IST-153 Workshop on **CYBER RESILIENCE**

Measuring Cyber Defense Team Resilience (Technical Paper)

Brad Lufkin[1,2], Diane Henshel[1,*], Gary Deckard[1,2]
[1]Indiana University, Bloomington, IN 47405
[2] Atterbury-Muscatatuck Center for Complex Operations, Camp Atterbury, Indiana, USA 46124

[*]Communicating Author
Email: dhenshel@indiana.edu Phone: (812) 345-0944

1 July 2017

1. INTRODUCTION

Organizations are increasingly utilizing a team approach to secure their enterprise information systems. This approach has been used by the government and particularly the US Department of Defense in various permutations for many years and has become more common in private and commercial entities as well (Mjelde et al, 2016). Once a security team has been assembled and trained, a significant challenge is personnel turnover. Understanding the impact of the loss of one or more members of the team is a critical component of readiness. Furthermore, it is vitally important to understand the impact of team composition and dynamics when forming and managing a security team.

Protecting the nation from cyber attacks is becoming an increasingly important component of overall national defense. With threats and attacks becoming progressively more sophisticated, it is critical to heighten cyber defenders' capabilities and to support the formation of well-crafted teams. Considerations of design of cyber defense teams are beginning to be studied (Gutzwiller et al. 2015). Within the Army National Guard, Defensive Cyber Operations Elements (DCOE) exist in each of the 54 states and territories as an "emergency response team" that can be used to supplement full-time personnel if needed for a cyber incident. These units consist of eight to ten Soldiers specially trained in cybersecurity.

Just as physical defense requires the effective use of highly trained individuals and teams, successful cybersecurity protection requires sufficient technical knowledge and skills from individuals as well as intelligent team design. Both team composition and dynamics directly funnel into how well assembled DCOEs perform and maintain performance in response to negative impacts such as losing a team members or the abilities for a team member to wholly contribute his or her full skillset and expertise. There is frequently a high degree of turnover within DCOEs, so when one individual leaves, it is imperative that the team is still ensured to have the skills that the departed team member took with them; this requires a certain degree of redundancy to be built into the team design.

The traditional paradigm of resilience when discussing teams is approached from a perspective of psychological trauma and stress in teams such as medical workers, firefighters, law enforcement, competitive sports teams, business organizations, and military personnel (Durkin et al., 2000; Gillespie et al., 2007; Paton et al., 2008; Morgan et al, 2013; Gomes et al, 2014; Rodríguez-Sánchez et al., 2015) When discussed in a sports context, resilience is generally inferred to mean the ability of the team to adapt and overcome adversity. In the context of cybersecurity teams, resilience may be taken as a synonym for "robustness" rather than as the strict definition of "resilience" as the ability of a body to return back to its original state following a disturbance. In this context of DCOEs, we are evaluating the ability of the team to continue performing at their current level; more specifically, we are evaluating the *potential* ability of the team to continue performing at their current level when one or more member is removed, based on the composition of individuals' observable characteristics. Since we are unable to run multiple iterations of the same exercise with the various permutations of team members, we must make theoretical predictions of how a less-than-complete team would perform based on observable characteristics.

There is currently no literature published on this type of team resiliency in the context of cybersecurity teams, so many of the analytical decisions made during the construction of this paper were made on the grounds of reasonable logic. The goal of this paper is to present an exploratory analysis paradigm for DCOE resilience that can be expanded and improved upon to better understand the role that individual characteristics and team dynamics play. The following sections detail the data collection process, the analytical methods used to quantify the metrics incorporated into the resilience analysis, the process of developing the heat map resilience summaries for each team, an overview of the results for the initial analysis, a discussion of the implications of this work, and a brief discussion of future work.

2. METHODS

2.1 DATA COLLECTION

The data used in this analysis comes from the Army National Guard-sponsored collective training event, Cyber Shield; Cyber Shield 2016 (CS16) took place from 18-30 April 2016 at Camp Atterbury, Indiana. The exercise framework serves as the primary annual event for the National Guard DCOEs. The event is comprised of one week of classroom training followed by one week of Red Team-Blue Team gameplay on virtualized networks.

This analysis explores one main avenue of thinking to frame team resilience within the context of DCOEs; we complete a hypothetical removal analysis using individual characteristics aggregated by team. Data from this analysis comes from a pre-event survey administered at CS16. All CS16 participants were asked to voluntarily complete a pre-event survey of 118 questions covering demographic information, employment, commercial certifications, military training, education, a self-assessment for cyber defense, passion and self-direction, military exercise-related information, security knowledge (formatted as quiz questions), computing habits, and some initial metrics for team resilience and maliciousness. While there are, of course, other team and individual characteristics that impact team proficiency and resilience, this survey was created through a comprehensive and iterative drafting process with cyber experts and representatives from partner academic institutions (originally derived from Deckard and Camp, 2016). 509 Individuals completed this survey in 2016, including 285 blue team members.

