EPiC Series in Computing

Volume 102, 2024, Pages 100–110

Proceedings of Conference on Cognitive and Computational Aspects of Situation Management 2023

Investigating Team Level KSAs in Cybersecurity: Insights from Observing a Cybersecurity-Themed Board Game Pilot Study

Crystal M. Fausett[1*], Jenna M. Korentsides[1], Sabina M. Patel[1], David Schuster[2], Elizabeth H. Lazzara[1], Joseph R. Keebler[1]

[1] Embry-Riddle Aeronautical University, Florida, US

[2] San José State University, California, US

fausetc1@my.erau.edu, korentsj@my.erau.edu, patels77@my.erau.edu, david.schuster@sjsu.edu, lazzarae@erau.edu, keeblerj@erau.edu

Abstract

Effective teamwork plays a crucial role in the dynamic field of cybersecurity. However, identifying the specific knowledge, skills, and attitudes (KSAs) required for successful cybersecurity teamwork poses challenges. One of these challenges is limited access to proprietary information, which hinders the study of cybersecurity teamwork KSAs. To address this issue, this research proposes the use of a cybersecurity-themed board game as an experimental testbed to observe and analyze teamwork dynamics. By studying teamwork within this simulated environment, valuable insights can be gained that have the potential to translate to real-world cybersecurity teams. This research aims to contribute to the understanding of cybersecurity team dynamics and inform the development of future experimental testbeds that can provide insights into effective cybersecurity teamwork. By acknowledging the challenges associated with limited accessibility and employing innovative methodologies, this study seeks to make meaningful contributions to knowledge of cybersecurity teamwork.

1 Introduction

Modern organizations encompass intricate systems, cognitively demanding tasks, and dynamic teaming activities. Organizations are constantly evolving, requiring employees to possess and update the necessary knowledge, skills, and attitudes (KSAs) to effectively accomplish their work. Continuous awareness and training on these KSAs are essential for employees to navigate the complex nature of their tasks and achieve desired outcomes. In the field of team performance,

* Corresponding author.

K. Baclawski, M. Kozak, K. Bellman, G. D'Aniello, A. Ruvinsky and C. Da Silva Ferreira Barreto (eds.), CogSIMA 2023 (EPiC Series in Computing, vol. 102), pp. 100–110

researchers have highlighted the importance of two distinct skill sets for effective teams: taskwork skills and teamwork skills [1]. Taskwork skills refer to the abilities required by team members to carry out their designated tasks, while teamwork skills primarily encompass the cognitions, attitudes, and behaviors necessary for teams to function effectively in completing these tasks [2]. For example, KSAs such as psychological safety, joint problem-solving orientation, perceived task interdependence, and internal learning behaviors have been shown to be positively associated with team performance outcomes across domains such as healthcare and aviation. Teams of interdependent, specialized individuals with the requisite KSAs to perform complementary taskwork provide a mechanism for teams to outperform individuals. Thus, an emergent property of teamwork is higher achievement together. Thus, teamwork skills are important to the performance of modern organizations, including those in cybersecurity functions.

Within cybersecurity, a lack of comprehensive understanding regarding the functioning of cybersecurity teams poses a significant challenge. Agyepong and colleagues [3] identified inadequate communication as one of the top challenges faced by security operations center analysts. This finding highlights the critical role of effective communication within cybersecurity teams, suggesting the need for a deeper understanding of the specific KSAs required for successful teamwork in this context. Although significant literature exists on enhancing team effectiveness [2], [4], [5], cybersecurity work presents distinct challenges. First, cybersecurity teams operate in a reactive environment, where threats rapidly emerge and evolve. This creates an atmosphere of demanding adaptability and resilience like the dynamic, high-pressure environments that military combat teams and emergency medical trauma response teams operate in. However, cybersecurity teams are relatively understudied compared to those teams, and may have unique aspects. Secondly, the abstract and cognitively demanding nature of cybersecurity work sets it apart from many professions [6]. While extensive literature exists on team effectiveness, the distinct characteristics of cybersecurity work necessitate domain specific studies. As a barrier for researchers, cybersecurity teams operate in a context where the dissemination of operational information is limited due to security concerns and the protection of proprietary data. This limited access to information about cybersecurity team dynamics may impede progress towards identifying and defining specific cybersecurity teamwork KSAs. Consequently, there remains a considerable gap in our understanding of the requisite KSAs for effective cybersecurity teamwork, some of which include psychological safety, join problem-solving orientation, perceived task interdependence, and internal learning behavior.

