structured and communicated within organizations. Decision-makers emphasized the need to differentiate between incentives given in advance (prepaid) versus those awarded after achieving specific outcomes (postpaid) and whether the terms are disclosed to participants or kept undisclosed. According to the decision-makers, these terms significantly influence the effectiveness of incentives. Additionally, the new dimension *Evaluation* with the layer *Method* emerged from the interviews, underscoring the importance of evaluating incentives through direct engagement with employees or stakeholders. Decision-makers noted that user studies and interviews provide valuable

insights into how incentives are perceived and their real-world impact, revealing that evaluation is essential for designing effective cybersecurity incentives tailored to specific organizational contexts.

**(3) Final Taxonomy.** The third and final iteration uses an *empirical-to-conceptual* approach. After refining the taxonomy based on expert interviews, we reexamined the 46 papers from the SLR to assess the newly added layers. This revealed two new characteristics for the *Terms* layer and one for the *Method* layer. Table 2 shows the finalized classification of the 46 papers.

Finally, we demonstrated the final taxonomy in accordance with Nickerson et al. (2013). Two authors independently verified that the objective ending conditions were met by reviewing the taxonomy development process and performing an iterative analysis of the taxonomy. The subjective ending conditions were confirmed by evaluating all incentives identified in the SLR and the 10 illustrative scenarios used in the evaluation process.

## 5. Taxonomy of Cybersecurity Incentives

We present the taxonomy of positive cybersecurity incentives as a morphological box in Table 3. It comprises five dimensions, eight layers, and 32 characteristics, which is an appropriate size for a taxonomy (Nickerson et al., 2013). The taxonomy includes incentives within organizations (e.g., for employees), external to organizations (e.g., for bug bounties), and between organizations (e.g., for threat intelligence sharing). Integrating these three perspectives facilitates the application and transfer of insights about incentives across different areas of cybersecurity. The dimensions are ordered according to the design science research methodology by Peffers et al. (2007). The last column indicates whether the characteristics are mutually exclusive (E) or not (N), determining how many can be selected. The taxonomy is applied by selecting at least one characteristic from each dimension, moving from top to bottom. Still, some contexts might require more flexibility, in which cases not all dimensions need to be mandatory Kundisch et al. (2021).

The first dimension, *Target*, distinguishes whether the incentive targets individual employees, the organization as a whole, or specific technological aspects (e.g., distributed security systems). The second dimension, *Outcome*, categorizes the desired results of the incentives, distinguishing between the impact on behavior or technical systems and the temporal aspect of short-term and long-term effects. The third dimension, *Mechanism*, outlines the means through which incentives operate. Economic mechanisms have a financial effect that typically has an objective value, including money, regulation

