

# **Unpacking the Complex Relationship Between Employees' Security Fears and Complacency**

**Early-stage paper**

**Ali Vedadi**

University of Tennessee,  
Knoxville  
avedadi@utk.edu

**Sahar Farshadkhah**

University of Illinois,  
Springfield  
sfars2@uis.edu

## **ABSTRACT**

As many organizations are aggressively employing AI-based and highly automated security tools, employees are expected to develop a sense of security cyber-complacency by overrelying on the efficacy of these tools. This reduced vigilance may lead to lower levels of compliance with information security policies. An antithetical factor to cyber-complacency is fear, which is often fueled by a heightened awareness of the pervasive nature of cyber threats and compliance bolstered by the fear appeals employed by the organization. Each employee may possess a certain level of cyber-complacency and fear simultaneously due to various circumstances that shape them. This research contributes to information security literature by examining and unpacking the intricate and curvilinear interrelationship between cyber-complacency and fear as two antithetical factors in shaping compliance behaviors. We use polynomial regression and response surface analysis to investigate the extent and pattern of how the (in)congruence between cyber-complacency and level of fear is associated with the extent of compliance with information security policies.

## ***Keywords***

Cyber-complacency; fear; information security policy compliance; perceptual congruence; polynomial regression; response surface analysis.

## INTRODUCTION

In the current digital landscape, ensuring a robust organizational information security posture has become imperative not only for safeguarding sensitive information but also for organizational survival. However, the number and severity of cyber incidents show no signs of abating. In response, organizations are increasingly turning to advanced artificial intelligence (AI) tools to automate and enhance their information security operations by employing adaptive threat detection, incident response, and vulnerability management (Grand Research View 2023). Such an approach can be critical in combating the ever-increasing sophistication and volume of cyber threats, as these new tools can continuously learn and improve their capabilities, enabling the organization to stay ahead of emerging cyber threats. Despite its significant advantages, this approach is not a panacea to cybersecurity problems and requires human intelligence and oversight as a complementary factor to maximize its full potential. Relatedly, employees' compliance with information security policies can significantly contribute to safeguarding organizational assets against attacks. By understanding and following established protocols, employees enhance the overall resilience of the organization against threats and serve as the frontline defense in protecting information assets (Menard et al. 2017; Cram et al. 2019; Chen et al. 2021).

Nevertheless, the increasing use of AI tools for cybersecurity in organizations can potentially lead to a phenomenon known as cyber-complacency, defined as the extent to which an employee may overrely on expert security protections at their workplaces (Stafford 2022). This attitude typically arises when individuals develop a false sense of security and become overly dependent on the capabilities of these automated tools, neglecting their own vigilance and adherence to information security policies. In other words, the widespread deployment of automated security tools can foster a sense of detachment among employees, as they may perceive

cybersecurity as solely the responsibility of these technologies. In general, complacency can lead to decreased personal accountability and a tendency to overlook human-centric information processing practices (Merritt et al. 2019).

In the context of information security, cyber-complacency can manifest in employees neglecting to report suspicious activities or potential security incidents, assuming that automated tools are infallible and will effectively defend against threats. Such lack of vigilance and reporting can delay identifying and mitigating threats, potentially leading to more severe consequences. For example, when employees are aware that their organization is employing highly automated, AI-based phishing detection tools within their email systems, automation-induced cyber-complacency may undermine their compliance with information security (infosec) policies, such as exerting cognitive effort into identifying phishing cues and reporting suspicious messages. In juxtaposition with cyber-complacency, prior research has shown that fear is critical in determining individuals' behavior when encountering phishing messages (Moody et al. 2017). Therefore, the increasing usage of highly automated, AI-based security tools by organizations is expected to lessen the positive impact of fear in exhibiting secure behaviors. The findings in some other disciplines lend support to this premise. For instance, aviation psychology literature has shown that pilot complacency, induced by overreliance on high-technology automatic systems and, consequently, sub-optimal human monitoring of threats, accounts for numerous accidents (Parasuraman et al. 1993; Prinzel 2002).

