


Same or Not the Same? Comparison Between Employees Prone to Overplacement, Overestimation, and Overprecision in Information Security

Muriel Frank 
Goethe University Frankfurt &
SnT - Interdisciplinary Centre for
Security, Reliability and Trust,
University of Luxembourg
muriel.frank@uni.lu

Mara Wacker
Goethe University Frankfurt
mara.w@cker-online.de

Lukas Manuel Ranft
Goethe University Frankfurt
lrnft@wiwi.uni-frankfurt.de

Abstract

Overconfidence has been shown to have a detrimental effect on information security in enterprises. However, research on this systematic misperception of one's abilities and skills is fragmented, and evidence on who is at risk of overconfidence is scarce. Using a cluster analysis in conjunction with a large-scale survey of 2,867 employees of a pharmaceutical company, we examine information security overconfidence and identify commonalities between risk groups. Our findings help raise awareness and understanding of this widespread phenomenon and can help design appropriate interventions.

Keywords: Information security overconfidence, overestimation, overprecision, overplacement, cluster analysis.

1. Introduction

It is widely recognized that the human factor plays an essential role in safeguarding corporate assets. Problems, however, can arise if employees place too much confidence in their security knowledge, their ability to detect phishing emails, and how to handle security risks (Ament & Jaeger, 2017; Wang et al., 2016). This kind of behavior, generally referred to as overconfidence, can lead to risky (mis)behavior, which can cause security incidents. To illustrate the problem being raised, employees act carelessly when protecting their computers because they are optimistic that they will never experience a security breach (Hewitt & White, 2020). Individuals may also overestimate their phishing detection capabilities, resulting in missing important cues of deception and disclosure of sensitive information (Wang et al., 2016).

While overconfidence has been increasingly studied in recent decades in fields like psychology (e.g., Moore et al., 2018) and finance (e.g., Huang & Kisgen, 2013), research on overconfidence in information

security is still sparse. Existing work on overconfidence in information security has shown that individuals can suffer from three distinct manifestations of overconfidence (Ament, 2017). The first one is called overestimation, which refers to people's inability to assess their own capabilities (Prims & Moore, 2017). Next is overprecision which builds on overestimation and occurs when people are too confident that they are correctly assessing their performance. Finally, there is overplacement, which occurs when individuals think they are doing better than others, even when they are not (Ament, 2017).

Although each manifestation is distinct, researchers tend to study only some of these manifestations, not all. The only exception to this is Ranft (2022) who examined the effect of individual's professional environment on all three manifestations of overconfidence. Hence, what is lacking in the existing literature is an understanding of whether there are similarities or differences between employees who exhibit different types of overconfidence. This seems valuable for two main reasons: First, it helps to identify employees with large security knowledge gaps and unravel the accuracy of security self-assessments to understand where to install better security measures. Second, a better understanding of this phenomenon can lead to lower costs and security investments (Ament, 2017). Therefore, our research question is as follows:

What are the similarities and differences between employees who exhibit different types of overconfidence in information security?

To the best of our knowledge, no research has explicitly addressed the extent to which employees who exhibit overestimation, overprecision, and overplacement differ or share similarities. Therefore, our work will complement existing research by extending our understanding of this cognitive bias. Furthermore, it will demonstrate that security quizzes in combination with self-assessments are useful tools for measuring security overconfidence in an organizational

context. In addition, our findings will help to better target interventions to at-risk groups.

The remaining sections of this paper are organized as follows: The next section discusses all pertinent academic findings on overconfidence, especially information security overconfidence, relevant to understanding our research approach and findings. Section 3 presents the methodology, including information on the design, sample characteristics, and data collection procedure. It also presents the descriptive results of the cluster analysis, which are then discussed in Section 4 in terms of their practical and theoretical implications. Section 5 summarizes the main findings of the study.

2. Related work

Overconfidence is one of the most important findings in the psychology of judgment and decision-making (De Bondt & Thaler, 1995). According to Kruger and Dunning (1999), overconfidence refers to a systematic misjudgment of skills and competencies, which means that people cannot correctly assess their abilities in various social and intellectual tasks. As mentioned above, overconfidence can manifest itself in three different ways: overestimation, overprecision, and overplacement (Moore & Healy, 2008). The first of these manifestations, overestimation, describes the tendency of individuals to systematically overestimate their own abilities and their own chances of success. For example, in the context of information security, overestimation occurs when individuals are unrealistically confident about their ability to defend against phishing attacks (Wang et al., 2016). Overprecision builds on overestimation and refers to an individual's excessive certainty in their beliefs (Moore & Healy, 2008). To give an example in the field of information security, employees are too confident in knowing a particular answer with regard to information security risks and threats and therefore choose a confidence interval that is too narrow (Ament, 2017). The third manifestation of overconfidence, overplacement, focuses on one's relative overconfidence compared to others (Moore & Healy, 2008). In the field of information security, for example, people may mistakenly think that they know more about security than their peers, when this is not the case (Ranft, 2022).