**Table 2. SLR classification in the final taxonomy**

Author	Incentive Design				
	Target	Outcome	Mechanism	Distribution	Evaluation
August et al. (2014)	•	•	•	•	
Giannetsos et al. (2014)	•	•	•		
M. Li et al. (2014)	•	•	•	•	•
Liao and Chen (2014)	•	•	•		•
Shoshitaishvili et al. (2014)	•		•	•	•
Nepal and Jamasb (2015)	•		•	•	
Gisdakis et al. (2016)	•	•	•	•	•
Naghizadeh and Liu (2016a)	•		•	•	
Naghizadeh and Liu (2016b)	•	•	•	•	
Chatfield and Reddick (2017)	•	•	•	•	•
Farhadi et al. (2017)	•		•	•	
Gonzalez and Treck (2017)	•	•	•	•	•
Korczynski et al. (2017)	•		•	•	•
Abe et al. (2018)	•	•	•	•	•
Xu et al. (2018)	•	•	•	•	•
Zhan et al. (2018)	•		•	•	•
Zhao et al. (2018)	•	•	•	•	
Berenjian et al. (2019)	•	•	•		•
Kenneally (2019a)	•	•	•		
Kenneally (2019b)	•	•	•		
Yang et al. (2019)	•		•	•	•
Zhu et al. (2019)	•	•	•	•	•
Goel et al. (2020)	•	•	•	•	•
Morgner et al. (2020)	•	•	•	•	•
Alkalabi et al. (2021)	•	•	•	•	•
Goel et al. (2021)	•	•	•	•	•
Kroll et al. (2021)	•	•	•		
Vlachos et al. (2021)	•	•	•		•
Wessels et al. (2021)	•	•	•		•
Arulprakash and Jebakumar (2022)	•	•	•	•	•
Kolini and Janczewski (2022)	•		•	•	•
H. Li et al. (2022)	•	•			•
Q. Li et al. (2022)	•		•	•	•
Lu et al. (2022)				•	•
McConnell et al. (2022)	•			•	
Wang et al. (2022)	•			•	
Wang (2022)	•				•
Ali et al. (2023)	•	•	•	•	
Bates et al. (2023)	•	•	•	•	•
Cai et al. (2023)	•	•	•	•	•
He et al. (2023)	•	•	•	•	•
Kalpana et al. (2023)	•	•	•	•	•
Y. Li and Hoffman (2023)	•	•	•	•	•
Rathore and Griffith (2023)	•	•		•	•
Yoshioka et al. (2023)	•	•		•	•
Sohail et al. (2024)	•	•	•	•	•
Σ	45	33	35	35	33

(e.g., for security patching like Morgner et al. (2020)), data (e.g., for threat intelligence sharing as Kolini and Janczewski (2022)), and subsidies. Social mechanisms have a social effect that usually has a subjective value, encompassing reputation, gamification, feedback, and certification. The most used mechanisms are money and reputation, which typically have a strong immediate effect. The fourth dimension, *Distribution*, focuses on how incentives are distributed. It covers three layers. First, the mode of distribution describes the form in

**Table 3. Taxonomy of positive cybersecurity incentives**

Dimension	Layer	Characteristics						N / E	
Target	Type	Individual		Organization		Technology		E	
Outcome	Impact	Behavior		Technical	Short-term		Long-term	N	
Mechanism	Economic	Money		Regulation	Data		Subsidy	E	
	Social	Reputation		Gamification	Feedback		Certification	E	
Distribution	Mode	Physical		Digital		Manual		Automatic	N
	Terms	Prepaid	Postpaid	Disclosed	Undiscl.	Fixed	Dynamic	N	
	Event	Competition		Evaluation		Surveillance		Deadline & Goal	E
Evaluation	Method	User study		Interviews		Simulation		E	

which the mechanism is delivered to the target. A digital mode occurs more often than a physical distribution, and an automatic distribution is more common than a manual one. Second, the terms further detail whether incentives are prepaid, postpaid, disclosed, undisclosed, fixed, or dynamic. Third, decision-makers can employ events such as competitions (primarily used in bug bounties), evaluations, surveillance, or deadlines as the distribution of an incentive. The most applied events by cybersecurity decision-makers are competitions, while the literature analyzes punishment in-depth. The final dimension, *Evaluation*, describes the methods used to evaluate the effectiveness of cybersecurity incentives, highlighting the importance of empirical and practical assessment techniques. The layers here include user studies, interviews, and simulations, with the latter primarily used in combination with technology as the target. This taxonomy offers a structured framework and a comprehensive knowledge base for decision-makers, enabling them to design and implement cybersecurity incentive programs tailored to their organizational needs. It aims to improve motivational effects, optimize resource utilization, and ensure consistent outcomes in cybersecurity practices.

Beyond the incentive design classified in the taxonomy, we examined the use of incentives across sectors, technologies, and stages of the cybersecurity lifecycle in the literature. Incentives are commonly applied in sectors such as security management, human aspects, and education (European Commission, Joint Research Center et al., 2019). They are also increasingly integrated into emerging technologies like cyber threat intelligence and artificial intelligence. When examining the use of incentives across the lifecycle based on the NIST Cybersecurity Framework (Barrett, 2018), we found that the *protect phase* prominently employs incentives, particularly in combination with human aspects and education.