Addressing this knowledge gap necessitates innovative approaches that circumvent the access problem yet still provide valuable insights into the composition and characteristics of effective cybersecurity teams. In this regard, an avenue of exploration involves observing teamwork dynamics within a cybersecurity-themed board game. By studying players engaged in such games, we can potentially uncover useful information that sheds light on the fundamental components of successful cybersecurity teamwork. Here, we take a step towards addressing the challenge of identifying and delineating cybersecurity teamwork KSAs by utilizing a cybersecurity-themed board game as an experimental platform. By examining the observable manifestations of effective teamwork within this simulated environment, we hope to extract valuable insights that contribute to the limited existing knowledge base. Such insights can lay the foundation for identifying comprehensive KSAs for cybersecurity professionals.

1.1 Psychological Safety

Psychological safety has been deemed invaluable characteristic of teams within many domains. Psychological safety is defined by how safe individual team members feel to speak up or take interpersonal risk [7]. An example of someone who has high psychological safety would be able to speak up to a supervisor or to the team when they find a mistake in the upcoming presentation slides. That individual feels as though they would not be reprimanded for informing the rest of the team

about this problem. A person with low psychological safety may feel uncomfortable or be unable to speak up and share information. A systematic review found, in the high-risk domains encouraging individuals to speak up can prevent injury or dangerous situations from occurring [8]. Within cybersecurity, having high psychological safety among team members could be valuable in identifying potential threats or problems within the existing security system. Measures of psychological safety from [7] were used for this study. Items included "I feel I can bring up problems and tough issues with the other party," and "I feel the other party would not deliberately act in a way that undermines my efforts."

1.2 Joint Problem-Solving Orientation

Joint problem-solving orientation refers to a collaborative approach where team members work together to identify, analyze, and solve problems collectively. It is characterized by a shared understanding that problems are not individual responsibilities but rather shared challenges that require the active participation and contributions of all team members. In joint problem-solving, team members collaborate, exchange ideas, and integrate their diverse perspectives and expertise to develop innovative solutions [9]. For example, by engaging in joint problem-solving, cybersecurity professionals, researchers, organizations, and even government agencies can share their insights, experiences, and best practices. This collaboration enables a more holistic understanding of the threat landscape and promotes the development of innovative solutions. Moreover, by engaging in joint problem-solving orientation, teams can improve overall performance and better enable them to accomplish their goals. Joint problem-solving orientation survey items were adapted from [9]. Items included "Problems arising as we worked were seen as joint rather than individual responsibilities," and "I view the other parties as a true partner in this work."

1.3 Perceived Task Interdependence

Interdependence is a construct that represents the degree to which individuals or entities rely on and influence each other within a system or relationship. It is used to describe the interconnectedness, mutual reliance, and reciprocal influence between the elements or components of a system. Although the board game requires task interdependence to some extent (players must complete their own turns before other players complete theirs), the extent to which participants rely on each other throughout the game will likely vary team to team. One team may have a leader that instructs others on the appropriate actions, whereas other teams may demonstrate a shared leadership approach or, alternatively, rarely consult each other at all. For the purposes of this study, perceived team task interdependence items were used to assess how well participants rated their relative task interdependence of their given team. Perceived interdependence was measured through survey questions from [10] upon completion of the board game task. An example of survey items used to assess perceived interdependence included "Members of this team had to depend heavily on one another to get the team's work done," and "Members of this team had their own individual jobs to do, with little need for them to work together."

