Scientific Research Publishing

Journal of Information Security, 2023, 14, 93-110
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Appraising the Manifestation of Optimism Bias and Its Impact on Human Perception of Cyber Security: A Meta Analysis

Khaled M. Alnifie, Charles Kim

Department of Electrical Engineering and Computer Science, Howard University, Washington DC, USA
Email: al.nifie.khaled@gmail.com, ckim@howard.edu

How to cite this paper: Alnifie, K.M. and Kim, C. (2023) Appraising the Manifestation of Optimism Bias and Its Impact on Human Perception of Cyber Security: A Meta Analysis. *Journal of Information Security*, **14**, 93-110.
https://doi.org/10.4236/jis.2023.142007

Received: January 5, 2023
Accepted: February 20, 2023
Published: February 23, 2023

Abstract

Cyber threats and risks are increasing exponentially with time. For preventing and defense against these threats and risks, precise risk perception for effective mitigation is the first step. Risk perception is necessary requirement to mitigate risk as it drives the security strategy at the organizational level and human attitude at individual level. Sometime, individuals understand there is a risk that a negative event or incident can occur, but they do not believe there will be a personal impact if the risk comes to realization but instead, they believe that the negative event will impact others. This belief supports the common belief that individuals tend to think of themselves as invulnerable, *i.e.*, optimistically bias about the situation, thus affecting their attitude for taking preventive measures due to inappropriate risk perception or overconfidence. The main motivation of this meta-analysis is to assess that how the cyber optimistic bias or cyber optimism bias affects individual's cyber security risk perception and how it changes their decisions. Applying a meta-analysis, this study found that optimistic bias has an overall negative impact on the cyber security due to the inappropriate risk perception and considering themselves invulnerable by biasing that the threat will not occur to them. Due to the cyber optimism bias, the individual will sometimes share passwords by considering it will not be maliciously used, lack in adopting of preventive measures, ignore security incidents, wrong perception of cyber threats and overconfidence on themselves in the context of cyber security.

Keywords

Cyber Security, Meta-Analysis, Optimistic Bias, Optimism Bias, Risk Perception, Cognitive Bias

1. Introduction

Cybercrime continues unabatedly and is unlikely to cease. Simply put, cybercrime is too simple to conduct, too profitable to achieve more in less effort and time, and there are too few chances to get caught and get punished [1]. The most technologically adept information technology or tech businesses are on par with high-end cybercriminals in terms of sophistication, and both have embraced latest and sophisticated technologies like cloud computing, artificial intelligence, software-as-a-service, and encryption rapidly [2] [3]. Cybercriminals use both basic and advance technologies like artificial intelligence tools, automated tools for creating software and exploits for special purposes, tools for target identification and finding vulnerabilities. They monetize what they steal through cyber breaches like selling of credentials and proprietary data as well as zero-day exploits. All these works because most of the users are still lacking in adopting very basic cyber security measures [4] and many technology products lack adequate defenses [2].

According to the predictions of the Cybercrime Magazine for 2023, the cybercrime damage is predicted to hit $10.5 trillion annually by 2025; global cyber security spending will exceed $1.75 trillion cumulatively from 2021 to 2025; and the cyber insurance market will predict to touch $14.8 billion annually [5]. Another report "Cyberwarfare in the C-Suite" assessed that cybercrime to cost the world $10.5 trillion annually by 2025 [6].

Why are the statistics going so high? This is because when a CEO or CISO faces a cyber-attack or data breach, they begin to worry about their technological weaknesses and neglect to consider the very common weakness, *i.e.*, the people (their employees) who utilize those technologies daily [7]. The 2022 Verizon Data Breach Investigations Report (DBIR) indicates that human errors both originate and amplify the risk of cybercrime and the harm it poses to enterprises, with 82% of cyber breaches being linked to human error and social engineering [8]. To counteract this threat, corporate directors, CEOs, CISOs, and managers should first identify the causes and human flaws before coming up with solutions to stop such breaches.

Individuals (humans), including both internal and external users, are the weakest link in cybersecurity, whether it is because of human error, script-kiddies, or deliberate attacks by skilled cybercriminals [9]. Users are frequently the victims of breaches that are brought on by unsafe activities such as using weak passwords, acting impulsively, taking risks, unintentionally installing viruses, and social engineering exploits [10]. Attackers' primary strategies include social engineering attacks such as impersonation, phishing emails, etc. For instance, hackers employed social engineering strategies to obtain credentials from the target employee in order to access to millions of Uber customers' records [11]. Technology by itself cannot significantly defend from cyber security risks and threats.

This study has been motivated by a cliché in the cyber security literature and community that is "understanding the cyber security issues—vulnerabilities,

threats and risks—by individuals but giving low priority to address or mitigating them". This has been investigated by whether users exhibit an optimistic bias in their assessment of cyber risk in an effort to explain the above axiom. People think they have lower odds of suffering a bad event than other people do [12]. Optimistic bias refers to this error in judgement, which is an underestimating of the likelihood or probability of encountering bad occurrences in comparison to others [13]. According to the assumptions of optimistic bias, people frequently believe that if they have special abilities or act in a less dangerous way than others, they will be less likely to be the target of security breaches [14]. This, according to Weinstein, is defensive or wishful thinking [12]. People exhibit a predisposition for optimistic bias in many bad scenarios, such as cyber attacks while using a computer, utilizing, or surfing the internet or social media platforms, or cyberattacks in general.

Despite a very important issue that leads to incorrect or inappropriate risk perception of being invulnerable, few studies have examined cyber optimism bias in the cyber security context. It can be inferred, however, that individuals may perceive themselves to be less likely than others to be the victim of cyber attacks, which can in turn have a substantial impact on their attitude toward adopting preventive measures against such attacks or act in a different way. Therefore, it has been contended in this study that it is crucially important to understand optimism bias in the context of cyber security, as this bias may interfere with one's decision about whether to take preventive measures to prevent cyber-attacks and breaches and consequently increase susceptibility to them. This study hypothesizes that a person with strong optimism bias holds a more unfavorable attitude toward preventive measures against cyber-attacks and adopting of preventive measures as compared to those with weak optimism bias. And as per different researchers like Komatsu *et al.* (2013) and Gratian *et al.*, (2018) a person's intentions influence their actual behavior indirectly through cognitive processes and a person having optimism bias in the context of cyber security and preventive measures, will have a different attitude due to which his or her intentions towards preventive measures of compliance with cyber security measures will be impacted [15] [16].