Over the past six decades, researchers have studied overconfidence from different angles and in different disciplines, from finance (e.g., Huang & Kisgen, 2013) and management (e.g., Billett & Qian, 2008) to marketing (e.g., Lewis, 2018) and politics (e.g., Ortoleva & Snowberg, 2015). Research on this cognitive bias in information security is still relatively

new but is gaining attention. One of the reasons is that overconfidence in information security often has detrimental consequences for business and personal lives (Frank et al., 2023). Researchers repeatedly show that overconfidence clouds one's ability to detect malicious emails (Canfield et al., 2019; Lawson et al., 2020; Wang et al., 2016) and assess the extent to which one's behavior could pose a security risk (Howah & Chugh, 2019). As a result, scholars have recently begun investigating the antecedents of overconfidence, as well as the characteristics of overconfident employees. For example, Frank et al. (2023) find that several traits such as training commitment, age, job level, and help desk reliance determine whether or not individuals are prone to overconfidence. However, to date, there has been no explicit research on the three manifestations, particularly in terms of differences or similarities between those who exhibit overestimation, overprecision, or overplacement. Only Ranft (2022) focuses on the professional environment and its influence on overestimation, overprecision, and overplacement. Therefore, we seek to close this gap and expand our understanding of overconfidence in information security.

3. Methodological approach

To better understand the phenomenon of overconfidence, we followed a two-step approach. In a first step, we surveyed 3,581 employees of an international pharmaceutical company with the aim of determining their level of overconfidence (broken down by overestimation, overprecision, and overplacement). In a second step, we used cluster analysis to detect patterns in the data (Halkidi et al., 2001) and identify individuals at risk of being unaware of security risks and overconfident in their knowledge of security threats and how to handle security incidents.

3.1. Research design and data collection

In this section, we provide an overview of the research design and data collection procedure. To capture the level of overconfidence of the employees, we relied on the approach of Frank et al. (2023) and used their security quiz with 20 questions on security-related topics. Using quizzes in combination with self-assessments is a valid approach to assess overconfidence in information security (see, e.g., Aggarwal et al., 2015; Frank et al., 2023; Ranft, 2022). The questions revolved around security risks and threats, device update behavior, and security incident responses. For example, one of the questions was: "Which of the following answers can turn a trusted employee into a malicious insider?" with the answer a)

frustration, b) financial problems, c) stress and d) all answers given are correct. As part of the questionnaire, participants also had to do a self-assessment of their performance. Firstly, they were asked to estimate how many of the questions they were likely to answer correctly (a number from 0 to 20). Second, they indicated how confident they were in their self-assessment. The confidence range was between 50% (guessing) and 100% (completely confident). Finally, participants compared themselves with their colleagues and assigned themselves a hypothetical rank between 1 (no one else has a better score) and 100 (no one else has a worse score).

Although the majority of studies on information security overconfidence have looked at American (e.g., Wang et al., 2016) or Asian individuals (Dong et al., 2019; Hanamura et al., 2013), our focus is on European employees. The reason for this is that previous findings from other disciplines suggest that overconfidence is also high in Europe (see, e.g., Friehe & Pannenberg (2019) or Stankov & Lee (2014)). This underlines the value of the current study for research. Within two weeks, all participants received an invitation to participate in the security study. They were informed that their participation was voluntary and that they were free to withdraw from the study at any time. To reduce common method bias, we included attention checks (Podsakoff et al., 2003). After the survey, we collected discrete contextual data on all participants. These data were anonymized before being processed by the authors. The selection of contextual data was not exhaustive (Johns, 2006) but served as an initial representation of task, social, and informational context variables thought to influence overconfidence (Frank et al. 2023, Ranft 2022). An overview of the selected variables is given in Table 6 in the Appendix.

3.2. Data cleaning and sample information

As we collected contextual data from various internal sources, we had to deal with missing and incomplete data. Missing values are usually a major problem for data mining endeavors, as they can lead to difficulties in performing analyses and affect the accuracy and validity of the test results (Alasadi & Bhaya, 2017). This makes data pre-processing a top priority. We scanned our data for missing values and discovered that attributes such as age, gender, or frequency of security training were missing for all external employees due to data minimization requirements. As a result, we removed them from the data set. For scatter data sets with missing values, we relied on data imputation, specifically k-nearest neighbor (k-NN). The k-NN algorithm, as a machine learning technique, is considered a particularly efficient

method to fill in missing values (Beretta & Santaniello, 2016). We also scanned our data sets for outliers and used logical reasoning to decide whether or not to make adjustments (Aguinis et al., 2013). Another point to consider is that our data consist of both categorical and numerical data, so we performed a dimensionality reduction using factor analysis for mixed data (FAMD) (Audigier et al., 2016).

After cleaning the data, a total of 2,867 out of the 3,581 collected data sets remained for analysis. As shown in Table 1, most participants are male (59.11%), on average 42.91 years old and have no managerial responsibilities. Interestingly, most participants show overestimation (52.49%). In fact, they expect to answer four more questions correctly than they actually do. Regarding overprecision, 24.03% of the participants are too precise when it comes to correctly assessing their security knowledge. Finally, about half of the participants (47.82%) tend to overplacement. In other words, they think they are better than they actually are compared to others.