Current information security literature has received only scant attention to the crucial role of cyber-complacency in influencing security behaviors and its interactive relationships with other relevant factors (Stafford 2022; Greulich et al. 2024). Regarding the evolving circumstances and the fact that many organizations are aggressively employing AI-based security tools (a market that

is projected to increase from USD 22.4 billion in 2023 to USD 60.6 billion by 2028, according to (Market and Market Research 2024)), there is a pressing need to advance the existing understanding of cyber-complacency in the information security context and investigate its effect on security behaviors. The importance of this inquiry also rests in the fact that the current information security literature has shown conflicting and mixed results regarding the impact of fear on security behaviors (Kajtazi et al. 2021, Johnston et al. 2023). This research contributes to information security literature by further examining cyber-complacency and unpacking the intricate and curvilinear interrelationship between cyber-complacency and fear as two antithetical factors and the level of (in)congruence between them. In sum, we aim to answer the following research question: *To what extent and in what pattern is the (in)congruence between employees' cyber-complacency and level of fear associated with their extent of compliance with information security policies?*

In the next few sections, we will discuss the theoretical background, present the hypotheses, and explain the analytical approach for hypothesis testing.

## **BACKGROUND AND HYPOTHESES**

### ***Cyber-Complacency: Theoretical Roots and Initial Evidence***

Complacency has received scholarly attention in other disciplines. For instance, regarding the profound consequences for flight safety, automation-induced complacency in aviation management has been extensively investigated. This phenomenon refers to the tendency of pilots to become overly reliant on automated systems, potentially resulting in attention degradation and reduced situational awareness. The findings have prompted ongoing debates regarding the optimal balance between automation and manual control, as well as the development of strategies to mitigate the potential negative effects of automation-induced complacency on pilot performance

and decision-making (Parasuraman et al. 1993, Prinzel et al. 2005; Singh et al. 1993). Complacency has also been studied in the healthcare context. For example, Goddard et al. (2012) discovered the negative effects of healthcare specialists' overreliance on highly automated clinical decision support systems and their tendency to accept inaccurate advice.

Cyber-complacency in the context of information security addresses the attitude among employees who exhibit reduced vigilance and a lower urge for proactiveness against cybersecurity threats. Cyber-complacency typically emerges as a gradual relaxation of compliance with security policies, diminished reporting of suspicious activities, and even increased instances of exhibiting risky behaviors. It can contribute to the gradual erosion of security consciousness and create the circumstances to tackle such issues before malicious actors exploit them. Stafford (2022) identified social cyber-complacency as a main type of cyber-complacency that is induced by an employee's perception that other people, coworkers, or the organization, in general, are protecting them against cyber threats and is based on the assumption that the information technology (IT) department is sufficiently and comprehensively ensuring security. Thus, the employee may tend to allocate full attention to task performance and productivity with relaxed security vigilance. Greulich et al. (2024) confirmed this by showing that trust in organizational protective structures can lead to employees' lower security fear to the extent that it constrains their cognitive efforts to inspect the security environment for potential cyber threats scrupulously.

### ***Cyber-complacency vs. Fear***

In the realm of information security, employees' cyber-complacency and fear of threats represent two diametrically opposed forces shaping security behaviors. These contrasting factors can be viewed as polar opposites, exerting divergent influences. Cyber-complacency suggests an indifferent attitude and nonchalance toward potential cyber threats and breeds a lackadaisical

approach to security, leading to more frequent cases of neglecting essential precautions. Such complacency among employees may be based on the perception that the organization sufficiently ensures information security by utilizing advanced and automated tools, thus minimizing the importance of the human factor in this area.

Antithetical to cyber-complacency is the fear of threats, defined as “a negative emotion evoked by a perceived threat that is considered harmful and pertinent” (Witte 1992). This fear is often fueled by a heightened awareness of the pervasive nature of cyber threats, bolstered by the fear appeals employed by the organizations (Johnston et al. 2015, Boss et al. 2015). Employees gripped by this fear may adopt a highly cautious approach, meticulously adhering to security policies and exhibiting thorough vigilance toward potential security risks. Excessive fear can also be related to maladaptive responses to fear appeals. When employees hold the belief that they are incapable of coping with fear, they may dismiss coping messages, exhibit sub-optimal security behaviors, or even develop fear-induced anxiety and depression (Wall and Warkentin 2019).