1.4 Internal Learning Behavior

Internal learning behavior plays a crucial role in the success of teams across various domains [11]. Internal learning behaviors encompass the cognitive and psychological processes through which individuals acquire new knowledge, skills, or understandings based on their experiences. It involves the interactions among team members, such as questioning, seeking feedback, and openly discussing errors, with the aim of improving future performance [7]. For instance, in team-based games, reflection and feedback processing are critical as players collaborate, communicate, and coordinate

their actions to maximize their individual and collective performance during each turn. Through internal learning, teams enhance their problem-solving and detection skills, collectively comprehend the situation, and uncover new information [7], [11]. While internal learning behavior is inherently individual, its components are essential for effective coordination among team members. This characteristic can be observed in various domains where professionals must focus on relevant information, acquire, process, and encode new knowledge into memory for future use, and translate this information into action or communication to achieve goals. In the context of cybersecurity, a rapidly evolving field, internal learning behaviors are particularly valuable as they enable professionals to continuously learn about new threats, vulnerabilities, and emerging solutions [12]. By utilizing internal learning behaviors, cybersecurity experts can adapt to evolving threats, enhance their awareness, strengthen problem-solving capabilities, and develop greater expertise in cybersecurity. Gaining a deeper understanding of internal learning behaviors and optimizing them can contribute to more effective learning strategies, improved problem-solving abilities, and enhanced decision-making skills, all of which are critical for a team's success. Internal learning behaviors were assessed through survey items adopted from [11] such as "We regularly took time to figure out ways to improve our team's work processes," and "People in the team often spoke up to test assumptions about issues under discussion."

1.5 The Current Paper

The current paper discusses the results of a pilot study with a small sample size of four teams of two to three individuals. Pilot studies may be thought of as preliminary studies that are conducted to evaluate the sustainability of a planned study and avoid problems that could arise when the large-scale study is conducted [13]. Through the exploration of a unique and accessible methodology, we endeavor to unveil findings that can inform future research in the field of cybersecurity team effectiveness. Some researchers have argued that there is an ethical obligation to attempt to publish the results of pilot studies to promote transparency and knowledge sharing within the research community, especially in an area with a limited amount of research [13]. Moreover, we recognize that disseminating the findings of this pilot study can have practical implications by influencing research resources and preventing unnecessary duplication of effort. Embracing this principle, we strive to contribute to the advancement of the cybersecurity field and facilitate evidence based approaches to enhance cybersecurity team performance.

2 Methods

2.1 Participants

Four teams of 2-3 players were recruited from a small southeastern university in the United States. This resulted in 9 total participants, with one team of three. The remaining three teams were dyads. No specific participant inclusion criteria were employed in the selection process; however, all participants were over 18 years of age. Participants received the following description of the study: "I am asking you to take part in a research project for the purpose of investigating the relationship between joint problem-solving orientation, psychological safety, interdependence, and internal learning behaviors on team performance. You will be asked to complete a couple of surveys and then assigned a role to play in the board game known as [d0x3d!]. You will be participating on a team with other team members. Your game play will be videotaped without capturing your face. After the game is completed, you will be asked to complete a survey about your experience. The total time of your participation is approximately 90 minutes."

2.2 Procedure

Upon participants' arrival, they were instructed to read and sign the consent forms. They were then directed to login to iPads to complete the demographic survey and cybersecurity knowledge quiz. Afterward, participants were seated and instructed to watch a tutorial video on game play and then engage in a practice round. Participants were informed of specific game rules during the tutorial, such as the flipping of starting tiles, trading or giving loot cards only between players on the same tile, flipping of tiles around pawns, and the consequences of decommissioning tiles or assets. During the practice round, participants had the opportunity to ask the researcher questions. Following the practice round, the board game was played for 60 minutes. Once the game started, researchers ceased providing assistance. Nonetheless, players had access to a packet containing the rules of the board game, which they could consult at any time during gameplay. The researcher would intervene if players made an incorrect move, stating, "that is incorrect/not allowed. Please refer to the rule book for more information on the appropriate actions." At the end of the game, participants were instructed to complete a second survey on the iPads which included items related to psychological safety, joint problem-solving orientation, interdependence, and internal learning behavior measures. Once completed, a debriefing was conducted, thanking participants for their participation, providing contact information for further questions, and explaining the purpose of the study.