Table 1. Sample characteristics

Gender		Team Leader	
Male	1,695 (59.12%)	Yes	431 (15.02%)
Female	1,172 (40.88%)	No	2,438 (84.98%)
Age (years)		42.91	
Job experience (years)		11.5	
		x_i	$E(x_i)$
Overestimation	1,505 (52.49%)	11.57	15.32
Overprecision	689 (24.03%)	66.54%	86.28%
Overplacement	1,371 (47.82%)	57.78	28.99

3.3. Cluster algorithm and cluster validation

For the actual cluster analysis, we relied on the k-means algorithm for mainly two reasons. First, the k-means is very easy to implement and, at the same time, very efficient, which is why it is often the method of choice for cluster analysis (Wu, 2012). Second, the k-means algorithm was identified as a suitable method for the analyses of the present work due to its particular suitability for clustering mixed data after prior reduction in dimensionality using FAMD (van de Velden et al., 2019). Generally, k-means aims to find k non-overlapping clusters (Wu, 2012), where the data points within a cluster are as similar as possible and as different as possible compared to other clusters (Jain, 2010). The parameter selection for the maximum iterations and the random initial configurations was 100. The SD validity

index was used to determine the optimal number of clusters for each overconfidence manifestation. This index, proposed by Halkidi et al. (2000), represents an approach to assessing the validity of clusters that takes into account both compactness and similarity. More generally, this index is defined based on the average dispersion within the clusters, as well as the total distance between the clusters (Halkidi et al., 2001). Table 2 presents the partitions based on the SD validity index, suggesting four clusters per overconfidence manifestation.

Table 2. Optimal numbers of clusters based on the SD validity index.

nc	Over-estimation	Over-precision	Over-placement
2	2.1390	2.2791	1.8734
3	1.6909	1.7490	1.5832
4	1.3721	1.4241	1.3312
5	1.4560	1.6745	1.4914
6	1.7948	1.8443	1.4687
7	1.8284	1.9090	1.7609
8	2.2181	2.1531	1.7541
9	2.1292	2.2845	1.7250
10	2.0447	2.2924	1.7775

3.4. Cluster interpretation

For interpretive purposes, we compared each cluster of excessively confident employees to the respective reference (non-overconfident) cluster. Chi-square tests were used to assess significance and Cramer's V was used to identify strong, medium, or small effect sizes (McHugh, 2013). Starting with overestimation, our results indicate four distinct clusters (see Table 3). The first cluster consists mainly of almost 90 percent men who show little interaction with the help desk (1,89 tickets per year), spend little time on security training, and need the most attempts to successfully complete such training compared to the other groups. With 52.6 years they are on average almost ten years older than the reference group and have an average work experience of 19 years. For this reason, we refer to this cluster as "Loyal Old-timers". Cluster 2 again includes significantly more men (71.6%). In contrast to the first cluster, however, these individuals are on average more than ten years younger than the reference group (32.7 years; SD: 7.7). Furthermore, employees in the second cluster earn the least, have been with the company the shortest (on average less than five years), and spend significantly less time on security training than the other groups. Thus, we term this cluster "Young Negligent". The third group consists of almost 91% women, of whom about 61% are working part-time. They tend to have no managerial responsibilities (97.3%), interact with the help desk frequently, and take the most time to

successfully complete security training sessions. Accordingly, we label this cluster "Committed Part-timers". The fourth and final cluster is characterized by a particularly high proportion of managers (78.9%) and the highest salary band. In addition, individuals have the highest average interaction with the IT help desk, with nearly ten tickets per year. They also work in the smallest teams (<7 employees). Consequently, we call this cluster "High Income Leaders".

Table 3. Clusters related to overestimation.

	Cluster size	Label	Significant attributes	Effect sizes
1	353	Loyal Old-timers	Males Age Job experience Help desk interaction No. of attempts	(+) (+++) (++) (-) (+)
2	549	Young Negligent	Age Salary band Job experience Time spent on training Team size	(---) (--) (--) (--) (+)
3	371	Committed Part-timers	Females Part-time Time spent on training	(++) (++) (+)
4	232	High Income Leaders	Salary band Leadership Team size Help desk interaction	(+++) (+++) (-) (++)

Regarding the second manifestation of overconfidence, overprecision, we again find four different clusters (see Table 4). The first cluster, "Loyal Old-timers", mainly contains men who are almost eleven years older and, with an average job experience of 21 years, have been with the company almost ten years longer than their colleagues in the reference group. They are generally more committed to completing security training because they spend comparatively more time conducting such training. However, this is accompanied by more attempts to successfully complete these training courses. The second cluster includes young employees who are in the lower pay grades. They have been with the company for about five and a half years and spend less effort (i.e., time) on security training sessions. For this reason, we label this cluster "Young Negligent". Cluster 3 is characterized by individuals who are in the higher pay grades while working in teams with no more than six colleagues. The majority of the cluster consists of managers with an average job experience of around eight years. Given this, we refer to this cluster as "High Income Leaders".

Table 4. Clusters related to overprecision.

	Cluster size	Label	Significant attributes	Effect sizes
1	144	Loyal old-timers	Males Age Job experience No. of training attempts	(+) (+++) (+++) (+)
2	283	Young negligent	Age Salary band Job experience Time spent on training Team size	(--) (--) (--) (--) (+)
3	118	High Income leaders	Salary band Leadership No. of training attempts Team size Help desk interaction	(+++) (+) (-) (--) (++)
4	144	Committed part-timers	Females Part-time No. of training attempts Time spent on training	(+) (+) (+) (++)

The last cluster, “Committed Part-timers”, includes women who spend the most time on security training. At the same time, they seem to have difficulties with successful completion, as they need more attempts than the reference group to successfully complete a training course.

Overplacement, the final manifestation of information security overconfidence, also has four different clusters (see Table 5).

