Applied Human Factors and Ergonomics (AHFE2025), Vol. 199, 2025, 2354–2364
https://doi.org/10.54941/ahfe1007048

Team Cybersecurity Training: A Feasibility Study

Jonathan Hurter[1], Crystal Maraj[1], Bruce Caulkins[2], and Corey Wrenn[2]

[1]Institute for Simulation and Training, University of Central Florida, Orlando, FL, USA
[2]Cyber Florida, University of South Florida, Tampa, FL, USA

ABSTRACT

To maintain the critical functioning of the United States' computing infrastructure, a virtual-simulation range for cybersecurity training has been established to train cybersecurity teams. The present study's objective is to review the feasibility of this training range, using the approach of a self-report survey collected from trainees. Results show the usefulness of the range, while also revealing paths for improvement. Eighty-two cybersecurity professionals replied to a survey comprised of Likert items and open responses. Results from the Likert items showed positive signs of the training's usefulness. User's confidence in managing cyberthreats mainly increased or remained unchanged after training. Individuals mostly reported their teams accomplishing the scenario task without much confusion. For open responses, the most-liked aspects of training were its challenge, its realism, and the involvement of teamwork. Next steps are to improve the training range and extend research directions. Based on results, range improvements are to integrate relevant ethical scenarios, add new tools, lengthen the scenario, and give refresher training. Results of strong task cohesion and high collective orientation suggest issues with technical factors. Other next steps are to use the range to improve the personnel selection of cybersecurity professionals, and to capture performance and subjective perceptions repeatedly at team levels, while considering team age, size, and composition.

Keywords: Cybersecurity training, Cybersecurity-team survey, Cyberthreat management, Feasibility, Self-report survey, Teams, User perspectives

INTRODUCTION

In order to maintain the critical functioning of the United States' computing infrastructure, a virtual-simulation range for cybersecurity training has been established (using commercial off-the-shelf software) to train cybersecurity teams. This range, which is designed for sustainment training in cyberthreat detection and response, needs to cater to a diverse range of teams (in terms of size and composition), meet budget constraints, and allow flexibility in scenarios. The present study's objective is to review the feasibility of this training range, using the approach of a self-report survey collected from trainees to inform the quality of range scenarios. The significance of the study is to inform future developments for such a wide-reaching training range through human-factor evidence.

The training range was established by Cyber Florida, who continues its operation to train existing cybersecurity teams. The effort began in 2022, when Cyber Florida approached the University of Central Florida to conduct a Cyber Range Feasibility Study to support the need to create, operate, and maintain an active cyber range primarily for Florida's public-sector (i.e., SLTT – State, Local, Tribal and Territorial) organizations. The feasibility study found that a high-fidelity, cloud-based cyber range provided by a viable third-party vendor would provide the training environment necessary to fit this need.

Methods associated with traditional cybersecurity training have been categorized into lecture-based training, text-based training, video-based training, web-based training, combined cybersecurity training, simulation training, cyber ranges, virtual environments, and game-based training (Alnajim et al., 2023). The present effort is focused on a cyber range and its quality. Cyber ranges, which range across sectors (e.g., government and academic), not only support cybersecurity exercises and training courses (by providing an environment with services and tools), but can help build organizational resilience and cyber capabilities in a simulated environment, while allowing team training, building a winning incident response team, and emphasizing the idea of using realistic content and tools to prepare for realistic threats (Grigoriadis et al., 2021). Some authors have proposed a cyber-range training method to reduce the concerning skills gap for a cybersecurity workforce, with ranges replicating experience gained on-the-job within a safe environment (Cyber Range Project Team and the NICE Community, 2023). To investigate barriers and promoters for cybersecurity for white-collar employees, multiple cybersecurity experts were interviewed: the latter proposed supporting training with real life cases, using interactivity, using small groups trained by their role if possible, and having periodical-and-applied forms of training (Ergen, Ünal and Saygili, 2021). These considerations may transfer to training cybersecurity professionals for a cyber range, in our context. The study delves into the cybersecurity professional's perception of the current virtual-simulation range.