2.3 Simulation Testbed

This study used a commercial off-the-shelf board game called [d0x3d!] [14] to cultivate an environment in which teamwork and decision making are emphasized. [d0x3d!] is a cooperative board game where players act as hackers aiming to infiltrate a network, collect digital assets, and escape before being apprehended by network administrators. The board of [d0x3d!] is modeled after a computer network, in which each player takes on a particular hacker role to help the other players travel through the network and retrieve stolen digital assets. For the purposes of this study, players were only allowed to serve in the roles of social engineer, traffic spoofer, and war driver.

2.4 Demographic Survey and Cybersecurity Knowledge Quiz

A demographic survey was used to gather essential information about participants. The survey asked participants to report their age and gender. The demographic survey also assessed video game playing and board game playing habits of participants. Specifically, participants were asked to indicate the hours per week they played video games, with the following options: "I don't play board games," "Less than 5," "5-10," "11-15," "16-20," and "20+." The same measurement was used to assess board game play.

The Pew Research Center's cybersecurity knowledge quiz [15] was designed to assess individuals' knowledge and awareness of cybersecurity issues and best practices. It consisted of a series of multiple-choice questions covering topics such as online safety, password security, and privacy. This quiz was used to measure cybersecurity knowledge.

2.5 Team Performance Assessment

Team performance was measured through multiple metrics at the end of game play. Those team performance measures were win/loss, the number of digital assets recovered, and infocon level. Each of these measures was recorded by the researcher upon completion of the game.

Win/Loss. This is a binary metric of performance, indicated by whether the team won or lost the game. To win, the team must have retrieved all four stolen digital assets, met on the Internet Gateway tile, and played a zero-day exploit card. If the team lost, this means that the threat level reached Infocon Level one, or that the game became impossible to win.

Number of Digital Assets Recovered. The object of the game was to recover all four digital assets and escape. The four digital assets include: authentication credentials, financial data, intellectual property, and personally identifiable information. Because recovering digital assets is a goal of the game, the number is a logical measure of team performance (i.e, the more digital assets recovered, the better the team performed).

Infocon Level. The infocon level measures performance inversely; it is raised whenever players have been spotted. The infocon level acts as a barrier to success in the game; the higher the infocon level, the more machines the admins investigate. The infocon level acts like the infection rate tracker in the popular board game Pandemic [16]. This metric is generally negatively associated with team performance (higher infocon levels increase the game difficulty and make it harder to win).

3 Results

The demographic survey collected information concerning each participant's background, video game experience, board game experience, and cybersecurity knowledge. The collected demographic survey items (Table 1) reveal a relatively homogenous sample, with participants reporting similar age ranges, board game experience, and cybersecurity knowledge. Additionally, no participant indicated that they had ever heard of or played [d0x3d!] previously.

Participant Age Ranges	**Percentage of Sample**
18-22	88.89%
23-26	11.11%
Gender	
Male	44.44%
Female	55.56%
How many hours a week do you play video games?	
I don't play video games	22.22%
Less than 5	44.44%
5-10	22.22%
11-15	11.11%
How many hours a week do you play board games?	
I don't play board games	44%
Less than 5	33%
5-10	22%
Cybersecurity Knowledge	
4 out of 10 questions correct	11%
5 out of 10 questions correct	11%
6 out of 10 questions correct	44%
7 out of 10 questions correct	11%
8 out of 10 questions correct	22%

Table 1: Participant Demographics

The following section will discuss each of the four teams and their outcomes as far as team

performance, psychological safety, joint problem-solving orientation, perceived task interdependence, and internal learning behaviors.