## 6. Evaluation

Next, we evaluated the taxonomy through 15 expert interviews following the ETDP by Kundisch et al. (2021). The cybersecurity decision-makers agreed that the taxonomy encompasses all components of cybersecurity incentives, indicating its *completeness*. Most found the taxonomy comprehensible, though three expressed uncertainty about the target of technology and the technical outcome. To enhance the taxonomy’s *comprehensibility*, we provide illustrative examples online that describe all characteristics.<sup>3</sup> One expert shared the perception of the taxonomy:

*“I am surprised that incentives in cybersecurity can be designed in such a variety of ways. [...] We could customize them more precisely to our use case.” (E12)*

To assess the taxonomy’s *reliability*, the cybersecurity decision-makers categorized incentives from 10 illustrative scenarios (five from literature and five from industry), which we published online,<sup>3</sup> using the taxonomy. The scenarios included incentives within organizations (e.g., rewards for employees reporting phishing emails), outside organizations (e.g., bug bounties), and between organizations (e.g., financial payments or a marketing label for threat intelligence sharing). We calculated each dimension’s inter-rater agreement using Fleiss’ Kappa (Fleiss, 1971). The results are displayed in Table 4 and indicate a very high inter-rater agreement, with Fleiss’ Kappa exceeding 0.8 for each dimension of the taxonomy (Landis & Koch, 1977). These findings indicate a strong reliability of the taxonomy of positive cybersecurity incentives.

<sup>3</sup>Illustrative scenarios and open-source interactive taxonomy with examples: <https://github.com/IncentiveTaxonomy/Availability>

**Table 4. Inter-rater agreement with Fleiss' Kappa**

Dimensions	Inter-rater agreement (Fleiss, 1971)	Interpretation (Landis & Koch, 1977)
Target	$\kappa = 0.89$	Very high
Outcome	$\kappa = 0.85$	Very high
Mechanism	$\kappa = 0.82$	Very high
Distribution	$\kappa = 0.81$	Very high
Evaluation	$\kappa = 0.92$	Very high

After the cybersecurity decision-makers applied the taxonomy, we inquired about its *applicability*. Most agreed that the taxonomy was highly applicable and successfully classified the 10 scenarios. Two participants, unfamiliar with morphological boxes, experienced minor difficulties with its application, as explained:

*“I haven’t used a taxonomy in the past, so I’m not sure where to start.” (E11)*

To further improve applicability, we developed an *interactive taxonomy*,<sup>4</sup> addressing these drawbacks. The interactive tool enhances the utility of the developed framework by making it more adaptable, accessible, and user-friendly. It also allows the customization of incentive characteristics to fit organizational contexts and enables cybersecurity decision-makers to explore and engage with the taxonomy interactively. By offering illustrative examples and guiding users through its application, the interactive version can facilitate the understanding and implementation of cybersecurity incentives.

Additionally, one participant was uncertain about classifying an incentive that offers multiple mechanisms (e.g., bug bounties can result in money and reputation). Hence, we added a note to the interactive taxonomy, recommending selecting the primary incentive mechanism (e.g., money for bug bounties). A participant summarized their experience with the taxonomy:

*“With the taxonomy, we can design cybersecurity incentives based on a guideline, as we lacked knowledge in that area.” (E15)*

## 7. Limitations and Future Work

We outline limitations and potential for future work. Since we used purposive sampling, participants might not have been selected randomly. Still, we included diverse participants to enrich the study’s insights. Most participants were from Europe, which may limit the generalizability of our findings. Future research could address this by replicating the study in other regions to validate the results in different contexts. Additionally,

<sup>4</sup>Interactive taxonomy: <https://taxonomy.uversy.com>

the same participants were involved in the taxonomy development and its evaluation, which could introduce bias. Recruiting cybersecurity decision-makers is challenging due to their limited availability, but we successfully gathered input from a diverse group.