These two opposing factors, cyber-complacency and fear of threats, represent the extremes of a continuum that governs employees' security behaviors. It is reasonable to argue that each employee might perceive a different level of cyber-complacency and fear simultaneously. Organizations can arouse fear in employees by making examples of security breaches and their negative consequences, framing security threats in terms of direct impact on employees' work and personal data, and using persuasive messages that emphasize the severe consequences of security breaches (Schuetz et al. 2020). Concurrently, employees' cyber-complacency may arise when the organization emphasizes its robust security infrastructure, leading them to develop an exaggerated sense of protection. When employees are informed and reminded about advanced firewalls, intrusion prevention systems, anti-phishing tools, and other sophisticated security measures, they

may believe the organization is impenetrable and, thus, develop a false sense of invulnerability, often stemming from a misunderstanding of security layers and an overestimation of technological solutions (Stafford 2022).

Although one could argue that compliance will be maximized when the fear is at the highest level and complacency at the lowest level, assuming linearity between these two opposing factors may mask the inherent theoretical intricacies and their potential curvilinear relationships. Specifically, employees' perceptual (in)congruence between cyber-complacency and fear of security threats is a complex psychological phenomenon that can significantly impact their compliance with information security policies. This (in)congruence, in the context of this study, refers to the extent of similarity between an employee's sense of cyber-complacency and their level of fear about potential security threats. The level of (in)congruence between cyber-complacency and fear of security threats can influence compliance with information security policies in several ways, depending on four conditions, such as low complacency, high fear (LC-HF), high complacency, low fear (HC-LF), high complacency, high fear (HC-HF), and low complacency, low fear (LC-LF).

In the low complacency, high fear (LC-HF) scenario, employees are likely to exhibit the highest levels of compliance with security policies. The low complacency keeps employees vigilant, while their high fear of threats motivates them to adhere strictly to security measures. Employees are more likely to follow protocols, report suspicious activities, and actively engage in security training in response to fear appeals (Boss et al. 2015). High complacency, low fear (HC-LF), however, may lead to the lowest compliance with security policies. Employees who feel overly secure and have little fear of threats may see security measures as unnecessary or a waste of time. They might circumvent policies for convenience, believing their role in security organizational

information assets is minimal because the existing technical measures and automated tools offer sufficient protection.

The high complacency, high fear (HC-HF) combination is expected to result in inconsistent compliance behaviors. Employees may intellectually understand the threats and recognize their potentially severe consequences (i.e., high fear) but still feel that the organization is doing enough to effectively ensure information security without much employee involvement (i.e., high complacency) (Stafford 2022). This cognitive dissonance might lead to selective and erratic compliance behavior, where employees follow some policies but ignore others based on the context or convenience. Therefore, the compliance level will be lower than LC-HF and higher than HC-LF.

Finally, the low complacency, low fear (LC-LF) condition presents a nuanced scenario of information security policy compliance in which employees are expected to exhibit low complacency, demonstrate a lack of overreliance on organizational security tools, possess a baseline awareness of potential vulnerabilities, and acknowledge the importance of proactiveness in contributing to organizational security. Concurrently, their low fear suggests an absence of heightened threat perception or anxiety regarding cyber threats. This cognitive state may result in a measured approach to policy adherence, characterized by rational evaluation rather than emotional reactivity (Johnston et al. 2023). It is reasonable to expect that the compliance level in this state is higher than that of HC-LF and HC-HF but lower than that of LC-HF.

These relationships, however, are expected to be non-linear and follow a complex pattern. Specifically, the extended parallel process model (EPPM) suggests that performance increases with mental arousal, but only up to a point (Shen 2017). When the level of arousal is too high, performance decreases. Applying this to cybersecurity, we posit that low fear leads to low



compliance, moderate fear leads to optimal compliance, and high fear leads to decreased performance (due to excessive anxiety and helplessness). Although some level of fear or perceived threat is necessary to motivate compliance with information security policies, excessive fear may be counterproductive. The optimal level would be a moderate amount of concern that motivates action without overwhelming or paralyzing employees.

The same logic may apply to cyber-complacency as well. Employees are expected to exhibit high compliance with information security policies at the low levels of cyber-complacency by being vigilant and aware of potential cyber threats and engaging in security behaviors, recognizing their important role in protecting information assets. As complacency increases to moderate levels, compliance may start to decline as employees overrely on the perceived sophistication of the organization's automated cybersecurity tools, leading to a false sense of security and reduced personal vigilance. The extreme levels of cyber-complacency may lead to actual or near-miss cyber incidents (e.g., falling for a phishing attack). This sudden realization of actual cyber threats could trigger an increased awareness of the threats among employees, leading to a rapid shift in security vigilance, recognizing the limitations of automated security measures, and realizing the critical importance of their proactiveness in security information assets. This newfound awareness can cause a surge in compliance behaviors. These arguments lead us to the following hypotheses:

H1: Congruence between cyber-complacency and fear is associated with a positive, curvilinear relationship with compliance.