3.1 Team 1

Team 1. Team 1 successfully won the board game. This team had the highest psychological safety score across all the four teams. They also had high scores for joint problem-solving orientation, perceived task interdependence, and internal learning behaviors. Interestingly, the individuals on this team had the lowest average score on the cybersecurity knowledge quiz. This indicates that it is unlikely prior knowledge of cybersecurity is necessary to play and understand the game. The team required all four digital assets, as is required to win. Notably, the team had a higher infocon level (4 out of 5) and still managed to win.

3.2 Team 2

Team 2 lost the game. This team had relatively average scores for psychological safety, joint problem-solving orientation, perceived task interdependence, and cybersecurity knowledge. This team only managed to recover one of the four digital assets and ended the game with an infocon level of 3.

3.3 Team 3

Team 3 arguably performed the worst of all for teams, losing the game. They had only one digital asset and ended the game with an infocon level of 5 (the maximum level before getting "doxed"). This team also consistently had the lowest scores for psychological safety, joint problem-solving orientation, perceived task interdependence, and internal learning behaviors. Internal learning behaviors was remarkably low (M = 1.5) and suggests that low scores in this area may be harmful to team performance. Interestingly, this team had high combined scores of cybersecurity knowledge.

3.4 Team 4

Team 4 successfully won the game. They had the highest score for joint problem-solving orientation (M = 4.9) and internal learning behaviors (M = 4.83). This team finished the game, acquiring all four digital assets, with an infocon level of 2. This team had the same averaged cybersecurity knowledge score as Team 3.

3.5 Fisher's Exact Tests

To determine if there was any association between board-game playing and winning or losing [d0x3d!] we performed Fisher's exact tests. Fisher's exact tests were chosen to understand if the proportions of one variable (win/lose) were dependent upon another variable (board game play) given that expected cell counts were < 5. The results ($p = 1.00$) do not indicate a significant association found between board game play and wins/losses. The same was done for video game play and wins/losses. The results ($p = 1.00$) do no indicate a significant association between video game play and wins/losses. Although this indicates these factors did not play a significant role in the success of failure of the four teams, these results are inconclusive due to low power. No interpretation should be made based on the results obtained.

Team 1	Mean	(*SD*)
Psychological Safety	5	*(0.0)*
Joint-Problem Solving Orientation	4.86	*(0.23)*
Perceived Task Interdependence	4.22	*(0.51)*
Internal Learning Behaviors	4	*(0.58)*
Cybersecurity Knowledge (*out of 10)*	5	*(1.0)*
Win/Loss	Win	-
Digital Assets Retrieved (*out of 4)*	4	-
Infocon Level (*out of 5)*	4	-
Team 2	Mean	*(SD)*
Psychological Safety	4.17	*(0.47)*
Joint-Problem Solving Orientation	4.5	*(0.28)*
Perceived Task Interdependence	3.83	*(0.24)*
Internal Learning Behaviors	3.33	*(0.24)*
Cybersecurity Knowledge (*out of 10)*	6.5	*(1.41)*
Win/Loss	Loss	-
Digital Assets Retrieved (*out of 4)*	1	-
Infocon Level (*out of 5)*	3	-
Team 3	Mean	*(SD)*
Psychological Safety	3.33	*(0.47)*
Joint-Problem Solving Orientation	3.8	*(0.28)*
Perceived Task Interdependence	3.16	*(0.24)*
Internal Learning Behaviors	1.5	*(0.24)*
Cybersecurity Knowledge (*out of 10)*	7	*(1.41)*
Win/Loss	Loss	-
Digital Assets Retrieved (*out of 4)*	1	-
Infocon Level (*out of 5)*	5	-
Team 4	Mean	*(SD)*
Psychological Safety	4.17	*(0.24)*
Joint-Problem Solving Orientation	4.9	*(0.14)*
Perceived Task Interdependence	4.5	*(0.71)*
Internal Learning Behaviors	4.83	*(0.24)*
Cybersecurity Knowledge (*out of 10)*	7	*(1.41)*
Win/Loss	Win	-
Digital Assets Retrieved (*out of 4)*	4	-
Infocon Level (*out of 5)*	2	-

Table 2: Summary of metrics and measurements by team

4 Discussion

4.1 Implications

With this study, we aimed to demonstrate a method for observing team performance in a cybersecurity context. Using the board game [d0x3d!], we found that we could obtain interpretable data from novice participants. Further, as participants with diverse levels of cybersecurity knowledge were able to successfully engage in the gameplay, this method may hold promise to observe teamwork in a general context. For example, it may be possible to measure and develop teamwork among novice cybersecurity professionals or K-12 students with limited domain knowledge.

