Overcoming Conflicting Risk Structures for Cybersecurity Practitioners

R. Ikuenobe Osolease, Ph.D., CISSP-ISSMP

Abstract

I completed my dissertation a few years ago (Osolease, 2021). Having created a model of conflicting risk structures (CRS), I speculated on how effective teamwork enhances decision-making among cybersecurity professionals, crucial for defending systems against threats. The findings showed when team members trust one another, share aligned goals, and resolve conflicts effectively, they make superior decisions. Imagine a group of cybersecurity experts working together to tackle a complex problem—they need mutual trust and a unified strategy. I also found the ability to handle disagreements constructively is vital for team success. The dissertation highlighted how robust teamwork is essential for safeguarding my digital world from cyber threats, providing valuable insights for anyone interested in a cybersecurity career. In this paper I discuss similar research conducted since my dissertation. Perhaps future researchers would follow up and conduct longitudinal research to track team dynamics over time, exploring additional variables such as leadership styles and organizational culture, and using more diverse and larger sample sizes to enhance the generalizability of the findings. Additionally, this paper presents advice to practitioners for overcoming CRSs.

Introduction

The term conflicting risk structures refers to the varying ways security team members perceive, prioritize, and handle risks within their chosen cybersecurity framework. This can include differences in risk tolerance, assessment methods, and strategic responses to potential threats. When team members have conflicting views on risk, it can lead to disagreements and inefficiencies in decision-making processes. There are significant challenges in some cybersecurity teams, such as lack of mutual accountability, unclear team roles, and insufficient task clarity, which can lead to a lack of mutual trust and ineffective team performance (Sinlapanuntakul, Fausett, & Keebler, 2022). There are some indications that humans are the weakest link in IT security, responsible for 86% of security risks, followed by cybernetic sciences at 63% (Triplett, 2022). My dissertation emphasized the importance of understanding and managing ever-present human behaviors, modeled as conflicting risk structures, which includes team cohesion, goal alignment, and conflict resolution. I showed the reader how to statistically measure the impact on decision quality using the following variables.

Team Cohesion

Practitioners should value building strong, trusting relationships among team members is crucial. Encourage open communication and team-building activities to foster mutual respect and trust. When team members feel comfortable with each other, they are more likely to share their views on risk, identify conflicting risk structures, and work towards common solutions.

Goal Alignment

Practitioners must ensure all team members have clear, aligned objectives. Regularly discuss and reinforce the team's goals and priorities to maintain focus. When everyone understands and agrees on what's important, it helps to reduce conflicting risk structures, as everyone is working towards the same end.

Conflict Resolution

Practitioners should develop and practice effective conflict resolution strategies. Provide training in constructive communication and problem-solving techniques. When teams can address and resolve disagreements effectively, they can manage conflicting risk structures better and integrate diverse perspectives into a unified strategy. Encourage an environment where differing opinions are respected and seen as opportunities for improvement. For example, Mitchell et al., 2022, specified debate as a mechanism for constructive discussion and advocacy of task-related differences—as key mediating processes. This example showed how might cognitive diversity translate into innovation in the health care field through structured team interactions.

Decision Quality

I discovered evidence supporting the concept of teams with aligned goals and consensus on what's important to make better decisions. Think of it as a team where everyone is focused on protecting the company's data and systems – they work better together because they share a common purpose. On the other hand, if some members prioritize different agendas, the team might struggle to make effective decisions. Additionally, teams that can resolve conflicts about policies, emotions, and roles tend to make better decisions. If members can discuss their disagreements constructively and find solutions, they can remain focused on the organization's goals and make sound decisions. Rajivan et al. demonstrated by providing team-level rewards leads to better performance compared to individual rewards. This finding also implies that aligned goals and a shared sense of purpose enhance team performance.

Method

Out of the 351 professionals initially considered for the dissertation, 146 met the inclusion criteria and completed the survey. This represents an inclusion rate of approximately 41.6%. The exclusion rate can be inferred from the difference between the total number of potential participants and those who were ultimately included. Out of the 351 invited, 205 were excluded either because they did not meet the inclusion criteria or did not complete the survey. This gives an exclusion rate of approximately 58.4%.

Inclusion Criteria:

Professional Role in Cybersecurity: Participants had to be directly involved in cybersecurity risk management within their organizations.

Experience Level: A minimum of five years of hands-on experience in cybersecurity risk management was required, with an emphasis on those with substantial practical knowledge.

Educational Background: Participants needed to have at least a bachelor's degree in a relevant field, with a preference for those who had pursued postgraduate studies.

Age Range: The target age range was primarily between 30 to 39 years old to ensure a sample with sufficient professional maturity and experience.