H2: Incongruence between cyber-complacency and fear is associated with a negative, curvilinear relationship with compliance.

## METHODOLOGY

### *Sample and Measures*

The target population for this research is employees who regularly use computers and other digital devices for task performance and have full-time employment in a US-based organization that offers regular security education, training, and awareness (SETA) programs. Participants are recruited through an online market research platform. We employed the survey approach for data collection. The market research firm distributed the online survey among the eligible participants. Compliance was measured using the self-report items adapted from Hsu et al. (2015). Fear was measured using the scale adapted from Moody et al. (2018). We developed our own scale because no validated measurement scale for cyber-complacency was available in the information security literature. The process is explained in the Appendix.

### *Analytical Approach*

After performing a rigorous data quality check and ensuring construct reliability and validity, we use polynomial regression (PR) and response surface analysis (RSA) to test the hypotheses. A second-order or quadratic polynomial equation corresponding to the theoretical model is shown below:

$$Y = b_0 + b_1X_1 + b_2X_2 + b_3X_1^2 + b_4X_2^2 + b_5X_1X_2 + \epsilon.$$

Where  $Y$  is the dependent variable,  $X_1$  and  $X_2$  are the predictor or independent variables, and  $\epsilon$  is the error term. Following Edwards and Parry (1993) methodology, the polynomial regression analysis is performed first to investigate whether 1) the second-order model can explain a significant amount of variance in the outcome variable compared with the first-order or linear model, 2) if a significant quadratic term is present 3) the variance explained by the terms one order

higher (i.e., cubic) explains significantly higher variance than the quadratic model. If not, there will be no need to consider the equation with cubic terms. Then, we will proceed to RSA, a visualization method that helps interpret the quadratic terms in polynomial regression. By producing three-dimensional surfaces, RSA provides insights into the complex relationship between variables of interest.

Two of the main features of a response surface are slopes along the lines of congruence (LOC), such as  $X_1 = X_2$  and line of incongruence (LOIC) ( $X_1 = -X_2$ ). In this study, where ( $X_1$  = cyber-complacency,  $X_2$  = fear, and  $Y$  = compliance), The LOC represents all combinations where the two predictor variables are equal. It depicts perfect congruence or alignment between the two constructs being measured. On a response surface plot, the LOC is typically represented by a straight line running diagonally from the front to the plot's back corner. The LOIC represents all combinations where the two predictor variables are opposite and equal in magnitude. It shows the effect of the discrepancy between the two constructs on the outcome variable. On a response surface plot, the LOIC is perpendicular to the LOC and typically runs from the left corner to the right corner of the plot. RSA also provides estimates for the slope and curvature values for these two lines. The slope values represent how the outcome variable changes as both predictors increase equally or how the outcome changes as the discrepancy between predictors increases. The curvature estimates indicate whether the relationship between the predictor discrepancy and the outcome is non-linear and curved.

## CONCLUSION AND EXPECTED FINDINGS

Examining the role of employee security cyber-complacency in behavioral information security research is crucial for several reasons. Cyber-complacency, characterized by reduced vigilance and lower compliance with security policies due to overreliance on organizational cybersecurity

tools, can significantly impact an organization's information security posture. Understanding this phenomenon is essential for developing effective strategies to maintain high-security awareness and employee compliance levels. It can also shed light on its interrelated and complicated relationship with the opposing factors that could shape security behaviors like compliance. By investigating this topic, researchers can provide valuable insights for organizations to more effectively manage human factors in cybersecurity, ultimately enhancing their ability to protect sensitive information and mitigate security risks.

By answering the overall research question, “To what extent and in what pattern is the (in)congruence between employees’ cyber-complacency and level of fear associated with their extent of compliance with information security policies?”, this research aims to contribute to information security literature by examining and unpacking the intricate and curvilinear interrelationship between cyber-complacency and fear as two antithetical factors in shaping compliance behaviors. We expect to find that 1) when employees’ simultaneous perceptions of cyber-complacency and level of fear are congruent, their extent of compliance with information security policies increases curvilinearly and, 2) when employees’ simultaneous perceptions of cyber-complacency and level of fear are incongruent, their extent of compliance with information security policies decreases curvilinearly.