Table 5. Clusters related to overplacement.

	Cluster size	Label	Significant attributes	Effect sizes
1	211	High Income Leaders	Salary band Leadership Team size Help desk interaction	(+++) (+++) (-) (+)
2	570	Young Negligent	Age Salary band Job experience Time spent on training Team size	(---) (-) (--) (--) (+)
3	285	Loyal Old-timers	Males Age Job experience	(+) (+++) (+++)
4	305	Committed Part-timers	Females Part-time Time spent on training	(++) (++) (+)

Starting with the first cluster, we find that more than 82% of the employees have management responsibilities. They earn the most compared to the other clusters and the reference group (6.41; SD: 2.16). They also make the most requests to the IT help desk. For this reason and in order to be consistent with similar clusters we have identified for the other two manifestations of overconfidence, we refer to this cluster as the "High Income Leaders". The second cluster is characterized by individuals who are young, work in large teams (14.9; SD: 26) and invest the least effort in security training but also need the fewest attempts for successful completion. Based on this, we term this cluster “Young Negligent”. A deeper look at the third cluster reveals that it consists mainly of men who are ten years older than their colleagues in the reference group. They are more committed to security training but need the most attempts to complete them successfully. For these reasons, we call this cluster “Loyal Old-timers”. Eventually, the fourth overplacement cluster is characterized by a very high proportion of women (almost 90%), most of whom work part-time. The individuals in this cluster have hardly any managerial responsibility, earn slightly less, and are on average around two and a half years older than those in the reference group. They also take the longest to complete security training. Therefore, we refer to this cluster as “Committed Part-timers”.

4. Discussion

Bearing in mind that the aim of the study was to uncover similarities and differences between individuals prone to one of the manifestations of overconfidence, we will now discuss our findings and their practical and theoretical implications. However, first, it is important to note that overconfidence appears to be a widespread phenomenon. Among the employees we surveyed, the likelihood of excessive self-confidence in their security knowledge and ability to manage threats and incidents was greater than 50%. Looking at the results of our cluster analysis, the most striking observation is that we detected roughly the same four clusters (with only minor variations) for each overconfidence manifestation. It seems that regardless of the type of overconfidence – be it overestimation, overprecision, or overplacement – there are four constant groups at risk.

To recall, the **first cluster**, which we have called “**Loyal Old-timers**”, mainly consists of older men with a lot of job experience (almost 20 years or more). They are usually reluctant to spend a lot of time calling the IT help desk for advice and need multiple attempts to successfully complete the security training. It appears that employee's assessments of their security knowledge

and skills become less accurate as they gain job experience. This contrasts with previous findings in other disciplines, which show that employees learn through experience and develop a more realistic assessment of their competencies and therefore engage in less risky behavior (Brozynski et al., 2004; Gervais & Odean, 2001). However, we also find studies that confirm our findings. Friehe & Pannenberg (2019), for example, find that full-time employees are more prone to overconfidence as they get older than those who are in their twenties.

Another aspect worth discussing is gender differences. According to Lundeberg et al. (1994), gender differences with respect to overconfidence are strongly dependent on the subject area studied. The authors show that men are more confident than women in certain domains, e.g., mathematics, while there are no gender differences in other domains. Although their study does not explicitly examine information security, it can be assumed that it can be considered more of a male-dominated domain (McGill & Thompson, 2018). Findings in the security realm suggest that gender affects at least overestimation and overprecision (e.g., Wang et al., 2016). Regarding age and especially seniority, Sebescen & Vitak (2017) find that the longer employees have worked for their organization, the greater the security risk. A possible explanation for this result is that seniority leads to increased self-confidence, which in turn leads them to act more carelessly. A final point to discuss with respect to the first cluster is the low interaction with help desks. In finance, for example, studies show that overconfident individuals are significantly less likely to seek professional advice (e.g., Lewis, 2018). According to Porto & Xiao (2016), overconfident individuals rarely or never seek advice because they believe that they have the necessary knowledge to overcome potential problems and challenges.

The **second cluster** of interest is referred to as “**Young Negligent**” and includes young employees, who typically work in low-paying positions and are bound into large teams. These results suggest that young employees in low-paying jobs show overconfidence, which is also confirmed in previous work by Porto & Xiao (2016). Focusing on overplacement, Friehe & Pannenberg (2019) also find that overconfidence is particularly pronounced among people with a low salary level. One possible explanation is that a low salary level implies less qualifications (Santos-Pinto & de la Rosa, 2020). Higher-qualified employees tend to earn more (Santos-Pinto & de la Rosa, 2020); at the same time, it can be assumed that they are better able to assess their performance due to their experience and greater knowledge (Aggarwal et al., 2015). To make matters worse, young people often underestimate the likelihood

of becoming a victim of a cyberattack (Hewitt & White, 2020), which corresponds to an overly optimistic assessment of their personal threat situation and leads to risky behaviors.

Another aspect to consider is that, as new joiners, young professionals do not yet identify sufficiently with their new employer and therefore do not show much commitment to the company (Stanton et al., 2004). A stronger commitment to a company could be accompanied by a stronger intrinsic motivation to protect the company's assets and, to this end, a higher awareness of information security. The latter does not seem to be particularly pronounced among the new joiner in this case. They put little effort into security training, which suggests that the mandatory security training is not being done with due diligence.