Resilience Questions: As part of the team resilience section, respondents were asked to rank a set of eight individual characteristics by importance to team resilience. Individual characteristics from the pre-event survey were classified as contributing to an individual's "importance" as a member of the DCOE. For instance, an individual who possesses certain certifications will contribute particular skills to the team's overall potential capabilities. While we were limited by the survey questions in the number and types of characteristics we could include, we completed a customized hypothetical analysis using these variables to determine the impact that one or more individuals leaving would have on the team.

2.2 ANALYSIS

This analysis is limited in scope to the data that was obtained during CyberShield 2016. We must conduct theoretical, predictive analyses that provide guidance as to how a team *would have* performed with each possible set of team members since timing and inevitable threats to internal validity prevent setting up an exercise to assess each team responding to similar injects with every possible permutation of team composition. Even in a situation where we set up our own teams for testing, there is no way of having a counterfactual for each instance.

To determine a subset of qualities from the pre-event expertise survey that we can reasonably claim affect team resilience, we extracted four main categories of "competency metrics" from the dataset: (1) education, (2) security knowledge, (3) certifications, and (4) experience. All four of these categories are linked to individual performance, and thus overall team resilience. Within each of these categories, we evaluated multiple individual variables at the team level.

1. Education
    a. Percentage of people on the team who have completed a degree above high school
    b. Percentage of people on the team who have an IT-specific degree
2. Security Knowledge
    a. The average cyber security knowledge score of the team
    b. The average physical security knowledge score of the team

    c. Percentage of people on the team who correctly answered at least 5 of the 6 cyber security knowledge questions correctly
    d. Percentage of people on the team who correctly answered at least 5 of the 6 physical security knowledge questions correctly
3. Certifications
    a. Percentage of certifying organizations uniquely possessed[1] by the team members
    b. Percentage of specific certifications uniquely possessed by the team members
4. Experience
    a. Percentage of people who work in information technology sector
    b. Percentage of the ideal total number of team years worked in information technology sector[2]
    c. Percentage of people who work in information security sector
    d. Percentage of the ideal total number of team years worked in information security sector

The competency metrics included in this analysis were not included simply for the intent of being a reductive attempt at capturing all relevant individual characteristics and qualities. Individuals are complex and cannot be entirely described by the set of quantitative metrics used here, but we can use numbers to guide our analysis and thought processes while providing some insight into what characteristics may lead to more resilient teams. While this analysis does not wholly represent individual or teams with these characteristics, this analysis provides a foundation and structural paradigm for future analyses regarding DCOE resilience.

Multiple steps were followed to determine the final suite of metrics as well as a single metric that effectively represents overall team resiliency.

Step 1: Find the value for each of the competency metrics under each team permutation. The number of people on the team who possess an IT-specific degree was found for the full team, as well as when each person was removed and when various combinations of people were removed from the team. In other words, the number of people on the team with an IT-specific degree was found when only person

[1] "Uniquely possessed" refers to the ability of multiple individuals on the team to possess the same certification. For instance, if person A and person B both possess certification X and person A is removed from the team, the team can still be said to possess certification X. Is it not until all of the individuals from the team who possess that certification (in this case person A and person B), that it can be said that the team no longer possesses certification X. This reasoning accounts for a certain degree of redundancy in the overall skillset of the team; an individual can be removed, but the team could still possess some of that individual's expertise through another team member.

[2] The "ideal" number of team years worked in a sector was found by determining the collective number of years that the members of the team have been 18 years old. This assumes that every individual worked in that particular sector their entire adult life. The actual number of collective years worked in this sector was then divided by this theoretical ideal.

1 was removed, when only person 2 was removed, when only person 3 was removed, and so on; it was further calculated when person 1 and 2 were removed, when person 1 and 3 were removed, when person 1 and 4 were removed and so on. All of the values for each of these metrics only came from blue team members to ensure that we only captured the characteristics that reasonably predict performance for defending teams. Note that these competency metrics were selected without regard to whether or not they are significantly correlated with team proficiency.[3]

Table 1 The combinations of individuals that were theoretically removed from the team for this analysis for an example 5-person team.

Full Team	1	2	3	4	5
		1, 2	1, 3	1, 4	1, 5
			1, 2, 3	1, 2, 4	1, 2, 5
				1, 2, 3, 4	1, 2, 3, 5
					1, 2, 3, 4, 5

While this analysis does not truly capture every single team composition possible from the team members available, it still provides insight into the impact of team member loss. Using tetrahedral numbers and deduction, the true number of combinations possible from a team of size N was found to be:

$$\mathrm{P}(N) = \frac{(N^3 + 5N)}{6}$$

Once these permutations were determined for each team depending on the team size, then the actual values for the competency metrics were calculated. (See appendix A for pattern of team member removal using a comparison to final result heat maps.) Putting these metrics in relative percentage terms accomplishes two main goals: (1) it allows for comparison across teams, and (2) it normalizes the units for and importance of each metric.