BACKGROUND

The background section highlights major themes related to the study facets: the survey elements of cyberthreat confidence, ethical organizational climate, collective orientation, team cohesion, and a transactive memory system are given elaboration, and relate to user perspectives. In the context of analyzing actual cybersecurity trainees, the authors are unaware of any other studies that implement the surveys we draw from, with some caveat to our confidence questions, as they were based on statements related to previous cybersecurity training, yet never given verbatim.

Cyberthreat Confidence

Confidence is a trust in one's capabilities to carry out a task and is considered a positive effect of training exposure. Cybersecurity training efforts using hands-on learning strategies (e.g., simulation and laboratory events) have

found positive feedback in the form of raised confidence with practical skills, as well as raised performance (Ismail and Alrabaee, 2024). The present study considers confidence in managing cyberthreats, similar to previous work (Chindrus and Caruntu, 2023).

Ethical Organizational Climate

Organizational climate amounts to a group's communal perception of the policies, practices, and procedures of an organization (Reichers and Schneider, 1990). Ethical organizational climate (EOC) is a specific climate in reference to ethics, or how one should behave within an environment. Kuenzi, Mayer and Greenbaum (2020) focused on a group of six formal organizational systems (e.g., decision-making and reward-and-punishment; Treviño and Nelson, 2017) to capture EOC views from a self-report survey: the EOC measure. Kuenzi, Mayer and Greenbaum (2020) found significant positive correlations between their EOC measure with both ethical leadership and collective moral identity. The EOC measure has also found to significantly and positively correlate with processes of knowledge sharing, at least for staff from universities (Moussa, 2020).

Collective Orientation

Collective orientation (CO) describes the values of someone who tends to pursue input from team members, who finds satisfaction from being part of a team, and who cares more about cooperation than domination (Driskell, Salas and Hughes, 2010). Driskell, Salas and Hughes (2010) operationalized CO by the Collective Orientation (CO) Scale, a self-report survey categorized by affiliation and dominance factors, where high affiliation and low dominance scores define someone with CO. The preference of CO has shown to positively relate to teamwork performance, in terms of correlations between two-person team performance (for tasks requiring interdependence), and the CO Scale (Driskell, Salas and Hughes, 2010). CO has been considered an attitudinal teamwork competency (in contrast to cognitive and skill competencies; Salas and Cannon-Bowers, 2000). In some relation to cybersecurity, information technology (IT) professionals did not differ from other professionals in the CO Scale, although people identifying as geeks were lower than non-geeks in the CO Scale (Bermack, 2014).

Team Cohesion

Work by Carless and de Paola (2000) defined team cohesion, via survey, from the context of an organizational work group, and found team cohesion as a multidimensional construct categorized by the three constructs of social cohesion (i.e., how much a team likes to interact socially), task cohesion (i.e., a team's commitment to task execution), and one's individual attraction to a group (i.e., a member's view of the team's social group being attractive). Out of the three constructs, team performance (from a supervisor rating) only related significantly to task cohesion. Past work using said survey (i.e., the Team Cohesion scale) for task cohesion and social cohesion focused on their

antecedents (such as team boundedness and organization tenure diversity) for co-located software development teams (Dey and M.P., 2020).

Transactive Memory System

The term transactive memory was coined by Wegner, Giuliano and Hertel (1985); a transactive memory functions equivalent to individual memory, with stored knowledge completely contained by a group of people. Transactive memory allows multiple minds to interdependently work as one mind, and is a repeatedly changing, core element of an intimate relationship (Wegner, Giuliano and Hertel, 1985). Liang, Moreland and Argote (1995) found teams trained together for a task (of assembling a radio) not only performed better than individually trained groups for the task, but were judged higher in cognitive factors manifest of a transactive memory system: memory differentiation (i.e., knowledge specialization), task coordination (i.e., smooth processing in teamwork), and task credibility (i.e., trusting another's knowledge). Lewis (2003) borrowed these factors as the foundation of the Transactive Memory System (TMS) Scale, which consists of a task-independent, self-report survey for specialization, credibility, and coordination factors. Using the TMS Scale, medical trauma teams training with a patient simulator increased significantly in credibility and coordination for four teams; and in specialization for two teams (Gardner and Ahmed, 2014). Post-training performance was also correlated significantly and positively with credibility and coordination.