Gender Diversity: Efforts were made to include a balanced representation of genders, with a target of at least 43% female professionals.

Exclusion Criteria:

Irrelevant Professional Role: Individuals not directly involved in cybersecurity risk management, such as those in unrelated IT roles, were excluded.

Insufficient Experience: Professionals with less than five years of hands-on experience in cybersecurity were not included.

Lack of Educational Qualification: Individuals without at least a bachelor's degree in a relevant field were excluded from the sample.

Age Outside Target Range: Practitioners outside the primary age range of 30 to 39 years old were less likely to be included unless they had significant experience and qualifications. The target range was 18 years old or older.

Incomplete Surveys: Participants who did not complete the survey fully were excluded from the final analysis to ensure the integrity and completeness of the data.

Participant Characteristics

By understanding and examining cybersecurity risk management teams, I can better sense and address conflicting risk structures, leading to more effective and unified decision-making processes. In my dissertation, I surveyed a diverse and highly qualified group of 146 professionals dedicated to cybersecurity risk management, selected from a pool of 351 respondents. These individuals bring extensive experience and expertise, with most working in information technology security offices and 59% holding roles directly related to safeguarding digital infrastructures. The largest segment of my sample, 37%, has five to ten years of hands-on experience, demonstrating a solid depth of practical knowledge. Educationally, 37% hold bachelor's degrees, and another 14% have pursued postgraduate studies, indicating a strong academic foundation. My participants are diverse in age, primarily between 30 to 39 years old, and gender, with 43% female professionals. Despite their qualifications, these professionals faced challenges in decision-making due to conflicting risk perceptions and priorities. My findings provide valuable insights to help members of the sample to overcome these challenges and enhance their team performance.

Results

My intent is to identify what helps cybersecurity risk management teams make the best decisions. I examined various factors such as how well team members get along, how aligned their goals are, how they handle disagreements, and the types of conflicts they encounter. I found teams where members respect and trust each other tend to make better decisions. It's like how a group of close colleagues working well together can address security issues more effectively because they communicate smoothly and trust one another's judgment. My findings highlight several indicators that can help teams to take action to resolve the negative impact of conflicting risk structures: team cohesion, goal alignment, and conflict resolution style.

Statistical and Data Analysis

I utilized a range of statistical and data analysis methods, including hierarchical multiple regression analysis, R^2, beta weights, significance levels, Confirmatory Factor Analysis (CFA), model fit indices, factor loadings, composite reliability (CR), average variance extracted (AVE), and discriminant validity. These analyses help to elucidate the impact of team cohesion, goal alignment, and conflict resolution on decision quality within cybersecurity risk management teams. For readers, this approach provides detailed insights into the importance of each variable and ensures confidence in the findings through validated measures. Future researchers can rely on methodological rigor and thorough validation, knowing that the constructs used are reliable and distinct. This information serves as a solid foundation for further exploration and practical application in improving team dynamics and decision-making in cybersecurity.

Analysis of Team Cohesion

To substantiate my findings on the effectiveness of cybersecurity risk management teams, I employed a rigorous analytical framework involving multiple statistical tests and models. Utilizing hierarchical multiple regression analysis, I specifically investigated the role of team cohesion in decision-making quality. My analysis revealed that team cohesion, operationalized as the degree to which team members like and consider each other friends, significantly contributes to the variance in decision quality, explaining 21% ($R^2 = .21$, $p < .05$). The regression coefficients indicated that positive interpersonal relationships within the team have a substantial impact on decision outcomes. This was evidenced by significant beta weights for variables representing liking ($\beta = .17$, $p < .05$) and friendship ($\beta = .32$, $p < .01$). These findings underscore the critical importance of fostering strong interpersonal relationships within cybersecurity teams to enhance their decision-making capabilities, highlighting the nuanced role of social dynamics in professional performance.

Analysis of Goal Alignment

Subsequently, I investigated the significance of goal alignment within cybersecurity risk management teams. Utilizing hierarchical multiple regression analysis, I assessed the impact of goal similarity, shared primary objectives, and consensus on critical priorities on decision quality. The results indicated that goal alignment accounted for 31% of the variance in decision quality ($R^2 = .31$, $p < .01$). Specifically, the analysis revealed that similarity of goals ($\beta = .25$, $p < .01$), shared main goals ($\beta = .09$, $p < .05$), and agreement on importance ($\beta = .08$, $p < .05$) significantly contributed to the variance explained. These findings underscore the appropriateness of the hierarchical multiple regression model in delineating the influence of aligned objectives on team performance. The substantial variance explained by goal alignment variables highlights the pivotal role of a unified direction and common objectives in enhancing the decision-making efficacy of cybersecurity teams. This statistical evidence reinforces the hypothesis that cohesive and aligned goals within teams are fundamental to operational success.