Step 2: Determine a single resiliency metric (the “index”) for each team permutation. For step 2, the percentages found were then summed for each team permutation; in other words, the relative competency values were added for every instance where person 1 was removed, for every instance where person 2 was removed, and so on. These indices represent the total “competency” that these team permutations have in relation to the actual, fully staffed blue team.

[3] Proficiency metrics for CS16 were noticeably incomplete and weak, and thus, there is little certainty and foundation for including specific competency metrics over others. This analysis trumped any significance findings and went purely with theoretical reasoning. If this analysis is done in future years, significance of potential competency metrics should be determined *a priori*.

Step 3: Determine the "index difference" for each team permutation. For step 2, the index for the full team was subtracted from each of the indices for each team permutation. These index differences represent the meta-relative team competency for each team permutation; in other words, the variability in competency that each permutation has in relation to the full team.

Step 4: Determine the suite of single value metrics that describe overall team resiliency. Three metrics were determined: (1) the total sum of the index differences[4], (2) the average index difference, and (3) the total sum of the index differences divided by the number of team members were found. Each of these values is a different representation of the same thing – overall team resiliency as determined by how invariable the sum of the teams' competency metrics is.

Step 5: Determine the "index percentage" for each team permutation. The values found in step 3 were converted to a percentage relative to the index for the original, full team (step 2 to 5). This converts the team index, which represents total team "competency," to a percentage of that total competency that remains when one or more individuals are removed from the team. This values are presented as a heat map for each team for easy visualization about how the team is generally impacted as more members are progressively removed from the team and about which specific individuals may be more "important" to the team (i.e., their removal heavily impacts the team). The change in index percentage when an individual person is removed quantifies how "important" that individual is to the team, considering all competency metrics used in this analysis – the lower the index once the individual is removed, the more "important" the individual is.

As part of this Hypothetical analysis, we would also be able found the relative prominence (not necessarily importance) of each competency metric that we selected to use. By looking at the full teams' actual value for each metric compared to the original blue team value for that metric (i.e., percentage; step 2), we would be able to determine which characteristics are most fully possessed by the members of the team and which are least fully possessed by the members of the team. Those characteristics that are either held by most of the team members or collectively covered by many of the team members are the characteristics that will be least impacted by the removal or one or more team members. For instance, if 90% of individuals on the team possess and IT degree, and 20% of individuals work full-time in the information technology sector, it follows that the team will feel more of an impact if a team member who works full-time in the IT sector were removed than if an individual who possessed an IT degree were removed. In other words, those characteristics that are "rarer" among the members of a team are more