METHOD

Participants, Procedure, and Equipment

Eighty-two cybersecurity professionals completed a self-report survey following their participation in a team-based cybersecurity scenario conducted within a virtual simulation range. Following each training simulation, participants (i.e., trainees) were provided with a link to a Qualtrics survey, which was generated through the approved presentation platform and shared by the instructor. The instructor's role was limited to distributing the link; they did not have direct access to any survey data. The cybersecurity-team survey was completed individually and was designed to take no more than 10 minutes to complete. The survey did not contain any personally identifiable information (PII).

Before the range scenario, trainees were given a scenario description: they were informed their superordinate organization had been notified that one or multiple systems found in the trainee's associated environment had been discovered to be in communication with infrastructure previously identified with carrying out malicious cyber-attacks. In terms of team objectives, instructions were given for identification (for devices and accounts compromised), containment and/or mitigation of any attack, eradication of any threat, and supplying an incident summary. The summary related to trainee's investigation and timeline of threat-actor actions. Participants were told to work as quickly as possible within an allotted 4 hours. Trainees were

also given simulation boundaries, including specific files and activities to ignore.

The network architecture of the simulated environment was a flat, segmented network with one firewall at the internet boundary, separate subnets for development users, accounting users, branch users, and security staff; one subnet for internal servers, and one demilitarized zone (DMZ) subnet with a mixture of open-source software and commercial off-the-shelf (COTS) software. System, security, and application logs for all servers, user workstations, and security appliances were forwarding logs to the security monitoring infrastructure. The tools provided to the trainees were Splunk, Security Onion, Palo Alto Firewalls, Vyatta Router/Switch, REMNUX, GHIDRA, CyberChef, and Wireshark.

Measurements: Self-Report Survey

The survey measurements were for demographics, cybersecurity confidence, EOC, CO, team cohesion, a TMS, and open-ended usability responses. Items were not aggregated at the team level. Demographic items were relevant to a cybersecurity background. The open-ended responses asked what each trainee liked most and least about their training, as well as what type of refresher training would be most useful to them, given the training they had just underwent. All other survey items were responded to on a five-point Likert-type scale, from *Strongly disagree* (1) to *Strongly agree* (5), except the cyberthreat confidence ratings, as explained next.

Work by Chindrus and Caruntu (2023) alluded to measuring confidence towards managing cybersecurity threats. Based on their idea, the question "What is your current level of confidence for managing real-world cybersecurity threats?" was developed in-house and rated from *Very low* (1) to *Very high* (5). Another question, "In comparison to before the simulation-based training scenario you just underwent, what is your current level of confidence for managing real-world cybersecurity threats?" was also developed with ratings from *Much lower* (1) to *Much higher* (5).

One statement for each of three factors from the EOC measure by Kuenzi, Mayer and Greenbaum (2020) were adapted by focusing on the ethical perspective of the trainee's cybersecurity team: (a) reward and punishment; (b) accountability and responsibility; and (c) decision-making. Two statements came from each of the affiliation and dominance factors of the CO Scale (Driskell, Salas and Hughes, 2010). Two task cohesion statements and one social cohesion statement were adapted from the Team Cohesion scale (Carless and de Paola, 2000). Three specialization items, two credibility items, and three coordination items were adapted from the TMS Scale (Lewis, 2003).

RESULTS & DISCUSSION

This section combines the results with their interpretations through discussion. Results show the usefulness of the range, while also revealing paths for improvement.

Demographics

A total of 82 individuals participated in this study. The most commonly reported current position among participants was cybersecurity analyst. After removing three ambiguous data points for tenure (i.e., two values for less-than-one year and one value for more-than-two years), the mean tenure for the remaining 79 participants' current positions was 2.298 years ($SD = 3.066$). Position duration ranged from 2 months to 40 years, indicating a mix of early-career and more experienced professionals.

Cyberthreat Confidence

Confidence with managing real-world cybersecurity threats, in comparison to before the simulation-based training scenario, was barely reduced (only eight of the participants reported any decrease in confidence). Perceived confidence in managing cyberthreats mainly unchanged (with 48 participants) or increased (with 26 participants). This suggests the training may have mainly reinforced what was already known, or the material was appropriate for strengthening the attitude of trainees. Next steps should focus on how confidence impacts performance.