The primary implication of this research is methodological. We have presented a framework for using easily available games to capture team performance. With replication and further refinement, the findings of this research may have several implications for both research and practice in the field of cybersecurity team effectiveness. By exploring the team-level KSAs that may be applicable to cybersecurity teamwork, future research can add to the limited knowledge base on teamwork and cybersecurity. Team-level KSAs, such as psychological safety, joint-problem solving orientation, perceived interdependence, and internal learning behaviors, may guide for organizations seeking to enhance the performance of their cybersecurity teams. Understanding the relevant KSAs for cybersecurity teams can help form high- performing teams that effectively respond to the ever-evolving cybersecurity landscape.

Second, the unique challenges faced by cybersecurity teams, including their reactive environment and high cognitive demands underscore the importance of domain-specific studies. The distinct nature of cybersecurity work calls for tailored approaches to studying teamwork dynamics and identifying the specific KSAs required for successful teaming. By addressing these challenges through innovative research methodologies, such as the use of cybersecurity-themed board games, researchers can gain deeper insights into the dynamics of cybersecurity teamwork and develop targeted interventions to improve team effectiveness.

This study's implications extend to both research and practice by contributing to the understanding of team-level KSAs specific to cybersecurity teamwork, emphasizing the need for domain-specific studies to overcome access problems, and highlighting the importance of effective teamwork. This work suggests that psychological safety, joint problem-solving orientation, perceived task interdependence, and internal learning behaviors are worthy of further investigation in the context of cybersecurity teams. By integrating these implications into future research and organizational practices, strides can be made in enhancing the effectiveness and performance of cybersecurity teams, ultimately strengthening the cybersecurity posture of organizations in the face of evolving threats.

4.2 Limitations

Despite the potential contributions of this pilot study to our understanding of cybersecurity teamwork KSAs, it is important to acknowledge its inherent limitations. First and foremost, the scope of the study is constrained by its pilot nature, which involves a small sample size and a limited duration of data collection. As a result, the findings may not be generalizable to the broader population of cybersecurity teams. It is essential to interpret the results within the context of the specific conditions and constraints of the study. Furthermore, the use of a cybersecurity-themed board game as an experimental platform introduces some unknowns we were not able to fully resolve. While efforts have been made to simulate real-world teamwork dynamics, it is important to recognize that it will not capture the complexity and nuances of actual cybersecurity team interactions. The game environment may differ from real-life scenarios in terms of stress levels, time pressure, and the consequences associated with cybersecurity decision-making. An important question for future research is how the cybersecurity aspects of the game affect team performance compared to similar

approaches in other domains (e.g., Pandemic; Leacock, 2008). Given the proprietary nature of cybersecurity activities, the board game testbed offers a valuable analog to studying real-world cybersecurity teaming. Another limitation is the reliance on observed metrics within the game as indicators of effective teamwork. While these observations can provide valuable insights, they may not fully capture the underlying cognitive processes, individual contributions, and team dynamics that contribute to cybersecurity team effectiveness. It is important to note that this pilot study is exploratory in nature and does not aim to provide definitive conclusions regarding cybersecurity teamwork KSAs. Instead, it serves as a starting point for further investigation and refinement of research methods and measures. Future research may benefit from investigating the effect of team size on performance in this context, and the differences between ad-hoc and intact teams. Despite these limitations, this pilot study makes a valuable methodological contribution to the literature and may prove to be useful for future research in the field of cybersecurity team effectiveness. It serves as an initial exploration of the potential benefits of using a cybersecurity-themed board game as an experimental platform and provides insights that can inform the development of more comprehensive research designs in the future.