While most dimensions of the taxonomy are mutually exclusive and collectively exhaustive (MECE), the *Outcome* and *Distribution* dimensions are not. Kundisch et al. (2021) suggest aiming for a MECE taxonomy but allowing justified deviations. During expert interviews in the second iteration of taxonomy development, the cybersecurity decision-makers noted that in practical scenarios, multiple selections within the *Outcome* and *Distribution* dimensions would be necessary, making strict mutual exclusiveness difficult to maintain. They emphasized that this approach better reflects the complexity of cybersecurity incentives, justifying the decision to retain the non-exclusiveness of these dimensions for a more accurate and practical representation.

Our proposed taxonomy offers a comprehensive knowledge base and a structured framework for positive cybersecurity incentives. Future research could explore which combinations of the 32 identified characteristics are most effective in different cybersecurity contexts and investigate the longevity to sustain motivation. Another potential extension of the taxonomy could involve integrating nudges, as emerging research in this area has shown promising results (Baumer et al., 2024).

## 8. Conclusion

This paper investigates the categorization and design of cybersecurity incentives, offering the *following contributions*: (1) We developed a comprehensive taxonomy of positive cybersecurity incentives based on an SLR of 46 papers and 15 interviews with cybersecurity decision-makers. (2) The evaluation by these decision-makers shows high inter-rater agreement, indicating the taxonomy’s completeness and reliability. (3) We created an interactive version of the taxonomy to further improve its applicability and usability. Overall, this paper provides a knowledge base and structured framework to guide cybersecurity decision-makers in designing incentive programs tailored to their organizational needs.

## Use of Generative AI

We refined the language and readability of this paper with DeepL, Grammarly, and ChatGPT (Version 4o) and take full responsibility for the content.<sup>5</sup>

<sup>5</sup>For full transparency, we report AI Usage Cards (Wahle et al., 2023): <https://ai.uversy.com/incentive-taxonomy>