Ethical Organizational Climate (EOC) Measure

The three statements for the EOC measure were, "Members of my organization's cybersecurity team receive positive feedback for making ethical decisions," "Members of my organization's cybersecurity team question authority if an unethical behavior occurs," and "When decisions are made, members of my organization's cybersecurity team discuss whether something is an ethical behavior to carry out." A minority of people (eight cumulatively for all statements) disagreed in some form with an existing EOC, a positive sign for existing organizations. However, several participants (56 cumulatively for all statements) neither agreed nor disagreed with the statements. The neutral trend may stem from ethical situations not occurring or participants having a murky viewpoint on ethical scenarios (i.e., unable to see all the details for a conclusive decision). To make explicit any ethical concerns, a next step is to enhance a scenario by integrating ethical elements relevant to the training.

Collective Orientation (CO) Scale

For most CO statements, many participants neither agreed nor disagreed, suggesting the statements were too vague in relation to their cybersecurity work experiences. Yet, a predominance (65 participants) agreed in some form with the affiliation statement, "I always ask for information before making any important decision," suggesting trainees typically were unafraid to communicate for critical information and had a team orientation for decision-making. A future consideration is to determine how cybersecurity teams within organizations differ in CO, when categorized by team size and position composition.

Team Cohesion Scale

The team cohesion statements had a mix of task and social cohesions. Half of all participants strongly agreed (and 37 agreed) with the statement, "Our team was united in trying to reach its goals for performance." This statement and the communication statement from CO relating to critical information gives signs of a strong team-reliance dynamic and shifts a focus to improving more technical training factors for the range. The response to the social cohesion statement, "Members of our team do not socialize together outside of work time," was close in mimicking a bell curve distribution, providing a range of responses, mainly within the range of *Agree* and *Disagree*. A sizeable portion of users may not have opportunities to formally socialize. The relation between social cohesion, personalities, and team performance within cybersecurity demands review.

Transactive Memory System (TMS) Scale

Many trainees disagreed (36 participants) in some form with the statement, "I had knowledge about an aspect of cybersecurity that no other team member had for the training scenario." Some people may already have known others' knowledge, thereby reducing the emphasis on exclusive specialization. However, the idea of needing specialized knowledge of different team members and knowing who they were showed some form of agreement via two different survey statements (with 70 and 63 participants, respectively): "The specialized knowledge of several different team members was needed to complete the training scenario's task," and "I knew which team members had expertise in specific areas related to the training scenario." There may be an overlap in knowledge between different roles, which helps team members easily switch roles and understand others. This nuanced view underscores a need to pool relevant knowledge to complete an objective, thereby giving team training further utility. To quantify specialization and allow access to the appropriate specialist for simulations, a repository of team-member certifications, such as digital badges, may be developed. A next step would be to understand how knowledge is distributed, in terms of specialization, based on the team size. Most participants (74) also agreed in some form for team-member credibility, via the statement, "I trusted that other members' knowledge about cybersecurity was credible." This solidification may have been enhanced from a common language of specialization. In addition, trainees mostly reported their teams accomplishing the scenario task without much confusion, with some form of disagreement (from 47 participants) with the statement, "There was much confusion about how our team would accomplish the training scenario's task," which deals with coordination. This suggests the scenario was mainly not too challenging to complete.

Open-Ended Responses

The trends found from the open-ended responses are shown in Table 1 (not all participants provided feedback). The most-liked (i.e., positive) aspects of training were its challenge, its realism, the experience, and the involvement of teamwork; these suggest training advantages, and underscore feasibility

aspects of the range's operation. Trends for the least-liked (i.e., negative) aspects of training were for the environment, tools, and the amount of time given; and trends for useful refresher training types were for Splunk and Security Onion. Next steps for improving the range are to add new tools, to provide refresher training for Splunk and Security Onion, and to lengthen the scenario to increase simulation fidelity.

Table 1: Trends from the open-ended responses.