Through a meta-analytic method, the current study aims to comprehensively evaluate the effects of cognitive biases, particularly optimism bias, on human attitudes and their perception of cyber risk and adopting of preventive measures. The sub-objectives of the study are as under: 1) this research will offer an up-to-date analysis with implications for both research and practice that are distinct, original, and practical; 2) this research will aid in determining whether or not an optimistic attitude toward cyberthreats has a negative impact on cyber security and how the optimism bias has been linked to human attitudes and cyber risk perceptions; 3) this research will find out that either the stance that people with optimism bias are more get infected and targeted as compared to other people or not.

The rest of this article is structured as follows. First, a succinct assessment of

the major themes, definitions, and specifics of optimism bias are provided. Second, a discussion of the methods utilized to find pertinent literature and carry out our meta-analysis follows. The findings of this meta-analysis are then provided. We conclude by discussing the findings, their significance for both research and practice, and conclusion.

2. Literature Review

In general, when faced with real threats, people react positively. The issue is that what we perceive is frequently not reality but a biased perspective, either because we lack the knowledge necessary to accurately estimate the hazards or because we have a motivation to underestimate the risk [17]. In other words, people exhibit a propensity to think they are less at risk than others in many dangerous situations. Unrealistic optimism or optimistic bias refers to this underestimating of the likelihood or probability of experiencing undesirable occurrences [18]. The parts that follow provide information on bias in general and elaborate on optimism bias in relation to cyber security and cyber risk perception.

2.1. Bias

The term "bias" refers to a person's propensity to see things from a specific point of view. This viewpoint makes it impossible for the person to remain unbiased and objective. Numerous cybersecurity concerns have been found to be caused by cognitive biases [19] [20]. Decision-making is impacted by cognitive bias which is a mistake in thinking. Studies on the subject reveal that in order to successfully exploit a system, attackers target cognitive biases in addition to technical weaknesses [19] [20] [21].

An analyst or investigator may focus incorrectly on a person during investigation because of their affiliation with a certain group for example, a highly technical person with extensive access rights or admin, rather than the facts or forensic data that appropriately define the person and their conduct in a security inquiry. Focusing on a specific person as a result of an incorrect application of characteristics might cause investigators to look for evidence to back up their presumptions and postpone finding the real cause of security problems, which can have an impact on security [21].

2.2. Optimism Bias (Illusion of Invulnerability)

It seems incredible that people purchase lottery tickets given the extremely slim possibilities of winning. Despite evidence to the contrary, many people purchase tickets because they feel they will perform better than most other participants in the same activity.

Optimistic bias, also referred to as social comparison bias, reflects the difference between perceived risk to oneself and to a selected other or generally to others [12] [17]. Coined by Weinstein (1980), the term optimistic bias describes the cognitive bias individuals exhibit when they compare themselves to others

and perceive the risk of negative events happening to them as lower than the risk of negative events happening to the selected target.

Overestimating the likelihood of positive events and underestimating the likelihood of undesired events are just a few examples of how this optimism bias manifests itself [13] [21] [22].

The consequences of optimism bias include that users may believe they are immune to cyberattacks even when others have been demonstrated to be vulnerable because these people underestimate the risk. For instance, optimism bias could make spear phishing possible in which the attackers impersonate himself or herself as a trusted person and the messages seeming to come from that trusted source, trying to gain unauthorized access to data in a particular organization. Additionally, optimism bias might lead people to disregard preventative actions like patching or installing anti-virus because they believe they won't be impacted [13] [22].

People who deal with cybercrime are at a psychological disadvantage [23]. In cases where privacy is at stake, they are frequently given insufficient information to make the best decisions [23]. Estimates of the risk-versus-payoff parameters that are calculated under this constrained rationality are biased. However, even when there is enough information available, people are prone to hyperbolic discounting and assign lower risk estimates to security related decisions because they are motivated by the possibility of receiving instant pleasure and are affected by optimism bias [23]. This is same for organizations as well. Contrary to the breaches of other organizations, unaware management dwell their heads in sand and remain optimistic that this can't be happen to them or adopting 'seats of the pants' approach [24]. This thinking and approach are a serious threat to the organizational cyber security culture and cyber resilience [24].

Even though they have the best of intentions, analysts risk wasting a lot of time by focusing their search on causes or problems that support their own hypotheses or insights rather than those that are more general or less personal or real based on facts and figures and analysis. For seasoned analysts who might "decide" what happened before analyzing an incident, this is especially important. Although extremely helpful, their knowledge and experience may be a hindrance if they just look at incidents to confirm their preconceived notions. For example, if a manager is not believing on the theory that air gap can also be breached, then how can he invest on it? Thus, causing serious security issues.

Rhee *et al.*, performed a survey for assessing the impacts of optimism bias and illusion of control in the context of information security. The authors found that the more aware the staff or managers are, the more they are optimistically biased, and they have wrong illusion of control on the information security. The aware employees are more optimistically biased that negative cyber events or incidents will occur to others instead of them and they will inappropriately perceive cyber risk which will lead to a gap in the cyber domain [25].

Hewitt & White studied the optimistic bias of the users and its impacts on the

security incidents on the home computers. The authors surveys college and university students and lead to the findings that those students which are surer they will be a target of cyber attack but doesn't care much about by optimism that it will not be serious or doesn't consider them serious will then visit more untrusted sites and will experience security incidents [26]. In another study by the same authors, they lead to a very different result which states that cyber optimist bias has a positive effect on the perception of security measures against them. In other words, the employees who will have more awareness and will have optimistic bias towards cyber incidents, they will put more controls and then they will be optimistic that I will not be a target and if I will be a target, the preventive measures will save me [27].

Phishing is a serious cyber security threat and unaware employees or individual having optimism bias are mostly fall victim to the phishing attacks. Lei *et al.*, studied the precautions taken against phishing attacks and the role of optimism bias. The authors found that although individuals who are more aware of the phishing risks and threats are positive in implementing the behaviors and precautionary measures against phishing, but the optimism bias weakens this phenomenon. Having optimism bias, the individuals then consider themselves invulnerable which thus weakens their decision in opting precautions or taking care [28].