## REFERENCES

- Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and Polak, P. 2015. “What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors,” *MIS Quarterly* (39:4), pp. 837–864. (<https://doi.org/10.25300/MISQ/2015/39.4.5>).
- Chen, Y., Galletta, D. F., Lowry, P. B., Luo, X., Moody, G. D., and Willison, R. 2021. “Understanding Inconsistent Employee Compliance with Information Security Policies through the Lens of the Extended Parallel Process Model,” *Information Systems Research* (32:3), pp. 1043–1065. (<https://doi.org/10.1287/ISRE.2021.1014>).

- Cram, A.W., D'Arcy, J., and Proudfoot, J. G. 2019. "Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance," *MIS Quarterly* (43:2), pp. 525–554. (<https://doi.org/10.25300/MISQ/2019/15117>).
- Edwards, J. R., and Parry, M. E. 1993. "On the Use of Polynomial Regression Equations As An Alternative to Difference Scores in Organizational Research," *Academy of Management Journal* (36:6). (<https://doi.org/10.5465/256822>).
- Goddard, K., Roudsari, A., and Wyatt, J. C. 2012. "Automation Bias: A Systematic Review of Frequency, Effect Mediators, and Mitigators," *Journal of the American Medical Informatics Association*. (<https://doi.org/10.1136/amiajnl-2011-000089>).
- Grand Research View. 2023. "AI in Cybersecurity Market Size & Trends," <https://www.grandviewresearch.com/industry-analysis/artificial-intelligence-cybersecurity-market-report>.
- Greulich, M., Lins, S., Pienta, D., Thatcher, J. B., and Sunyaev, A. 2024. "Exploring Contrasting Effects of Trust in Organizational Security Practices and Protective Structures on Employees' Security-Related Precaution Taking," *Information Systems Research*. (<https://doi.org/10.1287/isre.2021.0528>).
- Hsu, J. S. C., Shih, S. P., Hung, Y. W., and Lowry, P. B. 2015. "The Role of Extra-Role Behaviors and Social Controls in Information Security Policy Effectiveness," *Information Systems Research* (26:2), pp. 282–300. (<https://doi.org/10.1287/isre.2015.0569>).
- Johnston, A. C., Warkentin, M., and Siponen, M. 2015. "An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric," *MIS Quarterly* (39:1), pp. 113–134. (<https://doi.org/10.25300/MISQ/2015/39.1.06>).
- Johnston, A., Gangi, P. M. D., Bélanger, F., Crossler, R. E., Siponen, M., Warkentin, M., and Singh, T. 2023. "Seeking Rhetorical Validity in Fear Appeal Research: An Application of Rhetorical Theory," *Computers and Security* (125). (<https://doi.org/10.1016/j.cose.2022.103020>).
- Kajtazi, M., Sarker, S., Johansson, B., Holmberg, N., Keller, C., and Tona, O. 2021. "Toward a Unified Model of Information Security Policy Compliance: A Conceptual Replication Study," *AIS Transactions on Replication Research* (7). (<https://doi.org/10.17705/1attr.00067>).
- Market and Market Research. 2024. "Artificial Intelligence in Cybersecurity Market."
- Menard, P., Bott, G. J., and Crossler, R. E. 2017. "User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory," *Journal of Management Information Systems* (34:4), pp. 1203–1230. (<https://doi.org/10.1080/07421222.2017.1394083>).