The **third cluster**, “**High Income Leaders**”, consists mainly of well-paid managers and, in most cases, frequent requests for advice from the IT help desk. Finding that managers tend to be overconfident is not new. More than a decade ago, Rhee et al. (2012) found that managers tend to overestimate their ability to control threats, have low information security awareness, and believe that their organization is less vulnerable than other organizations. The authors note that managers are aware of information security risks but do not associate them with themselves. However, this finding is particularly critical. First, overconfident leaders tend to invest far too little in information security countermeasures (Dong et al., 2019). Second, their leadership role and high self-confidence can lead them to be mistakenly seen as a good role model (Ament, 2017). As for the higher reliance on the help desk, we assume that managers are too busy managing their subordinates and completing their core tasks, which is why they often seek advice from internal IT experts. According to Wright et al. (2020), it is conceivable that the IT help desk provides a certain sense of security that encourages individuals to engage in riskier behavior. The assistance provided by the IT help desk could lead individuals to feel particularly well informed and, in combination with the sense of security, to make an unrealistically positive self-assessment regarding information security.

The **final cluster**, “**Committed Part-timers**”, consists of women who work mostly part-time but are very dedicated to their security training, as they spend the most time completing the training. Consistent with our findings, McGill and Thompson (2018) have revealed that women have less information technology knowledge and exhibit lower overall security behaviors than men. Similarly, Anwar et al.'s (2017) findings suggest deficits in women's information security experience and behaviors, as well as general computer literacy. Looking at the employment status, we see that

part-time employees generally perceive the risk of cyber threats to be lower than full-time employees (Anwar et al., 2016). Consequently, the former often underestimate information security threats. One possible explanation is that part-time employees may not always have access to a computer (Hanus et al., 2021). Therefore, they simply lack experience using computers and consequently underestimate the relevance of information security because they do not have touch points. And while we see them spending a lot of time with security training and appearing very engaged, they lack a proper self-assessment of their skills. This contradicts the findings of Frank et al. (2023), who showed that greater training commitment reduced overconfidence. Therefore, we assume that a large amount of time devoted to online training indicates problems in understanding the tasks and a lack of security knowledge.

4.2. Theoretical and practical implications

To underscore the findings of this study, both theoretical and practical implications are provided in this section. For researchers, our work offers some interesting insights as it explores commonalities and differences among groups of overconfident workers. Our results confirm that discrete contextual factors play a significant role in determining overconfidence among employees. This is consistent with the findings of Frank et al. (2023), who show that understanding the context in which a person is embedded and acts can help predict whether or not they will become overconfident. However, our work extends previous findings by showing that different manifestations of overconfidence affect similar groups of employees.

For practitioners, our findings provide important insights. First, they indicate that this potentially harmful cognitive bias is widespread in organizations and that it must be addressed and overcome. In this regard, our work can serve as a first step toward a better understanding of who is affected by overconfidence and should be addressed by organizational interventions. It emphasizes that there is no one-size-fits-all approach for organizations. However, it is much easier to identify and address vulnerable groups and to demonstrate that individuals' knowledge and expertise in information security are limited (Ament, 2017). Calibration appears to be another effective way for controlling systematic misperceptions of individual knowledge and skills (Fischhoff et al., 1977). According to Stone & Opel (2000), calibration can be improved by providing individuals with feedback on their performance. Therefore, it seems advisable to provide employees with feedback on their performance after security training. This is a cost-effective way for organizations to ensure,

in the ever-changing context of information security, employees develop and maintain a high awareness of their knowledge gaps (Frank, 2021). At the same time, researchers should continue to study calibration in information security intensively and, above all, context-specifically, in order to gain new insights and derive concrete guidance for organizations.

By showing the differences to the non-overconfident population we enhance identifying groups of people who are particularly susceptible to overconfidence and allow practitioners to intervene more effectively. It is particularly important to recognize that different groups have different training needs. For example, with regard to "Committed part-timers", the managers in charge could ensure that the part-time employees are sufficiently sensitized to information security issues during the shorter working hours. This could help create a strong awareness of their vulnerability to cyber threats (Anwar et al., 2016). Looking at the cluster "High-income leaders", executives also need to have enough time to do security training in order to adequately assess their security competencies. They should be regularly encouraged to critically examine their security skills, identify gaps in their security knowledge, and actively pursue further training.

Especially in large teams, companies should take measures to reduce the social and psychological distance between employees, as this generally increases the susceptibility to overconfidence (Rhee et al., 2005). Conducting team-building activities on a regular basis could be a good way to promote knowledge sharing among colleagues and to reduce the distance between employees.

The role of the IT help desk must be clearly defined. On the one hand, employees should be motivated to seek help from experts when they have questions about information security. On the other hand, the IT help desk should not be perceived as an omnipresent safety net on which employees can blindly rely, as this could lead to risky behavior (Wright et al., 2020). Instead, employees must critically reflect on the advice they receive and accept it as help to expand their personal skills and knowledge. Only then can their increase in knowledge contribute to making their self-assessment more realistic (Aggarwal et al., 2015). Finally, the measures and actions taken by the top management should be designed to ensure that everyone acts diligently and in accordance with the security guidelines.