Chen & Yuan, 2022 adopted protection motivation theory to study the intentions of employees to cope with information security treats based on awareness of the threats and coping appraisals. The authors collected data from 356 Chinese respondents and analyzed through Structure equation modelling (SEM). The authors found that optimism bias led to lower perception of information security risks although the lack of knowledge of those risks does not significantly affect the perceived threat [29].

Mostly the literature found the negative impact of optimism bias on the adopting of preventive measures, inappropriate cyber risk perception and threat appraisal but some researchers have pointed positive impacts of optimism bias. Therefore, it is crucial to conduct a meta-analysis to find a collective effect of cyber optimism or cyber optimistic bias and its impacts on individuals risk perception and cyber security. In the next section, the research model for the impacts of optimism bias on the attitudes of the employees in the form of inappropriate risk perception, not adopting preventive measures, ignoring incidents, security overconfidence has been presented.

3. Research Model

Information technology and information systems are embedded in almost all aspects of daily operations within today's organizations, and dependence on the Internet is increasing daily [30]. The pervasive presence and dependence on information systems intensifies the importance of information security as system risks are directly linked to business risks [31]. This link is recognized and dem-

onstrated by the increase in resources spent annually to protect organizational information systems [31]. By 2025, the cybercrime damage is predicted to hit $10.5 trillion annually, global cyber security spending will exceed $1.75 trillion cumulatively from 2021 to 2025 and the cyber insurance market has been predicted to touch $14.8 billion annually [5].

From literature, it is clear that the humans are the weakest link and almost 82% of cyber breaches are attributed to humans. One of the main causes is the wrong perception of risks and lack in adopting of preventive measures against the cyber risks and threats due to optimism bias and wrong risk perception. It is hypothesized that cyber optimistic bias leads to inappropriate cyber risk perception that will results in decrease of overall cyber security through lack of adopting preventive measures, ignore security incidents, sharing passwords, wrong perception of cyber threats and overconfidence on themselves.

The following figure (**Figure 1**) presents the research model for this meta-analysis. Overall, there is only one hypothesis in this study as the lack of adopting preventive measures, ignore security incidents, sharing passwords, wrong perception of cyber threats and overconfidence on themselves are considered as an outcome due to inappropriate cyber risk perception.

This research will show how people who have an optimistic bias concerning cyber incidents are more victims than those who are not biased. Therefore, the following hypothesis has been formulated.

H1: *Optimism bias has negative influence on cyber security implying that individuals who have some bias perceives risk inappropriately which thus affects their attitude for taking rational decision and adopting more effective solutions or preventive measures for cyber security.*

4. Methodology

PRISMA methodology was adopted for systematic review and analysis which

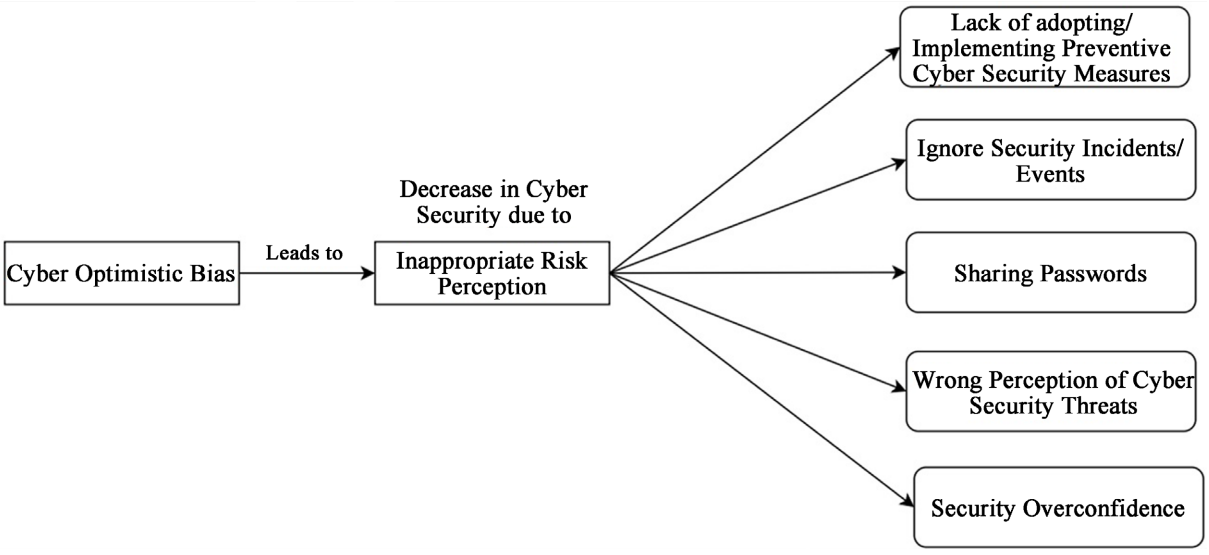

Figure 1. Research model for assessing cyber optimism/ optimistic bias.

stand for Preferred Reporting Items for Systematic Reviews and Meta-Analyses, and it comprises of following four stages *i.e.*, identification, screening, eligibility, and inclusion. Some benefits of using the PRISMA method include, improved transparency and clarity of reporting, which allows for easier replication and evaluation of the review; increased consistency in reporting across different studies and fields, which facilitates comparison and synthesis of findings; enhanced ability to identify and address potential biases and limitations in the review; greater accountability and credibility of the review, as it demonstrates that the review team has followed established best practices for conducting and reporting systematic reviews and meta-analyses [32]. Keyword searching using specific keywords or combinations of keywords to identify relevant articles in online databases, Boolean searching with AND, OR, NOT operators, Citation searching and hand searching that involves manually reviewing the reference lists of relevant articles and other sources (such as conference proceedings) to identify additional articles that may not be captured by database searches, were performed in this review. In this study research articles were searched through different online databases such as Google Scholar, IEEE Explorer, Research Gate, Science Direct and Springer published during 2000 to 2022 using different keywords. The search criteria included combination of keywords for searching such as "optimistic bias" OR "biases" OR "overconfidence" OR "behavior influencing" OR "optimism biases" with "information security" and "cyber security". The below PRISMA flowchart (**Figure 2**) shows the process of articles selection in this study.