Trend (Percentage)	Example
	Positive responses ($N = 73$)
Realism (19%)	"It seemed pretty realistic, with lots of false positive events we'd have to sift through."
Team (18%)	"Working with my team on solving the issue."
Experience (8%)	"I appreciate the Hands on experience being that I am a Pc support member"
Challenge (7%)	"I liked the challenge. I think we need to be trained and tested more on some things."
	Negative responses ($N = 64$)
General tools (28%)	"The tools. It's not tools we use; we don't know how to use them to find what we need."
Specific tools (23%)	"Having to learn tools / linux commands on the fly."
Environment (9%)	"Unknown environment with very little info given."
Time (9%)	"Amount of time for the exercise. Should have additional time for working through the exercise."
	Refresher-training responses ($N = 29$)
Splunk (31%)	"Splunk training. Each of us are trained in Palo Alto firewall admin roles, so Splunk would complement that well."
Security Onion (11%)	"a refreshed on efficiently utilizing each tool (Security Onion, Splunk, Firewalls) would always be beneficial with analysis and interpreting findings."

Limitations

The study was constricted by not tracking team membership and only focusing on post-scenario responses. The responses from trainees, such as for a TMS, were not validated through an additional method, such as observer ratings. Also, a longer scenario, which could affect fidelity, may also allow teams to evolve and thus affect their perspectives.

CONCLUSION

Overall, the training appeared to have a positive effect on the trainees' confidence, with only a minor reported decrease in confidence for cyberthreat management. Most trainees either remained steady or experienced an

increase. Participants demonstrated strong task cohesion and a willingness to communicate critical information, suggesting a collaborative and mission-focused culture.

However, the lack of opportunity for formal socialization may impact the broader team dynamics. Neutral responses regarding ethical behavior may indicate that ethical situations are absent or unclear. The potential for overlap in roles may promote adaptability and mutual understanding within a team. Feedback highlighted appreciation for the realistic, team-based nature of the training, though dissatisfaction with the tools used was noted. Participants expressed interest in future refresher training, particularly involving platforms like Splunk for continued, practical skill development. The results show strengths related to the range and support the range's feasibility, despite some drawbacks.

Implications

The research serves to inform stakeholders, including managers and their technical cybersecurity teams. For trainers, the inclusion of realistic and challenging team scenarios had a positive effect on trainees, suggesting fidelity as a strength. Managers and their organizations may benefit from this strength, due to its effect on their technical cybersecurity team. Trainees may have also become more confident managing cybersecurity threats due to better understanding their own gaps, such as procedures, which in turn could also benefit organizations.

Future Directions

Future studies should explore how personality traits, such as being organized or open to new ideas, affect teamwork and communication in cybersecurity settings. Team size, age, and composition may also influence how well teams perform and can be explored. To better understand training impact, performance should be measured repeatedly alongside changes in confidence, teamwork, and ethical decision-making. Performance includes files protected, speed of recovery, tool-actions frequency, and the amount of guidance given from observers. Training scenarios could be improved by including ethical challenges and making them longer to feel more realistic. Survey questions should be adjusted to reduce neutral answers, such as by asking for explanations or changing how options are presented, to gather clearer and more useful feedback. A future goal is to improve personnel selection. One may use data gathered from the training to reverse-engineer ideal candidates for certain cybersecurity positions. The perceptions from the present study may be fused with performance to better understand mappings to the National Initiative for Cybersecurity Education (NICE) Framework (https://www.nist.gov/nice/framework). The iterative nature of the range offers a method to increase the dataset size and develop a profile of a professional, improving personnel-selection science.

REFERENCES

Alnajim, A. M., Habib, S., Islam, M., AlRawashdeh, H. S. and Wasim, M. (2023) 'Exploring cybersecurity education and training techniques: A comprehensive review of traditional, virtual reality, and augmented reality approaches', *Symmetry*, 15(12). https://doi.org/10.3390/sym15122175.

Bermack, B. (2014) *Interpersonal Relationships and Life Satisfaction Among Information Technology Professionals* [Dissertation], Massachusetts School of Professional Psychology. Available at: https://www.proquest.com/docview/1624877416?pq-origsite=gscholar&fromopenview=true&sourcetype=Dissertations%20&%20Theses.

Carless, S. A. and De Paola, C. (2000) 'The measurement of cohesion in work teams', *Small Group Research*, 31(1), pp. 71–88. https://doi.org/10.1177/104649640003100104 .

Chindrus, C. and Caruntu, C. F. (2023) 'Securing the network: A red and blue cybersecurity competition case study', *Information*, 14(11). https://doi.org/10.3390/info14110587.