Analysis of Conflict Resolution

I also conducted a thorough analysis of how cybersecurity risk management teams handle various types of conflicts, specifically task-related, emotional, and role conflicts. Using hierarchical multiple regression models, I found that effective conflict resolution practices accounted for 24% of the variance in decision quality ($R^2 = .24$, $p < .01$). Furthermore, the management of task conflicts alone explained 11% of the variance ($R^2 = .11$, $p < .05$). These results were obtained by examining conflict resolution norms and intragroup conflicts. The regression coefficients indicated significant beta weights for conflict resolution variables, demonstrating the critical impact of these factors on decision quality. My findings substantiate that the ability to address and resolve disputes constructively is essential for maintaining team focus and fostering effective collaboration. This empirical evidence underscores the importance of robust interpersonal relationships, goal alignment, and conflict resolution mechanisms in enhancing the decision-making capabilities of cybersecurity risk management teams, thereby optimizing their overall performance.

Analysis of Decision Quality

To ensure the reliability of my findings on what enhances decision-making in cybersecurity risk management teams, I conducted thorough statistical analyses using hierarchical multiple regression models. These tests allowed us to quantify the impact of various factors such as team cohesion, goal alignment, and conflict resolution on decision quality. For instance, I found that positive interpersonal relationships within the team accounted for 21% of the decision quality variance, aligned goals explained 31%, and effective conflict resolution added another 24%. Additionally, I assessed the normality of my data through histograms and P.P. plots, checked for multicollinearity with Variance Inflation Factors (VIF), and confirmed the independence of observations using the Durbin-Watson statistic. This rigorous approach gives us confidence that my results are both accurate and meaningful, demonstrating the critical role of these factors in enhancing team performance.

Factor Analysis

The Confirmatory Factor Analysis (CFA) was conducted to validate the measurement model and ensure that the observed variables accurately represent the underlying latent constructs. The model fit indices provide a comprehensive assessment of the model's adequacy. The chi-square test, which assesses the discrepancy between the observed and expected covariance matrices, yielded a significant value ($\chi^2 = 145.67$, $df = 73$, $p < .001$). Although significant chi-square values are common in large samples, other fit indices indicated a good model fit. The Root Mean Square Error of Approximation (RMSEA) was 0.045, indicating a good fit, as values less than 0.05 are ideal. Additionally, the Comparative Fit Index (CFI) and Tucker-Lewis Index (TLI) were 0.94 and 0.92, respectively, both above the 0.90 threshold, suggesting a good fit. The Standardized Root Mean Square Residual (SRMR) was 0.038, further confirming a good model fit.

Factor Loadings. Factor loadings for all observed variables were significant ($p < .001$) on their respective latent constructs, indicating that the items are strong indicators of the underlying factors. The factor loadings ranged from 0.68 to 0.89, which are considered robust. This supports the reliability and validity of the measurement model. Construct reliability and validity were further assessed using Composite Reliability (CR) and Average Variance Extracted (AVE). CR values ranged from 0.78 to 0.92, surpassing the 0.70 threshold for good reliability. AVE values ranged from 0.55 to 0.76, indicating good convergent validity as they exceed the 0.50 threshold. Discriminant validity was confirmed as the square roots of the AVEs were greater than the inter-construct correlations, demonstrating that each construct is distinct from others in the model.

Model Fit. Fortunately, the CFA results affirm that the measurement model possesses moderate fit, reliability, and validity. The significant factor loadings, high composite reliability, and average variance extracted values underscore that the observed variables reliably and validly measure the underlying constructs. This validation bolsters the confidence in the constructs used for future analyses, ensuring the robustness and meaningfulness of the findings. The minor adjustments suggested by the modification indices were not substantial, indicating that the initial model was well-specified. These results provide a strong foundation for the continued use of these constructs in further research and practical applications.

Discussion

Key Take Aways

So, what does this mean for cybersecurity risk management teams? For team leaders, fostering respect and trust among team members and ensuring everyone has clear, shared goals can lead to better teamwork and decision-making. For the team members, understanding that mutual respect, goal alignment, and effective conflict resolution can significantly enhance the team's performance. The lesson of my dissertation is that good relationships, clear goals, and effective conflict resolution are crucial for making quality decisions to protect organizations from adversaries, competitors, and rivals. Similarly, other researchers have found that trust is crucial for the long-term success of an organization and affects the confidence of stakeholders in the organization's ability to safeguard sensitive information (Ciekanowski et al., 2024). The concept of shared ownership has been used to foster a culture or security awareness and cooperation (Clark and Martin, 2024).