Initially 945 articles were identified by searching keywords in online research databases and 35 papers through other sources and expert recommendations. 65 duplicate records were removed which were matching bibliographic information and duplicate information. 915 records were identified for screening. 880 publications were excluded from the study during the abstract level screening process. Full text screening was conducted for the remaining 35 articles with inclusion/exclusion criteria. Eligibility of these studies were assessed at this stage, in which 26 articles were excluded and 9 articles were finally included for meta-analysis after quality assessment to find the impact of optimistic bias on cyber security. The final selection papers were limited to those articles which had relation with optimistic bias in cyber security thus publications with most relevant information were selected for final meta-analysis.

Quantitative results of nine research empirical studies have been synthesized in this paper. Out of these studies 5 studies were carried out in USA, two in UK, one in Nigeria and one in Germany. Hypothesis relevant to the optimistic bias were selected from each article and used in the meta-analysis. The following table (**Table 1**) depicts the paper, sample size, relevant hypothesis, test type, test value and the r value obtained based on test statistics.

Results in these papers were not in the same effect size and scale. Two papers were showing correlation, five papers have beta correlation, one paper has F test,

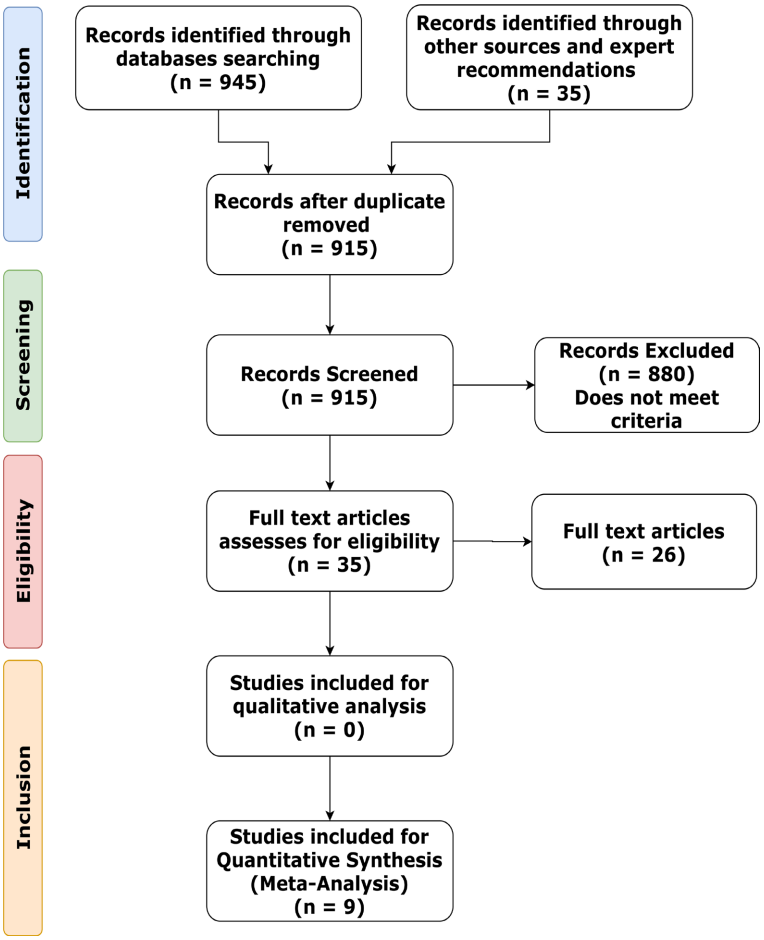

Figure 2. PRISMA flowchart.

Table 1. Studies included in meta-analysis.

Sr. No	Author, Year	Sample Size	Test Type	Test Statistic	p-value	r
1	[1] Rhee *et al.*, 2005	248	Correlation	0.561	0.000	0.561
2	[26] Hewitt & White, 2020	234	Correlation	0.148	0.024	0.148
3	[27] Hewitt & White, 2021	616	Beta coefficient	0.100	0.01	0.148
4	[28] Lei *et al.*, 2022	196	Beta coefficient	−0.204	0.009	−0.19992
5	[33] White *et al.*, 2016	945	Beta coefficient	0.42	0.01	0.4616
6	[34] Whitty *et al.*, 2015	630	Beta coefficient	0.18	0.08	0.2264
7	[35] Marek, 2015	116	F−Test	0.474	0.493	0.06377
8	[36] Williams et. al., 2019	370	Beta coefficient	0.217	0.05	0.26266
9	[37] Ament, 2017	239	T−Test	1.23	0.22	0.0796

and one has T test. According to Hak *et al.* (2016) the effect size should be in same scale across all the studies included in the Meta Analysis to compare them [39]. Therefore, the result of beta coefficient, F Test and T test were converted to R (Correlation) using the Practical Meta-Analysis Effect Size Calculator [40].

5. Meta-Analysis and Result

The meta-analysis calculation was done in the Comprehensive Meta Analysis (MCA). The random effect model was used for analysis in this studying and included nine studies using correlation as index of effect size. It is assumed that random samples were taken in all the studies [41] [42] [43]. Fisher's Z values were estimated to make sure that the variance of effect size or magnitude of effect is based on sample size. The upper and lower bound limits of 95% confident interval were used to measure the effectiveness of the study. P-value was used to test the null hypothesis and the value below 0.05 is considered as significant. The result of Meta-analysis is shown in the below figure (**Figure 3**).

The analysis shows mean effect size, or the summary effect size is 0.351 with a 95% confidence interval of 0.079 to 0.574. This shows the optimistic bias has relatively more effect on the cyber security. The effect size comparable studies can be anywhere in this interval. The Z-value is 2.500 with $p = 0.012$. Using a criterion alpha of 0.050. The Z-value tests the null hypothesis that the mean effect size is zero. Hence the null hypothesis is rejected, and it is concluded that mean effect size is not precisely zero in the populations of comparable studies included in the analysis. In the random effect model, actual effect size can vary among studies. Q-test is performed to check the heterogeneity among the studies and test the null hypothesis to see the sharing of common effect size. If the Q is equal to the degree of freedom, it is concluded that all studies share same true effect size. The criterion alpha for the Q-test is typically set at 0.100. The following table (**Table 2**) show heterogeneity statistics.