- Merritt, S. M., Ako-Brew, A., Bryant, W. J., Staley, A., McKenna, M., Leone, A., and Shirase, L. 2019. "Automation-Induced Complacency Potential: Development and Validation of a New Scale," *Frontiers in Psychology* (10:FEB). (<https://doi.org/10.3389/fpsyg.2019.00225>).
- Moody, G. D., Galletta, D. F., and Dunn, B. K. 2017. "Which Phish Get Caught An Exploratory Study of Individuals' Susceptibility to Phishing," *European Journal of Information Systems* (26:6). (<https://doi.org/10.1057/s41303-017-0058-x>).
- Moody, G. D., Siponen, M., and Pahnla, S. 2018. "Toward a Unified Model of Information Security Policy Compliance," *MIS Quarterly* (42:1), pp. 285–311. (<https://doi.org/10.25300/MISQ/2018/13853>).
- Parasuraman, R., Molloy, R., and Singh, I. L. 1993. "Performance Consequences of Automation-Induced 'Complacency,'" *The International Journal of Aviation Psychology* (3:1). ([https://doi.org/10.1207/s15327108ijap0301\\_1](https://doi.org/10.1207/s15327108ijap0301_1)).
- Prinzel, L. J., Freeman, F. G., and Prinzel, H. D. 2005. "Individual Differences in Complacency and Monitoring for Automation Failures," *Individual Differences Research* (3:1).
- Prinzel, L. J. I. 2002. "The Relationship of Self-Efficacy and Complacency in Pilot-Automation Interaction," *NASA/TM-2002-211925* (September).
- Schuetz, S. W., Benjamin Lowry, P., Pienta, D. A., and Bennett Thatcher, J. 2020. "The Effectiveness of Abstract Versus Concrete Fear Appeals in Information Security," *Journal of Management Information Systems* (37:3). (<https://doi.org/10.1080/07421222.2020.1790187>).
- Shen, L. 2017. "Putting the Fear Back Again (and Within Individuals): Revisiting the Role of Fear in Persuasion," *Health Communication* (32:11). (<https://doi.org/10.1080/10410236.2016.1220043>).
- Singh, I. L., Molloy, R., and Parasuraman, R. 1993. "Automation-Induced 'Complacency': Development of the Complacency-Potential Rating Scale," *The International Journal of Aviation Psychology* (3:2). ([https://doi.org/10.1207/s15327108ijap0302\\_2](https://doi.org/10.1207/s15327108ijap0302_2)).
- Stafford, T. F. 2022. "Platform-Dependent Computer Security Complacency: The Unrecognized Insider Threat," *IEEE Transactions on Engineering Management* (69:6). (<https://doi.org/10.1109/TEM.2021.3058344>).
- Wall, J. D., and Warkentin, M. 2019. "Perceived Argument Quality's Effect on Threat and Coping Appraisals in Fear Appeals: An Experiment and Exploration of Realism Check Heuristics," *Information and Management* (56:8). (<https://doi.org/10.1016/j.im.2019.03.002>).

Witte, K. 1992. "Putting the Fear Back into Fear Appeals: The Extended Parallel Process Model," *Communication Monographs* (59:4), pp. 329–349. (<https://doi.org/10.1080/03637759209376276>).

## APPENDIX

The process of developing the measurement scale for the cyber-complacency construct was informed by MacKenzie et al. (2011) guidelines. The next few sections describe the scale development process, including conceptualization, development of measures, model specification, and scale evaluation and refinement.

### *Conceptualization and Item Development*

We first specified the domain and developed a conceptual definition of cyber-complacency. Based on the related studies, we defined cyber-complacency as the “the extent to which an employee may overrely on expert security protections at their workplaces”. For the subsequent stages of scale development, we used two independent samples. Sample A was used for content validation. Sample B was used for the exploratory factor analysis (EFA), and since all items loaded perfectly, we continued with the same sample for the confirmatory factor analysis (CFA). Sample A was a panel of scholars with extensive experience in behavioral information security research. Sample B was determined to be the employees of a US-based organization who regularly used computers and other digital devices for task performance and had full-time employment in an organization that offered regular security education, training, and awareness (SETA) programs. Participants of sample B were recruited through an online market research platform.

Initially, we developed items that corresponded to the construct's definition by reviewing scales for measuring complacency in other fields of study, such as aviation and healthcare (e.g., Parasuraman et al. 1993; Betsch et al. 2018), and ran a few iterations to ensure that all essential

tenets of cyber-complacency are sufficiently captured. To assess the content validity of items, a total of eight items, alongside the definition, were presented to sample A, who were asked to rate each item's validity using a five-point scale and provide comments. After collecting the comments and seeking additional feedback from the panel, the items were refined to ensure that the items do not have any significant overlap with the other related core constructs in the behavioral information security nomological network. There was also a consensus that the items should be specified as reflective (Bollen 2002). The revised items were as follows:

1. My organization takes such good care of my information security that I don't really need to be concerned about it.
2. I don't need to bother with information security in my job because my organization is fully controlling it.
3. I believe that my organization is protecting me against information security attacks so well that I don't need to worry about them.
4. I believe that my organization is handling my information security so well that I can largely depend on it.
5. I spend little time thinking about information security in my job because my organization is totally taking care of it.
6. I don't need to worry about information security at the workplace because my organization thoroughly watches over it.
7. I can fully rely on my organization's capability to deal with everything security-related.
8. My organization addresses everything information security-related so effectively that I don't really need to be alert all the time.