4.2. Limitations and future research avenues

Although this study provides insightful findings regarding overconfidence in information security, the results must be evaluated in light of their potential

limitations. One point to mention is that our investigations are limited to one pharmaceutical company. While this is a valid approach to studying this particular phenomenon (Frank et al., 2023), further insights can be gained if data are collected in different companies with different organizational cultures. This is because previous studies have shown that organizational culture has a significant impact on employee awareness and behavior with respect to information security (Hu et al., 2012; Tang et al., 2016). Furthermore, researchers could also replicate our study in other industries, such as the top two industries by cost per data breach, healthcare and financial services (IBM, 2022).

Since the selection of the discrete context variables is not exhaustive (Johns, 2006), it would also be interesting to consider other variables, for example, whether a person has already experienced a security incident. According to Tatu et al. (2018), security incidents pose a tremendous learning opportunity for employees. This, in turn, usually increases security knowledge and thus leads to better self-assessment (Aggarwal et al., 2015; Kruger & Dunning, 1999). In contrast, studies suggest that victims of cybercrime are more likely to be affected by security incidents again (Junger et al., 2017). In addition to that, scholars may want to include other security training variables, such as whether or not employees complete their training on time (Frank et al., 2022). Previous research have demonstrated that regular security training has a positive impact on attitudes towards information security and information security policy compliance (Puhakainen & Siponen, 2010).

5. Conclusion

Overconfident employees solidify into issues that can jeopardize a company's assets. Therefore, the goal of this study was to examine the three manifestations of information security overconfidence and their similarities and differences. Using a security quiz, we surveyed more than 2,867 employees of a pharmaceutical company. Subsequent cluster analysis revealed striking similarities between employees who exhibit different types of overconfidence. Therefore, our findings augment existing research on this cognitive bias in information security and help to better target at-risk groups.

Acknowledgement

This research was funded in part by the Luxembourg National Research Fund (FNR) and PayPal, PEARL grant reference 13342933/Gilbert Fridgen.

References

- Aggarwal, R., Kryscynski, D., Midha, V., & Singh, H. (2015). Early to Adopt and Early to Discontinue: the impact of self-perceived and actual IT-knowledge on technology use behaviors of end users. *Information Systems Research*, 26(1), 127–144. <https://doi.org/10.1287/isre.2014.0564>
- Aguinis, H., Gottfredson, R. K., & Joo, H. (2013). Best-Practice Recommendations for Defining, Identifying, and Handling Outliers. *Organizational Research Methods*, 16(2), 270–301. <https://doi.org/10.1177/1094428112470848>
- Alasadi, S. A., & Bhaya, W. S. (2017). Review of Data Preprocessing Techniques in Data Mining. *Journal of Engineering and Applied Sciences*, 12(16), 4102–4107.
- Ament, C. (2017). The Ubiquitous Security Expert: Overconfidence in Information Security. *Proceedings of the 38th International Conference of Information on Information Systems*, 1–18.
- Ament, C., & Jaeger, L. (2017). Unconscious of the Own Ignorance: Overconfidence in Information Security. *Proceedings Of the 21st Pacific Asia Conference on Information Systems*.
- Anwar, M., He, W., Ash, I., Xiaohong, Y., Ling, L., & Xu, L. (2017). Gender Difference and Employees' Cybersecurity Behaviors. *Computers in Human Behavior*, 69, 437–443.
- Anwar, M., He, W., & Yuan, X. (2016). Employment Status and Cybersecurity Behaviors. *IEEE International Conference on Behavioral, Economic and Socio-Cultural Computing*, 1–2.
- Audigier, V., Husson, F., & Josse, J. (2016). A principal component method to impute missing values for mixed data. *Advances in Data Analysis and Classification*, 10(1), 5–26. <https://doi.org/10.1007/s11634-014-0195-1>
- Beretta, L., & Santaniello, A. (2016). Nearest neighbor imputation algorithms : a critical evaluation. *BMC Medical Informatics and Decision Making*, 16(74), 197–208. <https://doi.org/10.1186/s12911-016-0318-z>
- Billett, M. T., & Qian, Y. (2008). Are overconfident CEOs born or made? Evidence of self-attribution bias from frequent acquirers. *Management Science*, 54(6), 1037–1051. <https://doi.org/10.1287/mnsc.1070.0830>
- Brozynski, T., Menkhoff, L., & Schmidt, U. (2004). *The Impact of Experience on Risk Taking, Overconfidence, and Herding of Fund Managers: Complementary Survey Evidence*. <http://hdl.handle.net/10419/22404%0D>
- Canfield, C. I., Fischhoff, B., & Davis, A. (2019). Better beware: comparing metacognition for phishing and legitimate emails. *Metacognition and Learning*, 14(3), 343–362. <https://doi.org/10.1007/s11409-019-09197-5>
- De Bondt, W. F. M., & Thaler, R. H. (1995). Financial Decision-Making in Markets and Firms: A Behavioral Perspective. In *Handbooks in Operations Research and Management Science* (Vol. 9). [https://doi.org/10.1016/S0927-0507\(05\)80057-X](https://doi.org/10.1016/S0927-0507(05)80057-X)
- Dong, K., Lin, R., Yin, X., & Xie, Z. (2019). How does