## References

- Abe, R., Nakamura, K., Teramoto, K., & Takahashi, M. (2018). Attack incentive and security of exchanging tokens on proof-of-work blockchain. *Proceedings of the 14th Asian Internet Engineering Conference*, 32–37.
- Ali, A., Ilahi, I., Qayyum, A., Mohammed, I., Al-Fuqaha, A., & Qadir, J. (2023). A systematic review of federated learning incentive mechanisms and associated security challenges. *Computer Science Review*, 50, 100593.
- Alkalabi, W., Simpson, L., & Morarji, H. (2021). Barriers and incentives to cybersecurity threat information sharing in developing countries: A case study of Saudi Arabia. *Proceedings of the 2021 Australasian Computer Science Week Multi-conference*.
- August, T., August, R., & Shin, H. (2014). Designing user incentives for cybersecurity. *Commun. ACM*, 57(11), 43–46.
- Barrett, M. (2018, April). Framework for improving critical infrastructure cybersecurity version 1.1.
- Bates, E., Mavroudis, V., & Hicks, C. (2023). Reward shaping for happier autonomous cyber security agents. *Proceedings of the 16th ACM Workshop on Artificial Intelligence and Security*.
- Baumer, T., Reitinger, T., Kern, S., & Pernul, G. (2024). Digital nudges for access reviews: Guiding deciders to revoke excessive authorizations. *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*, 239–258. <https://www.usenix.org/conference/soups2024/presentation/baumer>
- Berenjian, S., Hajizadeh, S., & Atani, R. E. (2019). An incentive security model to provide fairness for peer-to-peer networks. *2019 IEEE Conference on Application, Information and Network Security (AINS)*, 71–76.
- Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, i'll do what i'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems*, 18, 151–164.
- Cai, X., Zhou, L., Li, F., Fu, Y., Zhao, P., Li, C., & Yu, F. R. (2023). An incentive mechanism for vehicular crowdsensing with security protection and data quality assurance. *IEEE Transactions on Vehicular Technology*, 72, 9984–9998.
- Deci, E. L., & Ryan, R. M. (2014). *Intrinsic motivation and self-determination in human behavior*. Springer Science+Business Media.
- Deterding, N. M., & Waters, M. C. (2021). Flexible coding of in-depth interviews: A twenty-first-century approach. *Sociological methods & research*, 50(2), 708–739.
- European Commission, Joint Research Center, Nai Fovino, I., Neisse, R., Hernandez Ramos, J., Polemi, N., Ruzzante, G., Figwer, M., & Lazari, A. (2019). *A proposal for a European cybersecurity taxonomy*. Publications Office.
- Farhadi, F., Tavafoghi, H., Teneketzis, D., & Golestani, J. (2017). A dynamic incentive mechanism for security in networks of interdependent agents. In L. Duan, A. Sanjab, H. Li, X. Chen, D. Materassi, & R. Elazouzi (Eds.), *Game theory for networks* (pp. 86–96).
- Fleiss, J. L. (1971). Measuring nominal scale agreement among many raters. *Psychological bulletin*, 76(5), 378.
- Friedl, S., Reitinger, T., & Pernul, G. (2024a). Digital detectives: A serious point-and-click game for digital forensics. *IFIP World Conference on Information Security Education*, 129–145.
- Friedl, S., Reitinger, T., & Pernul, G. (2024b). From play to profession: A serious game to raise awareness on digital forensics. *IFIP Annual Conference on Data and Applications Security and Privacy*, 269–289.
- Gelhaar, J., Gürpınar, T., Henke, M., & Otto, B. (2021). Towards a taxonomy of incentive mechanisms for data sharing in data ecosystems. *PACIS*, 121.
- Giannetos, T., Gisdakis, S., & Papadimitratos, P. (2014). Trustworthy people-centric sensing: Privacy, security and user incentives road-map. *2014 13th Annual Mediterranean Ad Hoc Networking Workshop (MED-HOC-NET)*, 39–46.
- Gibbons, R., & Roberts, J. (2013). Economic theories of incentives in organizations. *Handbook of organizational economics*, 56–99.
- Gisdakis, S., Giannetos, T., & Papadimitratos, P. (2016). Security, privacy, and incentive provision for mobile crowd sensing systems. *IEEE Internet of Things Journal*, 3(5), 839–853.
- Goel, S., Williams, K., Huang, J., & Warkentin, M. (2020). Understanding the role of incentives in security behavior. *Hawaii International Conference on System Sciences 2020, HICSS-53*.
- Goel, S., Williams, K. J., Huang, J., & Warkentin, M. (2021). Can financial incentives help with the struggle for security policy compliance? *Information & Management*, 58(4), 103447.
- He, Y., Luo, M., Wu, B., Sun, L., Wu, Y., Liu, Z., & Xiao, K. (2023). A game theory-based incen-