Cyber Range Project Team and the NICE Community (2023, September) 'The Cyber Range: A Guide', National Institute for Cybersecurity Education. Available at: https://www.nist.gov/system/files/documents/2023/09/29/The%20Cyber%20Range_A%20Guide.pdf.

Dey, C. and M. P., G. (2020) 'Impact of team design and technical factors on team cohesion', *Team Performance Management: An International Journal*, 26(7/8), pp. 357–374. https://doi.org/10.1108/TPM-03–2020-0022.

Driskell, J. E., Salas, E. and Hughes, S. (2010) 'Collective orientation and team performance: Development of an individual differences measure', *Human Factors*, 52(2), pp. 316–328. https://doi.org/10.1177/0018720809359522.

Ergen, A., Ünal, A. N. and Saygili, M. S. (2021) 'Is it possible to change the cyber security behaviours of employees? Barriers and promoters', *Academic Journal of Interdisciplinary Studies*, 10(4), p. 210. https://doi.org/10.36941/ajis-2021–0111.

Gardner, A. K. and Ahmed, R. A. (2014) 'Transforming trauma teams through transactive memory: Can simulation enhance performance?', *Simulation & Gaming*, 45(3), pp. 356–370. https://doi.org/10.1177/1046878114547836.

Grigoriadis, A., Darra, E., Kavallieros, D., Chaskos, E., Kolokotronis, N. and Bellekens, X. (2021) 'Cyber ranges: The new training era in the cybersecurity and digital forensics world', in Akhgar, B., Kavallieros, D. & Sdongos, E. (eds.) *Technology development for security practitioners*. Cham: Springer, pp. 97–117. https://doi.org/10.1007/978–3-030–69460-9_6.

Ismail, M. and Alrabaee, S. (2024, October) 'Empowering future cyber defenders: Advancing cybersecurity education in engineering and computing with experiential learning', in *2024 IEEE Frontiers in Education Conference (FIE)*. IEEE, pp. 1–9. https://doi.org/10.1109/FIE61694.2024.10892990.

Kuenzi, M., Mayer, D. M. and Greenbaum, R. L. (2020) 'Creating an ethical organizational environment: The relationship between ethical leadership, ethical organizational climate, and unethical behavior', *Personnel Psychology*, 73(1), pp. 43–71. https://doi.org/10.1111/peps.12356.

Lewis, K. (2003) 'Measuring transactive memory systems in the field: Scale development and validation', *Journal of Applied Psychology*, 88(4), pp. 587–604. https://doi.org/10.1037/0021–9010.88.4.587.

Liang, D. W., Moreland, R. and Argote, L. (1995) 'Group versus individual training and group performance: The mediating role of transactive memory', *Personality and Social Psychology Bulletin*, 21(4), pp. 384–393. https://doi.org/10.1177/0146167295214009.

Moussa, A. (2023) 'Committed to ethics: How ethical leadership and ethical climate foster knowledge sharing in private higher education institutions', *Journal of Educational Studies and Multidisciplinary Approaches*, 3(2), pp. 133–150. https://doi.org/10.51383/jesma.2023.73.

Reichers, A. E. and Schneider, B. (1990) 'Climate and culture: An evolution of constructs' in Schneider, B. (ed.) *Organizational climate and culture*. San Francisco, CA: Jossey-Bass, pp. 5–39.

Salas, E. and Cannon-Bowers, J. A. (2000) 'The anatomy of team training', in Tobias, S. & Fletcher, D. (eds.) *Training and retraining: A handbook for businesses, industry, government and military*. Farmington Hills, MI: Macmillan, pp. 312–335. Available at: https://archive.org/details/trainingretraini00tobi/page/314/mode/2up.

Treviño, L. K. and Nelson, K. A. (2017) *Managing business ethics: Straight talk about how to do it right*. 7th edn. Hoboken, NJ: John Wiley & Sons.

Wegner, D. M., Giuliano, T. and Hertel, P. T. (1985) 'Cognitive interdependence in close relationships', in *Compatible and incompatible relationships*. New York, NY: Springer, pp. 253–276. Available at: https://archive.org/details/compatibleincomp0000unse/page/n9/mode/2up.