- overconfidence affect information security investment and information security performance? *Enterprise Information Systems*, 1–18.
<https://doi.org/10.1080/17517575.2019.1644672>
- Fischhoff, B., Slovic, P., & Lichtenstein, S. (1977). Knowing with certainty: The appropriateness of extreme confidence. *Journal of Experimental Psychology Human Perception & Performance*, 3(4), 552–564.
<https://doi.org/10.4324/9780203141939>
- Frank, M. (2021). Using Calibration to Help Overcome Information Security Overconfidence. *Proceedings of the 41st International Conference on Information Systems, ICIS 2020*, 1–9.
- Frank, M., Jaeger, L., & Ranft, L. M. (2022). Contextual drivers of employees' phishing susceptibility: Insights from a field study. In *Decision Support Systems* (Vol. 160). <https://doi.org/10.1016/j.dss.2022.113818>
- Frank, M., Jaeger, L., & Ranft, L. M. (2023). Using contextual factors to predict information security overconfidence: A machine learning approach. *Computers and Security*, 125, 103046.
<https://doi.org/10.1016/j.cose.2022.103046>
- Friehe, T., & Pannenberg, M. (2019). Overconfidence over the lifespan: Evidence from Germany. *Journal of Economic Psychology*, 74, 102207.
<https://doi.org/10.1016/j.joep.2019.102207>
- Gervais, S., & Odean, T. (2001). Learning to Be Overconfident. *The Review of Financial Studies*, 14(1), 1–27. <https://www.jstor.org/stable/2696755>
- Halkidi, M., Batistakis, Y., & Vazirgiannis, M. (2001). On Clustering Validation Techniques. *Journal of Intelligent Information Systems*, 17(2–3), 107–145.
<https://doi.org/10.1023/A:1012801612483>
- Halkidi, M., Vazirgiannis, M., & Batistakis, Y. (2000). Quality scheme assessment in the clustering process. In D. A. Zighed, J. Komorowski, & J. Żytkow (Eds.), *Principles of Data Mining and Knowledge Discovery* (Vol. 1910, pp. 265–276). Springer.
https://doi.org/10.1007/3-540-45372-5_26
- Hanamura, K., Takemura, T., & Komatsu, A. (2013). Analysis of characteristics of victims in information security incidents: The case of Japanese internet users. *The Review of Socionetwork Strategies*, 7(1), 143–151.
- Hanus, B., Wu, Y. A., & Parrish, J. (2021). Phish Me, Phish Me Not. *Journal of Computer Information Systems*.
<https://doi.org/10.1080/08874417.2020.1858730>
- Hewitt, B., & White, G. L. (2020). Optimistic Bias and Exposure Affect Security Incidents on Home Computer. *Journal of Computer Information Systems*, 1–11. <https://doi.org/10.1080/08874417.2019.1697860>
- Howah, K., & Chugh, R. (2019). Do we trust the internet? Ignorance and overconfidence in downloading and installing potentially spyware-infected software. *Journal of Global Information Management*, 27(3), 87–100. <https://doi.org/10.4018/JGIM.2019070105>
- Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. *Decision Sciences*, 43(4), 615–660. <https://doi.org/10.1111/j.1540-5915.2012.00361.x>
- Huang, J., & Kisgen, D. J. (2013). Gender and corporate finance: Are male executives overconfident relative to female executives? *Journal of Financial Economics*, 108(3), 822–839.
<https://doi.org/10.1016/j.jfineco.2012.12.005>
- IBM. (2022). *Cost of a Data Breach Report 2022*. <https://www.ibm.com/downloads/cas/3r8n1dzj>
- Jain, A. K. (2010). Data clustering: 50 years beyond K-means. *Pattern Recognition Letters*, 31(8), 651–666.
<https://doi.org/10.1016/j.patrec.2009.09.011>
- Johns, G. (2006). The Essential Impact of Context on Organizational Behavior. *Academy of Management Review*, 31(2), 386–408.
<https://doi.org/10.5465/AMR.2006.20208687>
- Junger, M., Montoya, L., Hartel, P., & Heydari, M. (2017). Towards the normalization of cybercrime victimization: A routine activities analysis of cybercrime in Europe. *2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment, Cyber SA 2017, June*.
<https://doi.org/10.1109/CyberSA.2017.8073391>
- Kruger, J., & Dunning, D. (1999). Unskilled and unaware of It: How Difficulties in Recognizing One's Own Incompetence Lead to Inflated Self-Assessments. *Journal of Personality and Social Psychology*, 77(6), 1121–1134. <https://doi.org/10.1037/0022-3514.77.6.1121>
- Lawson, P., Pearson, C. J., Crowson, A., & Mayhorn, C. B. (2020). Email phishing and signal detection: How persuasion principles and personality influence response patterns and accuracy. *Applied Ergonomics*, 86(December 2018), 103084.
<https://doi.org/10.1016/j.apergo.2020.103084>
- Lewis, D. R. (2018). The perils of overconfidence: Why many consumers fail to seek advice when they really should. *Journal of Financial Services Marketing*, 23(2), 104–111. <https://doi.org/10.1057/s41264-018-0048-7>
- Lundeberg, M. A., Fox, P. W., & Punčohař, J. (1994). Highly Confident but Wrong: Gender Differences and Similarities in Confidence Judgments. *Journal of Educational Psychology*, 86(1), 114–121.
<https://doi.org/https://doi.org/10.1037/0022-0663.86.1.114>
- McGill, T., & Thompson, N. (2018). Gender differences in information security perceptions and behaviour. *ACIS 2018 - 29th Australasian Conference on Information Systems*, 1–11. <https://doi.org/10.5130/acis2018.co>
- McHugh, M. L. (2013). The Chi-square test of independence. *Biochemia Medica*, 23(2), 143–149.
<http://dx.doi.org/10.11613/BM.2013.018>
- Moore, D. A., Dev, A. S., & Goncharova, E. Y. (2018). Overconfidence Across Cultures. *Collabra: Psychology*, 4(1), 1–19.
<https://doi.org/10.1525/collabra.153>
- Moore, D. A., & Healy, P. J. (2008). The Trouble With Overconfidence. *Psychological Review*, 115(2), 502–517. <https://doi.org/10.1037/0033-295X.115.2.502>
- Ortoleva, P., & Snowberg, E. (2015). Overconfidence in political behavior. *American Economic Review*, 105(2), 504–535.