- tive mechanism for collaborative security of federated learning in energy blockchain environment. *IEEE Internet of Things Journal*, 10, 21294–21308.
- Holmstrom, B., & Milgrom, P. (1994). The firm as an incentive system. *The American economic review*, 972–991.
- Kalpana, G., Habelalmateen, M. I., Hussein, A. H. A., Kumar, G. R., & Shreeharsha, J. (2023). Reward and punishment strategy based security enhancement in iot using mobile cloud computing. *2023 International Conference on Ambient Intelligence, Knowledge Informatics and Industrial Electronics (AIKIIIE)*, 1–7.
- Kävrestad, J., Burvall, F., & Nohlberg, M. (2024). A taxonomy of factors that contribute to organizational cybersecurity awareness (csa). *Information & Computer Security*.
- Kenneally, E. (2019a). Economics and incentives driving iot privacy and security, pt. 1. *IEEE Internet of Things Magazine*, 2(1), 6–7.
- Kenneally, E. (2019b). Economics and incentives driving iot privacy and security, pt. 2. *IEEE Internet of Things Magazine*, 2(2), 5–7.
- Kirsch, L., & Boss, S. (2007). The last line of defense: Motivating employees to follow corporate security guidelines. *Proceedings of the 2007 ICIS conference*, 103.
- Kolini, F., & Janczewski, L. J. (2022). Exploring incentives and challenges for cybersecurity intelligence sharing (cis) across organizations: A systematic review. *Communications of the Association for Information Systems*, 50(1).
- Kroll, J. A., Michael, J. B., & Thaw, D. B. (2021). Enhancing cybersecurity via artificial intelligence: Risks, rewards, and frameworks. *Computer*, 54(6), 64–71.
- Kundisch, D., Muntermann, J., Oberländer, A., Rau, D., Roeglinger, M., Schoormann, T., & Szopinski, D. (2021). An update for taxonomy designers - methodological guidance from information systems research. *Business & Information Systems Engineering*, 64.
- Landis, J. R., & Koch, G. G. (1977). An application of hierarchical kappa-type statistics in the assessment of majority agreement among multiple observers. *Biometrics*, 363–374.
- Li, H., Lin, X., & Wu, J. (2022). On-demand incentive design for security-defense resource allocation in 6g vehicular edge learning. *ICC 2022 - IEEE International Conference on Communications*, 1421–1426.
- Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, 45, 13–24.
- Li, M., Salinas, S., & Li, P. (2014). Locaword: A security and privacy aware location-based rewarding system. *IEEE Transactions on Parallel and Distributed Systems*, 25(2), 343–352.
- Li, Q., Wang, X., Wang, P., Zhang, W., & Yin, J. (2022). Farda: A fog-based anonymous reward data aggregation security scheme in smart buildings. *Building and Environment*, 225, 109578.
- Liao, C.-H., & Chen, C.-W. (2014). Network externality and incentive to invest in network security. *Economic Modelling*, 36, 398–404.
- Lu, S., Yang, H., Xu, Y., & Jiang, B. (2022). Incentive-based probability sensitivity suppression in the behavioral security games. *55(6)*, 631–636.
- Luft, J. (1994). Bonus and penalty incentives contract choice by employees. *Journal of Accounting and Economics*, 18(2), 181–206.
- Mair, K., & Schwondra, G. (2023). Deloitte cyber security report 2023 [Accessed: 05/06/24]. *Deloitte*. <https://www2.deloitte.com/content/dam/Deloitte/at/Documents/presse/at-deloitte-cyber-security-report-2023.pdf>
- McConnell, H. J. M., VADM, R., USN, & Grzegorzewski, M. (2022). Cybersecurity and strategic deterrence: Changing adversary's risk versus reward calculations. In A. Farhadi, R. P. Sanders, & A. Masys (Eds.), *The great power competition volume 3: Cyberspace: The fifth domain* (pp. 49–67). Springer International Publishing.
- Morgner, P., Mai, C., Koschate-Fischer, N., Freiling, F., & Benenson, Z. (2020). Security update labels: Establishing economic incentives for security patching of iot consumer products. *2020 IEEE Symposium on Security and Privacy (S&P)*, 429–446.
- Nepal, R., & Jamasb, T. (2015). Incentive regulation and utility benchmarking for electricity network security [Energy]. *Economic Analysis and Policy*.
- Nickerson, R., Varshney, U., & Muntermann, J. (2013). A method for taxonomy development and its application in information systems. *European Journal of Information Systems*, 22.
- Okoli, C., & Schabram, K. (2015). A guide to conducting a systematic literature review of information systems research.
- Peffer, K., Tuunanen, T., Rothenberger, M., & Chatterjee, S. (2007). A design science research