The Q-value of this study is 576.988 with 8 degrees of freedom and $p < 0.001$.

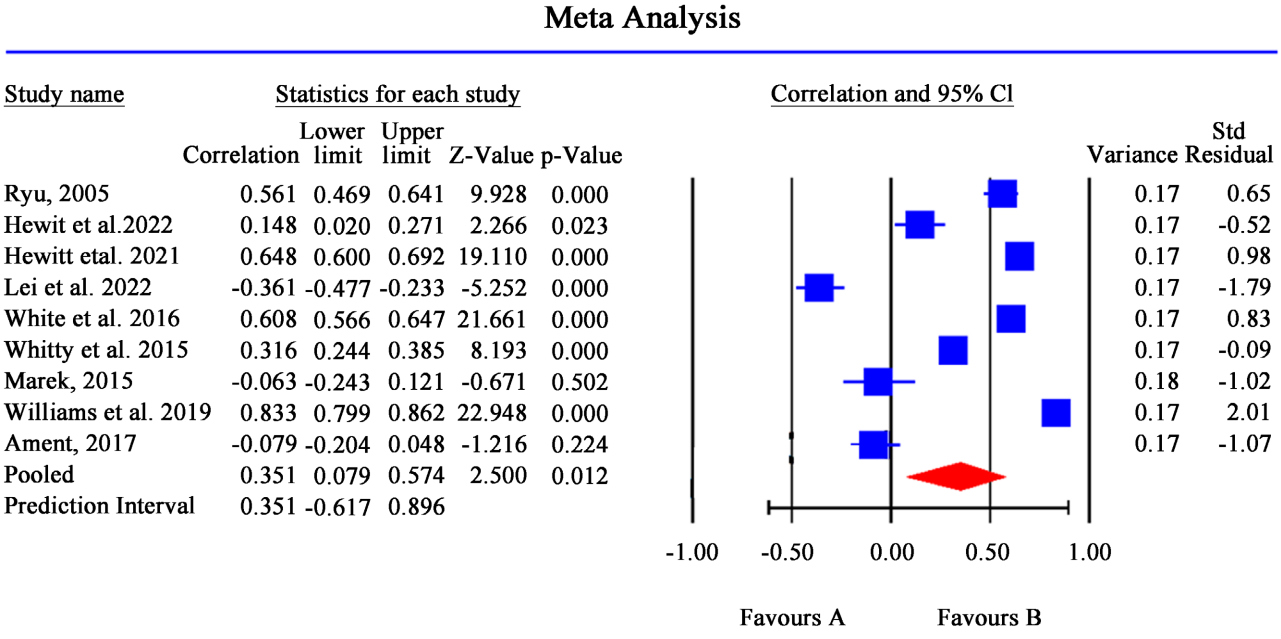

Figure 3. Meta analysis of optimistic/optimism bias in cyber security.

Table 2. Heterogeneity statistics.

Number Studies	Effect Size and 95% Interval			Tau	Tau^2	Heterogeneity statistics			
	Point estimate	Lower limit	Upper limit			Q-Value	df (Q)	P-value	I^2
9	0.351	0.079	0.574	0.435	0.189	576.988	8	0.000	98.613

Using a criterion alpha of 0.100 the null hypothesis of homogeneity is rejected, and it is proved that the true effect size varies in these studies, and it has high variability. The Q values or the associated p-value just tell if there is any variation or not, but it does not tell the size of variation. How much the effect size vary, can be found through prediction interval I-square (I^2) which tell how much the effect size varies across studies. I^2 is 99% which shows 99% variance in the true effect size. The remaining 1% can be sampling error. Similarly, the Tau-squared (Tau2) indicates the variance of true effect sizes which is 0.189 in Fisher's Z units. Tau, the standard deviation of true effect sizes, is 0.435 in Fisher's Z units in this study. If it is assumed that the true effects are normally distributed (in Fisher's Z units), it can be estimated that the prediction interval is −0.617 to 0.896. The true effect size in 95% of all comparable samples falls in this interval [44] [45] [46] [47].

Egger Regression Test was conducted to check the publication bias using funnel plot asymmetry. The value of intersection (B0) is -14.55679, 95% confidence interval (−33.68383, 4.57026), with t=1.79962, df = 7. The 1-tailed p-value (recommended) is 0.05747, and the 2-tailed p-value is 0.11495. The p-value is not significance in both tails which indicate there is no publication bias. Furthermore, the standard error is 8.0883 which close to the line of regression or degree of freedom (df) which reassure that there is no publication bias. Begg and Mazumdar rank correlation shows P-value (1-tailed) is 0.03817 and P-value (2-tailed) is 0.07633 which means no publication bias exists.

The funnel plot is graphical representation used to assess the publication bias. The following funnel plot (**Figure 4**) of this study also confirms variability in publications as it is asymmetric and most of studies are outside of the funnel.

In the absence of publication bias it would be expected the studies to be distributed symmetrically about the combined effect size. By contrast, in the presence of bias, we would expect that the bottom of the plot would show a higher concentration of studies on one side of the mean than the other.

6. Discussion

The results of this meta-analysis have been based on 9 studies available and fulfilled the criteria of the meta-analysis. For these studies sufficient empirical data existed which can be used to infer meta-analysis and calculate effect size.