### ***Scale Evaluation and Validity Assessment***

Once our content-validated items were generated, we conducted a pretest and an exploratory factor analysis from sample B. The online survey instrument included quality check filters, such as attention-check, speed-check, response set, and reCAPTCHA verification. We also randomized the items and ensured the anonymity of the survey participants to reduce common-method bias.



Before data collection, IRB approval was acquired. We collected 80 complete responses that passed all the filters. The average was 45 years old, with a standard deviation of 14.38 and an equal distribution between male and female respondents. The respondents were from various industries. We performed a principal components analysis in SPSS on the eight items with varimax rotation. Hinkin (1995) recommends retaining only items with factor loadings exceeding 0.40. All of the item loadings exceeded 0.40 on the single-factor solution. The Cronbach's alpha was 0.90. To investigate whether there is initial evidence for discriminant validity, we selected two similar constructs that are theoretically germane to cyber-complacency and share core characteristics. These constructs included dispositional optimism and information security apathy<sup>1</sup>. To measure information security apathy, we used the scale adapted from Boss et al. (2009), which include items "paying attention to security takes too much time" and "I am too busy to be bothered by information security concerns".

Moreover, we used Scheier et al. (1994) scale for dispositional optimism that includes three items, such as "In uncertain times, I usually expect the best", "I'm always optimistic about my future", and "Overall, I expect more good things to happen to me than bad.". The responses were scaled at the seven-point agree/disagree Likert scale. The exploratory analysis extracted three separate factors. The cyber-complacency items were loaded on a separate factor, and there were no cross-loadings. Table 1 depicts the item loading details.

---

<sup>1</sup> Similar to this method, Amo et al. (2022), in the same stage of scale development for the information technology entitlement construct, included general entitlement and narcissism in the factor analysis to compare the loadings.

Item	Factor		
	1	2	3
Cyber-complacency 1	<b>.683</b>	.105	.007
Cyber-complacency 2	<b>.693</b>	-.025	.079
Cyber-complacency 3	<b>.813</b>	.163	.039
Cyber-complacency 4	<b>.741</b>	.109	.068
Cyber-complacency 5	<b>.798</b>	-.093	.161
Cyber-complacency 6	<b>.751</b>	-.014	.139
Cyber-complacency 7	<b>.810</b>	.173	.085
Cyber-complacency 8	<b>.794</b>	.301	.077
Optimism1	.254	<b>.864</b>	-.072
Optimism2	.049	<b>.930</b>	.102
Optimism3	.022	<b>.925</b>	.090
Apathy1	.145	.036	<b>.948</b>
Apathy2	.142	.077	<b>.956</b>

**Table 1. Item Loadings**

Next, we conducted the confirmatory factor analysis using Amos v28. The fit statistics values were acceptable ( $\chi^2 / df = 1.30$ , CFI = 0.97, RMSEA = 0.06, SRMR = 0.06) (Hu and Bentler 1999; MacKenzie et al. 2011). To assess the convergent validity, we calculated the average variance extracted (AVE) values, which were greater than 0.50, thus indicating convergent validity (Fornell and Larcker 1981). Moreover, the composite reliability (CR) values were all above 0.90, exceeding the recommended minimum of 0.70. We also employed the heterotrait-monotrait ratio of correlations (HTMT) approach to assess the discriminant validity. The HTMT ratios for the constructs were well below the conservative threshold of 0.85, indicating discriminant validity (Henseler et al. 2015). Table 3 shows these values.

Construct (CR; AV)	Cyber-complacency	Optimism	Apathy
Cyber-complacency (0.90; 0.54)	-		
Optimism (0.90; 0.76)	0.236	-	
Apathy (0.93; 0.87)	0.257	0.115	-

**Table 2. Construct Reliability and Validity**