- methodology for information systems research. *Journal of Management Information Systems*, 24.
- Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue. *SAGE open*, 11(1).
- Reittinger, T., Glas, M., Aminzada, S., & Pernul, G. (2024). Employee motivation in organizational cybersecurity: Matching theory and reality. *International Symposium on Human Aspects of Information Security and Assurance*.
- Ryan, R. M., & Deci, E. L. (2017, February 14). *Self-determination theory: Basic psychological needs in motivation, development, and wellness* (Hardcover). The Guilford Press.
- Sharma, S., & Warkentin, M. (2019). Do i really belong?: Impact of employment status on information security policy compliance. *Computers & Security*, 87, 101397.
- Sohail, M. N., Anjum, A., Saeed, I. A., Syed, M. H., Jantsch, A., & Rehman, S. (2024). Optimizing industrial iot data security through blockchain-enabled incentive-driven game theoretic approach for data sharing. *IEEE Access*, 12.
- Statista. (2024, May). Estimated cost of cybercrime worldwide 2017-2028 [Accessed: 05/28/24]. <https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide>
- Vance, A., Siponen, M., & Pahlila, S. (2012). Motivating is security compliance: Insights from habit and protection motivation theory. *Information & management*, 49(3-4), 190–198.
- Verizon. (2024). *2024 data breach investigations report* (tech. rep.).
- Vlachos, V., Katsidimas, I., Kerimakis, E., Nikolettseas, S., Panagiotou, S., & Spirakis, P. (2021). Aspida: A client-oriented platform for assessing websites security practices adoption and reward. *2021 29th Telecommunications Forum (TELFOR)*, 1–4.
- Wahle, J. P., Ruas, T., Mohammad, S. M., Meuschke, N., & Gipp, B. (2023). Ai usage cards: Responsibly reporting ai-generated content. *2023 ACM/IEEE Joint Conference on Digital Libraries (JCDL)*, 282–284.
- Wang, X. (2022). Simulation of the role of emphasis on scheduling in the optimal incentive scheme for marine engineering employee's routine job and information security compliance. *Journal of Ocean Engineering and Science*.
- Wang, X., Wang, C., Sun, Z., & Wang, C. (2022). An optimal coupling incentive mechanism concerning insider's compliance behavior towards marine information security policy. *Journal of Ocean Engineering and Science*.
- Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems*, 18(2), 101–105.
- Wessels, M., van den Brink, P., Verburch, T., Cadet, B., & van Ruijven, T. (2021). Understanding incentives for cybersecurity investments: Development and application of a typology. *Digital Business*, 1(2), 100014.
- Willis, G. B. (2004). *Cognitive interviewing: A tool for improving questionnaire design*. sage publications.
- Xu, J., Chen, L., Liu, K., & Shen, C. (2018). Designing security-aware incentives for computation offloading via device-to-device communication. *IEEE Transactions on Wireless Communications*, 17(9), 6053–6066.
- Yang, Y., Ji, G., Yang, Z., & Xue, S. (2019). Incentive contract for cybersecurity information sharing considering monitoring signals. *2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 507–512.
- Yoshioka, R., Sakurai, Y., Oyama, S., & Shinoda, M. (2023). Proposing a new security game with reward and penalty. *2023 IEEE/WIC International Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT)*, 205–212.
- Zhan, X., Nah, F. F.-H., & Cheng, M. X. (2018). An assessment of users' cyber security risk tolerance in reward-based exchange. In F. F.-H. Nah & B. S. Xiao (Eds.), *Hci in business, government, and organizations* (pp. 431–441). Springer International Publishing.
- Zhao, R., Jiang, L., & Zhang, J. (2018). An insurance-based incentive mechanism for mobile crowdsourcing to improve system security. *2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design*.
- Zhu, X., Zhao, J., & Hu, Z. (2019). Incentive mechanism design for security investment with local exit equilibrium on structured populations. *Physica A: Statistical Mechanics and its Applications*.
- Zimmermann, V., & Renaud, K. (2019). Moving from a 'human-as-problem' to a 'human-as-solution' cybersecurity mindset. *International Journal of Human-Computer Studies*, 131, 169–187.