All the research included in the meta-analysis selected cyber optimism bias or optimistic bias as an independent variable and cyber risk perception and adopting of preventive measures as dependent variable. Although the wordings were

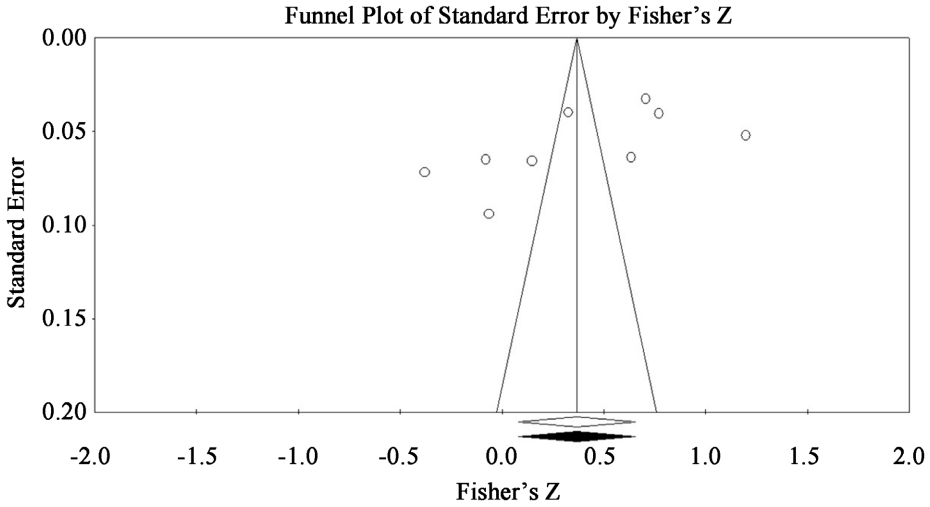

Figure 4. Assessing publication bias through funnel test.

different, but the theme of the dependent and independent variables were the same. The factors like share passwords by considering it will not be maliciously used, lacks adopting of preventive measures, ignore security incidents, wrong perception of cyber threats and overconfidence on themselves in the context of cyber security are the outcomes after wrong perception of risks or threats and illusion of control on the information risks and threats. Therefore, only one hypothesis has been formulated.

The purpose of the meta-analysis was to understand the impact of optimism bias on human perception about cyber security. There is strong correlation between the optimistic bias and the human risk perception which is a potential factor which impact the cyber security. Incorrect cyber risk perception leads to thinking that the individual has preventive measures, or the risk is low, not very serious and I will not be a target. Ament (2017) stated that optimism bias will lead to overconfidence on the skills of the individual as well as create a thinking that I will not be a target thus will not opt preventive measures due to that overconfidence and optimism bias [37] Cho *et al.*, 2010 [38] and Chen & Yuan, 2022 [29]. Overconfidence and optimism bias will affect the decision making of the individual both in personal context as well as in organizational context [29] [38].

The results of the meta-analysis confirms that cyber optimism bias impacts the perception of cyber risks and that incorrect or wrong perception of threats and risks will impact the decision and the individual will involve in risk behaviors and actions like sharing of passwords by considering it will not be maliciously used, lack adopting of preventive measures, ignore security incidents, wrong perception of cyber threats and overconfidence on himself or herself in the context of cyber security. These results are consistent with the results of most of the individual studies of optimistic bias in the context of cyber security. Chen & Yuan, in a recent study found that due to optimistic bias, the decisions of the analysts will not be objective and will be biased and flawed [29].

The study of meta-analysis is consistent with the literature showing a relationship between optimism bias of human perception and cyber security. The optimistic bias has adverse impact on the cyber security due to wrong perception of cyber threats and risks.

7. Research Implications and Significance

The research has both theoretical and practical implications. Theoretically the meta-analysis is first of its kind on this topic and subject. Although the optimism bias has very serious impact on cyber security risks perception, overall risks, and assessment but there were very limited and dispersed studies available. This meta-analysis combined all the studies and provided a combined effect size that confirms that optimism bias will lead to inappropriate risk perception which will results in wrong or subjective decisions that will lack objectivity.

Practically, the research provide insight to the organizational management that while deciding on the cyber security matters, perceived risks, and vulnerabilities, they should be objective and unbiased. The organizational management like CISOs must aware employees of this bias by stating that although the individuals doesn't think that are biased but in reality, they are. Therefore, the workforce must follow the instructions given to them by the security teams from time to time and comply with the cyber security policies and requirements. Realization of this bias by an individual at the individual level or by an organization at the organizational or team level is the first step for its mitigation.

Furthermore, this research has significance in many ways. Meta-analysis in studying optimism bias in cyber security lies in its ability to provide a comprehensive and robust examination of the phenomenon across multiple studies. By pooling data from multiple studies, this meta-analysis has provided a more precise estimate of the true effect size of optimism bias, which can help to identify the magnitude and scope of the problem.

This meta-analysis provided a comprehensive and robust examination of the phenomenon across multiple studies. It provided a precise estimate of the true effect size, identify moderating factors, and guide future research. The overall significance of this research is that it can help organizations and individuals to better understand and mitigate the risks associated with optimism bias, which can lead to more effective cyber security practices and a reduction in the number of security breaches.

8. Conclusions and Future Research Directions

Cyber security is dependent on the decision of human beings which are the operators and administrators of the systems, and they are considered the major cause of cyber breaches. While doing cyber security decisions and assessing risks, the assessors must be objective and not biased. But unfortunately, research stated that at times the individuals at any capacity dealing with the systems and risks, perceive the risks inappropriately due to a thinking that "I/we am (are) not

vulnerable or overconfident on the security measures or think that I will not be a target". This is optimistic bias. Due to this thinking, the perceived risk is flawed, and the decisions are not objective. This meta-analysis was conducted by combining all the available studies which were fulfilling the criteria of meta-analysis about optimism bias in the cyber security context. The results of the meta-analysis found that optimism bias has a huge impact on the overall cyber insecurity due to the inappropriate risk perceptions. Administrators, analysis, investigators, and operators/users should be very objective while considering the cyber related events, risks, threats and incidents. Otherwise, research states that people with optimistic bias in the cyber security context are more targeted than others which is contrary to the thinking of people having optimistic bias.