Focus Areas

In conclusion, cybersecurity risk management teams can significantly improve their decision-making capabilities by focusing on three key areas: fostering team cohesion, aligning team goals, and developing effective conflict resolution strategies. Building strong, trusting relationships through open communication and team-building activities encourages members to share their views on risk and work towards common solutions. Ensuring all team members have clear, aligned objectives helps maintain

focus and reduces conflicting priorities, leading to more effective decision-making. Additionally, providing training in constructive communication and problem-solving techniques enables teams to address and resolve disagreements effectively, integrating diverse perspectives into a cohesive strategy. By applying these strategies, teams can enhance their performance and better protect their organizations.

Weaknesses of this Research

One primary weakness of the research is the sample size and its generalizability. Although the sample size was adequate for statistical analysis, it may not be large enough to generalize the findings to a broader population. The sample was also limited to specific roles within cybersecurity risk management, which might not represent the entire field of IT security. Additionally, the cross-sectional design of the dissertation captures data at a single point in time, limiting the ability to infer causal relationships between variables. Another concern is the reliance on self-reported data, which can introduce preconceptions such as social desirability bias and recall bias.

Variables. The dissertation also has a limited scope of variables, focusing primarily on team cohesion, goal alignment, and conflict resolution. Other potentially influential factors, such as leadership style, organizational culture, and external environmental factors, were not examined. Furthermore, the research found high correlations among some variables, indicating potential multicollinearity, which can inflate the variance of coefficient estimates and complicate the assessment of individual predictor impacts. The context-specific nature of the findings, which are limited to cybersecurity risk management teams, further restricts the generalizability to other more diverse sample that covers a broader range of roles and industries within cybersecurity to enhance the generalizability of the findings. Longitudinal studies should be conducted to track changes over time and establish causal relationships, providing a more comprehensive understanding of how team dynamics influence decision-making quality. To mitigate the biases associated with self-reported data, future studies should incorporate multiple data sources, such as observational data, peer evaluations, and performance metrics. Expanding the scope of research to include additional variables, such as leadership style and organizational culture, will offer a more holistic view of the factors contributing to effective team performance.

Alternative Measures. To address potential multicollinearity, researchers should continue to use statistical alternative techniques to variance inflation factor (VIF) analysis and consider partial least squares (PLS) regression or ridge regression if multicollinearity is present. Additionally, replicating the dissertation multiple times, but having the sample participants in the different contexts and industries will help determine the applicability of the findings beyond cybersecurity risk management. Comparative studies across different sectors can provide insights into the universality of the identified factors. By addressing these weaknesses and implementing the recommended strategies, future research can enhance the robustness, validity, and generalizability of findings related to team dynamics and decision-making in cybersecurity risk management teams.

References

Clarke, M., & Martin, K. (2024). Managing cybersecurity risk in healthcare settings. In Healthcare Management Forum (Vol. 37, No. 1, pp. 17-20). Sage CA: Los Angeles, CA: SAGE Publications.

Ciekanowski, Z., Nowicka, J., Czternastek, M., Żurawski, S., & Mikosik, P. (2024). How Cybersecurity Shapes Effective Organizational Management. European Research Studies Journal, 27(2), 454-464.

Henshel, D., Cains, M. G., Hoffman, B., & Kelley, T. (2015). Trust as a human factor in holistic cyber security risk assessment. Procedia Manufacturing, 3, 1117-1124.

Mathew, A. J. (2024). Unscripted Practices for Uncertain Events: Organizational Problems in Cybersecurity Incident Management. Science, Technology, & Human Values, 01622439241240411.

Mitchell, R., Boyle, B., O'Brien, R., Malik, A., Tian, K., Parker, V., ... & Chiang, V. (2017). Balancing cognitive diversity and mutual understanding in multidisciplinary teams. Health care management review, 42(1), 42-52.

Osolease, R. I. (2021). Conflicting Risk Structures and Decision Quality: The Moderating Effects of Cognitive Diversity (Doctoral dissertation, Capella University).

Rajivan, P., Champion, M., Cooke, N. J., Jariwala, S., Dube, G., & Buchanan, V. (2013). Effects of teamwork versus group work on signal detection in cyber defense teams. In Foundations of Augmented Cognition: 7th International Conference, AC 2013, Held as Part of HCI International 2013, Las Vegas, NV, USA, July 21-26, 2013. Proceedings 7 (pp. 172-180). Springer Berlin Heidelberg.

Sinlapanuntakul, P., Fausett, C. M., & Keebler, J. R. (2022, September). Exploring Team Competencies in Cybersecurity. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting (Vol. 66, No. 1, pp. 1110-1114). Sage CA: Los Angeles, CA: SAGE Publications.