- <https://doi.org/10.1257/aer.20130921>
- Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879–903. <https://doi.org/10.1037/0021-9010.88.5.879>
- Porto, N., & Xiao, J. J. (2016). Financial Literacy Overconfidence and Financial Advice Seeking. *Journal of Financial Service Professionals, 70*(4), 78–88.
- Prims, J. P., & Moore, D. A. (2017). Overconfidence over the lifespan. *Judgement and Decision Making, 12*(1), 29–41.
- Puhakainen, P., & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly, 34*(4), 757–778. <http://www.jstor.org/stable/25750704>
- Ranft, L. M. (2022). Professional Environment Matters—National Characteristics of Information Security Overconfidence. *Twenty-Eighth Americas Conference on Information Systems*, 0–10. https://aisel.aisnet.org/amcis2022/sig_sec/sig_sec/17
- Rhee, H.-S., Ryu, Y., & Kim, C.-T. (2005). I Am Fine but You Are Not: Optimistic Bias and Illusion of Control on Information Security. *ICIS 2005 Proceedings*. <http://aisel.aisnet.org/icis2005>
- Rhee, H.-S., Ryu, Y. U., & Kim, C.-T. (2012). Unrealistic optimism on information security management. *Computers and Security, 31*(2), 221–232. <https://doi.org/10.1016/j.cose.2011.12.001>
- Santos-Pinto, L., & de la Rosa, L. E. (2020). Overconfidence in Labor Markets. In K. F. file:///C:/Users/Muriel/Desktop/Forschung/2023_HICSS_Overconfidence/dong2021.pdf. Zimmermann (Ed.), *Handbook of Labor, Human Resources and Population Economics* (pp. 1–42). Springer Nature Switzerland. https://doi.org/10.1007/978-3-319-57365-6_117-1
- Sebescen, N., & Vitak, J. (2017). Securing the Human: Employee Security Vulnerability Risk in Organizational Settings. *Journal of the American Society for Information Science and Technology, 68*(9), 2237–2247. <https://doi.org/10.1002/asi>
- Stankov, L., & Lee, J. (2014). Overconfidence Across World Regions. *Journal of Cross-Cultural Psychology, 45*(5), 821–837. <https://doi.org/10.1177/0022022114527345>
- Stanton, J. M., Mastrangelo, P. R., Stam, K. R., & Jolton, J. (2004). Behavioral Information Security: Two End User Survey Studies of Motivation and Security Practices. *Proceedings of the 10th Americas Conference on Information Systems*.
- Stone, E. R., & Opel, R. B. (2000). Training to Improve Calibration and Discrimination: The Effects of Performance and Environmental Feedback. *Organizational Behavior and Human Decision Processes, 83*(2), 282–309. <https://doi.org/10.1006/obhd.2000.2910>
- Tang, M., Li, M., & Zhang, T. (2016). The impacts of organizational culture on information security culture: a case study. *Information Technology and Management, 17*(2), 179–186. <https://doi.org/10.1007/s10799-015-0252-2>
- Tatu, T., Ament, C., & Jaeger, L. (2018). Lessons learned from an information security incident: A practical recommendation to involve employees in information security. *Proceedings of the Annual Hawaii International Conference on System Sciences, 3736–3745*. <https://doi.org/10.24251/hicss.2018.471>
- van de Velden, M., Iodice D'Enza, A., & Markos, A. (2019). Distance-based clustering of mixed data. *Wiley Interdisciplinary Reviews: Computational Statistics, 11*(3), 1–12. <https://doi.org/10.1002/wics.1456>
- Wang, J., Li, Y., & Rao, H. R. (2016). Overconfidence in Phishing Email Detection. *Journal of the Association for Information Systems, 17*(11), 759–783. <https://doi.org/10.17705/1jais.00442>
- Wright, R., Johnson, S., & Kitchens, B. (2020). *A Multi-Level Contextualized View of Phishing Susceptibility*. <https://doi.org/10.2139/ssrn.3622310>
- Wu, J. (2012). Cluster Analysis and K-means Clustering: An Introduction. In *Advances in K-means Clustering* (Springer T, pp. 1–16). Springer. https://doi.org/https://doi.org/10.1007/978-3-642-29807-3_1

Appendix

Table 6. Discrete context variables

Discrete Context Dimension	Attribute	Variable Type
Informational Context	Age (in years)	Continuous
	Gender	Binary
Social Context	Helpdesk reliance	Continuous
	Team size	Continuous
Task Context	Employment status	Binary
	Job experience (in days)	Continuous
	No. of security training	Continuous
	Salary band	Categorical
	Training compliance	Binary