5 Conclusion

In conclusion, this study sheds light on the important role of team-level KSAs in cybersecurity teamwork and the unique challenges faced by cybersecurity teams. The findings emphasize the significance of taskwork skills and teamwork skills for effective team performance, highlighting the need for continuous training and development in these areas. The specific team-level KSAs studied such as psychological safety, joint-problem solving orientation, perceived task interdependence, and internal learning behaviors, serve as valuable guides for organizations aiming to enhance the performance of their cybersecurity teams.

References

[1] E. R. Crawford and J. A. LePine, “A Configural Theory of Team Processes: Accounting for the Structure of Taskwork and Teamwork,” Acad. Manage. Rev., vol. 38, no. 1, pp. 32–48, Jan. 2013, doi: 10.5465/amr.2011.0206.

[2] E. Salas, M. A. Rosen, C. S. Burke, and G. F. Goodwin, “The wisdom of collectives in organizations: An update of the teamwork competencies.,” Team Eff. Complex Organ. Cross-Discip. Perspect. Approaches, pp. 39–79, 2009.

[3] E. Agyepong, Y. Cherdantseva, P. Reinecke, and Burnap, “Challenges and performance metrics for security operations center analysts: a systematic review,” J. Cyber Secur. Technol., vol. 4, no. 3, pp. 125– 152, 2020.

[4] J. Mathieu, M. T. Maynard, T. Rapp, and L. Gilson, “Team Effectiveness 1997-2007: A Review of Recent Advancements and a Glimpse Into the Future,” J. Manag., vol. 34, no. 3, pp. 410–476, Jun. 2008, doi: 10.1177/0149206308316061.

[5] M. I. Delgado Piña, A. María Romero Martínez, and L. Gómez Martínez, “Teams in organizations: a review on team effectiveness,” Team Perform. Manag. Int. J., vol. 14, no. 1/2, pp. 7–21, Jan. 2008, doi: 10.1108/13527590810860177.

[6] Psychosocial dynamics of cyber security. in Psychosocial dynamics of cyber security. New York, NY, US: Routledge/Taylor & Francis Group, 2016, pp. xxx, 321.

[7] A. Edmondson, “Psychological safety and learning behavior in work teams,” Adm. Sci. Q., vol. 44, no. 2, pp. 350–383, 1999.

[8] A. Newman, R. Donohue, and N. Eva, “Psychological safety: A systematic review of the

literature," Hum. Resour. Manag. Rev., vol. 27, no. 3, pp. 521–535, 2017.
[9] M. J. Kerrissey, A. T. Mayo, and A. C. Edmondson, "Joint problemsolving orientation in fluid cross-boundary teams," Acad. Manag. Discov., vol. 7, no. 3, pp. 381–405, 2021.
[10] R. Wageman, "Interdependence and Group Effectiveness," Adm. Sci. Q., vol. 40, no. 1, pp. 145–180, 1995, doi: 10.2307/2393703.
[11] H. Bresman and M. Zellmer-Bruhn, "The structural context of team learning: Effects of organizational and team structure on internal and external learning," Organ. Sci., vol. 24, no. 4, pp. 1120–1139, 2013.
[12] L. Lee, "Cybercrime has evolved: it's time cyber security did too," Comput. Fraud Secur., vol. 2019, no. 6, pp. 8–11, 2019.
[13] L. Thabane et al., "A tutorial on pilot studies: the what, why and how," BMC Med. Res. Methodol., vol. 10, pp. 1–10, 2010.
[14] M. Gondree and Z. N. Peterson, "Valuing security by getting [d0x3d!]: Experiences with a network security board game," presented at the 6th Workshop on Cyber Security Experimentation and Test ({CSET} 13), 2013.
[15] K. Olmstead and A. Smith, "Americans and cybersecurity," Pew Res. Cent., vol. 26, no. 311–27, 2017.
[16] M. Leacock, "No single player can win this board game. It's called pandemic," N. Y. Times, vol. 25, 2020.