There are several directions that future research on optimism bias and its impact on cyber security could take:

Longitudinal studies: Longitudinal studies that track the development and evolution of optimism bias over time could provide a more detailed understanding of how optimism bias arises and how it changes over time. This could help to identify the factors that contribute to optimism bias and to develop interventions that are more effective at reducing the risk of security breaches. **Interventions**: Research on interventions that aim to reduce the risk of security breaches by reducing optimism bias could be valuable. This could include studies that test the effectiveness of different types of interventions, such as training programs, awareness campaigns, and other types of educational initiatives. **Cultural studies**: Research on the cultural factors that influence optimism bias could provide insights into how different cultures approach cyber security and how this affects their level of optimism bias. **Comparative studies**: Comparative studies that examine the level of optimism bias in different countries or regions could provide insights into how optimism bias varies across different cultures and regions, and how it can be mitigated in these contexts. **Artificial Intelligence and Machine Learning**: With the increasing use of AI and Machine Learning in cyber security, future research could focus on how these technologies can be used to detect and mitigate optimism bias. **Human and Organizational Factors**: Studies that focus on the human and organizational factors that contribute to optimism bias, such as decision-making processes, communication patterns, and organizational culture, could provide valuable insights into how to mitigate the risks associated with optimism bias.

Overall, future research on optimism bias and its impact on cyber security should aim to provide a more detailed and comprehensive understanding of the phenomenon, and to develop effective interventions that can reduce the risk of security breaches.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Tsagourias, N. and Farrell, M. (2020). Cyber Attribution: Technical and Legal Approaches and Challenges. *European Journal of International Law*, **31**, 941-967. https://doi.org/10.1093/ejil/chaa057

[2] Rundle, J. (2022, October 5) Rise in Cyberattacks Stretches and Stresses Defenders. *Wall Street Journal*. https://www.wsj.com/articles/rise-in-cyberattacks-stretches-and-stresses-defenders-11664962202

[3] Sayegh, E. (2022, December 15) Top Cybersecurity Predictions 2023. *Forbes*. https://www.forbes.com/sites/emilsayegh/2022/12/15/top-cybersecurity-predictions-2023

[4] Hughes-Lartey, K., Li, M., Botchey, F.E. and Qin, Z. (2021) Human Factor, a Critical Weak Point in the Information Security of an Organization's Internet of Things. *Heliyon*, **7**, e06522. https://doi.org/10.1016/j.heliyon.2021.e06522

[5] Morgan, S. (2022, December 12) Top 10 Cybersecurity Predictions and Statistics for 2023. *Cybercrime Magazine*. https://cybersecurityventures.com/stats

[6] Morgan, S. (2021, January 21) 2021 Report: Cyberwarfare in the C-Suite—Cybercrime Facts and Statistics. *Cybercrime Magazine*. https://cybersecurityventures.com/wp-content/uploads/2021/01/Cyberwarfare-2021-Report.pdf

[7] Rahman, T., Rohan, R., Pal, D. and Kanthamanon, P. (2021) Human Factors in Cybersecurity: A Scoping Review. *The 12th International Conference on Advances in Information Technology*, Bangkok, June 2021, Article No. 5. https://doi.org/10.1145/3468784.3468789

[8] Verizon (2022) 2022 Data Breach Investigations Report. *Verizon Business*. https://www.verizon.com/business/resources/reports/dbir https://doi.org/10.12968/S1361-3723(22)70578-7

[9] Hadlington, L. (2021) The "Human Factor" in Cybersecurity: Exploring the Accidental Insider. In: *Research Anthology on Artificial Intelligence Applications in Security*, IGI Global, Hershey, 1960-1977. https://doi.org/10.4018/978-1-7998-7705-9.ch087

[10] Hadlington, L. (2017) Human Factors in Cybersecurity; Examining the Link between Internet Addiction, Impulsivity, Attitudes towards Cybersecurity, and Risky Cybersecurity Behaviours. *Heliyon*, **3**, e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

[11] Ray, S. (2022, September 20) Social Engineering: How a Teen Hacker Allegedly Managed to Breach both Uber and Rockstar Games. *Forbes*. https://www.forbes.com/sites/siladityaray/2022/09/20/social-engineering-how-a-teen-hacker-allegedly-managed-to-breach-both-uber-and-rockstar-games

[12] Weinstein, N.D. (1980) Unrealistic Optimism about Future Life Events. *Journal of Personality and Social Psychology*, **39**, 806-820. https://doi.org/10.1037/0022-3514.39.5.806

[13] Pfleeger, S.L. and Caputo, D.D. (2012) Leveraging Behavioral Science to Mitigate Cyber Security Risk. *Computers & Security*, **31**, 597-611. https://doi.org/10.1016/j.cose.2011.12.010

[14] Chapin, J.R. and Pierce, M. (2012) Optimistic Bias, Sexual Assault, and Fear. *The Journal of General Psychology*, **139**, 19-28. https://doi.org/10.1080/00221309.2011.635724

[15] Komatsu, A., Takagi, D. and Takemura, T. (2013) Human Aspects of Information Security. *Information Management & Computer Security*, **21**, 5-15. https://doi.org/10.1108/09685221311314383

[16] Gratian, M., Bandi, S., Cukier, M., Dykstra, J. and Ginther, A. (2018) Correlating Human Traits and Cyber Security Behavior Intentions. *Computers & Security*, **73**, 345-358. https://doi.org/10.1016/j.cose.2017.11.015

[17] Schwarzer, R. (1994) Optimism, Vulnerability, and Self-Beliefs as Health-Related Cognitions: A Systematic Overview. *Psychology & Health*, **9**, 161-180. https://doi.org/10.1080/08870449408407475

[18] Weinstein, N.D. and Klein, W.M. (1996) Unrealistic Optimism: Present and Future. *Journal of Social and Clinical Psychology*, **15**, 1-8. https://doi.org/10.1521/jscp.1996.15.1.1

[19] Jalali, M.S., Siegel, M. and Madnick, S. (2019) Decision-Making and Biases in Cybersecurity Capability Development: Evidence from a Simulation Game Experiment. *The Journal of Strategic Information Systems*, **28**, 66-82. https://doi.org/10.1016/j.jsis.2018.09.003

[20] Cunningham, M. (2020) Thinking about Thinking: Exploring Bias in Cybersecurity with Insights from Cognitive Science. https://www.forcepoint.com/sites/default/files/resources/files/report_thinking_about_thinking_cybersecurity_bias_en.pdf

[21] Parsons, K., Mccormac, A., Butavicius, M. and Ferguson, L. (2010) Human Factors and Information Security: Individual, Culture and Security Environment. https://apps.dtic.mil/sti/pdfs/ADA535944.pdf

[22] Rhee, H.-S., Ryu, Y.U. and Kim, C.-T. (2012) Unrealistic Optimism on Information Security Management. *Computers & Security*, **31**, 221-232. https://doi.org/10.1016/j.cose.2011.12.001

[23] Wiederhold, B.K. (2014) The Role of Psychology in Enhancing Cybersecurity. *Cyberpsychology, Behavior, and Social Networking*, **17**, 131-132. https://doi.org/10.1089/cyber.2014.1502

[24] Ross, R. (2022, January 1) More Assurance, Less Seat of the Pants. https://www.linkedin.com/pulse/new-years-resolution-more-assurance-less-seat-pants-ron-ross

[25] Rhee, H.-S., Ryu, Y.U. and Kim, C.-T. (2005) I Am Fine but You Are Not: Optimistic Bias and Illusion of Control on Information Security. *International Conference on Information Systems*, Las Vegas, 11-14 December 2005, 11-24.

[26] Hewitt, B. and White, G.L. (2020) Optimistic Bias and Exposure Affect Security Incidents on Home Computer. *Journal of Computer Information Systems*, **62**, 50-60. https://doi.org/10.1080/08874417.2019.1697860

[27] Hewitt, B. and White, G. (2021) Factors Influencing Security Incidents on Personal Computing Devices. *Journal of Organizational and End User Computing*, **33**, 185-208. https://doi.org/10.4018/JOEUC.20210701.oa9

[28] Lei, W., Hu, S. and Hsu, C. (2022) Unveiling the Process of Phishing Precautions Taking: The Moderating Role of Optimism Bias. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4147323

[29] Chen, H. and Yuan, Y. (2022) The Impact of Ignorance and Bias on Information Security Protection Motivation: A Case of e-Waste Handling. *Internet Research*. https://doi.org/10.1108/INTR-04-2022-0238

[30] Picincu, A. (2018) Role of Information Systems in an Organization. Bizfluent.

https://bizfluent.com/about-6525978-role-information-systems-organization.html

[31] Nosova, E., Anisimova, L., Murovana, T., Sviatiuk, Y. and Iafinovych, O. (2021) Information Security System in Provision of the Economic Security and Risk Management of the Enterprise. https://ceur-ws.org/Vol-3188/paper3.pdf

[32] Stewart, L.A., Clarke, M., Rovers, M., Riley, R.D., Simmonds, M., Stewart, G. and Tierney, J.F. (2015) Preferred Reporting Items for a Systematic Review and Meta-analysis of Individual Participant Data. *JAMA*, **313**, 1657. https://doi.org/10.1001/jama.2015.3656

[33] White, G., Ekin, T. and Visinescu, L. (2016) Analysis of Protective Behavior and Security Incidents for Home Computers. *Journal of Computer Information Systems*, **57**, 353-363. https://doi.org/10.1080/08874417.2016.1232991

[34] Whitty, M., Doodson, J., Creese, S. and Hodges, D. (2015) Individual Differences in Cyber Security Behaviors: An Examination of Who Is Sharing Passwords. *Cyberpsychology, Behavior, and Social Networking*, **18**, 3-7. https://doi.org/10.1089/cyber.2014.0179

[35] Marek, J.M. (2015) Presence of Optimistic Bias and Illusion of Control in Information Security Risk Perceptions. https://www.proquest.com/openview/488e1f743c01c2f6bdfdf4d6c839154d/1?pq-origsite=gscholar&cbl=18750

[36] Williams, A., *et al*. (2019) Employee Behavioural Factors and Information Security Standard Compliance in Nigeria Banks. *International Journal of Computing and Digital Systems*, **8**, 387-396. https://doi.org/10.12785/ijcds/080407

[37] Ament, C. (2017) The Ubiquitous Security Expert: Overconfidence in Information Security. Semantic Scholar.

[38] Chung, S. (2010) Optimistic Bias about Online Privacy Risks: Testing the Moderating Effects of Perceived Controllability and Prior Experience. *Computers in Human Behavior*, **26**, 987-995. https://doi.org/10.1016/j.chb.2010.02.012

[39] Hak, T., van Rhee, H. and Suurmond, R. (2016) How to Interpret Results of Meta-Analysis. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3241367

[40] Wilson, D. B. (2019) Practical Meta-Analysis Effect Size Calculator. https://www.campbellcollaboration.org/escalc/html/EffectSizeCalculator-Home.php

[41] Borenstein, M., Hedges, L.V., Higgins, J.P. and Rothstein, H.R. (2010) A Basic Introduction to Fixed-Effect and Random-Effects Models for Meta-Analysis. *Research Synthesis Methods*, **1**, 97-111. https://doi.org/10.1002/jrsm.12

[42] Borenstein, M., Hedges, L.V., Higgins, J.P.T. and Rothstein, H.R. (2021) Introduction to Meta-Analysis. Second Edition, Wiley, Hoboken. https://doi.org/10.1002/9781119558378

[43] Hedges, L.V. and Vevea, J.L. (1998) Fixed and Random-Effects Models in Meta-Analysis. *Psychological Methods*, **3**, 486-504. https://doi.org/10.1037/1082-989X.3.4.486

[44] Borenstein, M., Hedges, L.E., Higgins, J.P.T. and Rothstein, H.R. (2022) Comprehensive Meta-Analysis Version 4. Biostat, Inc., Tampa. https://www.Meta-Analysis.com

[45] Borenstein, M., Higgins, J.P., Hedges, L.V. and Rothstein, H.R. (2017) Basics of Meta-Analysis: I2 Is Not an Absolute Measure of Heterogeneity. *Research Synthesis Methods*, **8**, 5-18. https://doi.org/10.1002/jrsm.1230

[46] Higgins, J.P.T. and Thomas, J. (2019) Cochrane Handbook for Systematic Reviews of Interventions. 2nd Edition, Wiley, Hoboken.

https://doi.org/10.1002/9781119536604

[47] IntHout, J., Ioannidis, J.P.A., Rovers, M.M. and Goeman, J.J. (2016) Plea for Routinely Presenting Prediction Intervals in Meta-Analysis. *BMJ Open*, **6**, e010247. https://doi.org/10.1136/bmjopen-2015-010247