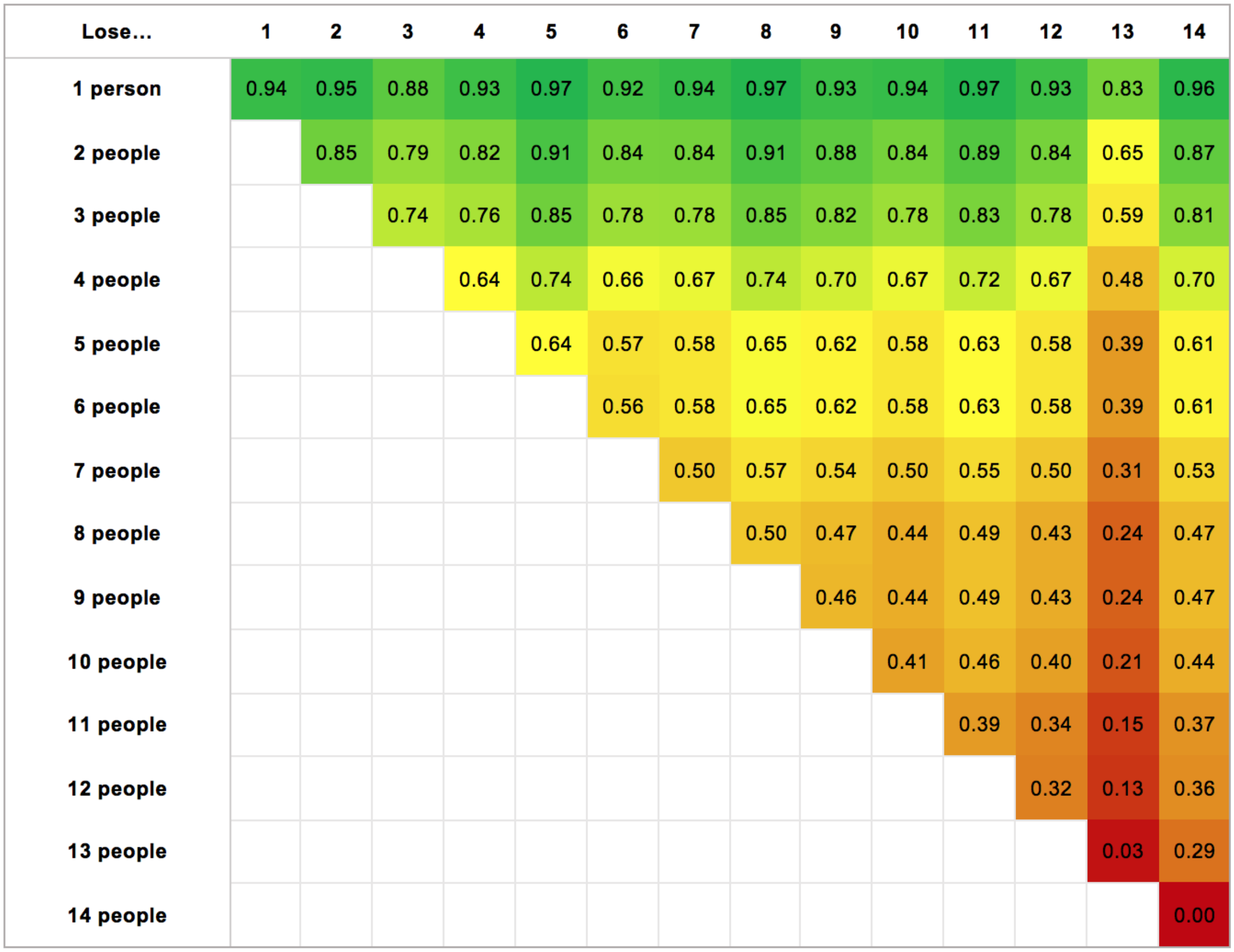
[4] We do not want to do the total sum of the index differences squared because we want to include directionality in the impact of removing people. If removing someone from the team makes them "better" (e.g., average security knowledge score increases when an individual is removed), then we want to capture that.

“valuable,” and the team will feel more of an impact when those characteristics are lost (i.e., the team is less resilient with respect to “rarer” characteristics). This thinking does not inform which individual characteristics have the greatest driving force behind team resilience due to some inherent qualities of those characteristics; rather, this thinking reveals that the criticalness of characteristics depends on the frequency of possession.

3. RESULTS

Results are presented as heat maps, showing the resilience index percentages across all team permutations; green indicates a more intact team after the removal of one or more individuals, and red indicates a less intact team. Further, the magnitude of differences in the resilience index percentage are shown as histograms which allows for easy comparison of team resilience to the full team. The higher the bar, the less critical that specific individual is to overall team resilience; the higher the bar, the stronger (i.e., better, healthier, sturdier) that team remains. See figure 1 for an example team heat maps.

Figure 1 Resilience Index Percentages for Removal of Each Blue Team Member Permutation (team 3)



Lose...	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1 person	0.94	0.95	0.88	0.93	0.97	0.92	0.94	0.97	0.93	0.94	0.97	0.93	0.83	0.96
2 people		0.85	0.79	0.82	0.91	0.84	0.84	0.91	0.88	0.84	0.89	0.84	0.65	0.87
3 people			0.74	0.76	0.85	0.78	0.78	0.85	0.82	0.78	0.83	0.78	0.59	0.81
4 people				0.64	0.74	0.66	0.67	0.74	0.70	0.67	0.72	0.67	0.48	0.70
5 people					0.64	0.57	0.58	0.65	0.62	0.58	0.63	0.58	0.39	0.61
6 people						0.56	0.58	0.65	0.62	0.58	0.63	0.58	0.39	0.61
7 people							0.50	0.57	0.54	0.50	0.55	0.50	0.31	0.53
8 people								0.50	0.47	0.44	0.49	0.43	0.24	0.47
9 people									0.46	0.44	0.49	0.43	0.24	0.47
10 people										0.41	0.46	0.40	0.21	0.44
11 people											0.39	0.34	0.15	0.37
12 people												0.32	0.13	0.36
13 people													0.03	0.29
14 people														0.00

Individuals' Impact: One may assess the individual impact of each person being removed by looking at the top row of the heat map. This provides some information, but is not perfect; there are interaction effects when multiple people are removed at the same time that might be greater than or less than the sum of their parts. For instance, when removed alone, person A could possess a certain certification, but person B could possess that certification as well and allow the team to be unaffected by the removal of person A. But if both of person A and B are removed, then the team is left without the certification. Thus, this method does not evaluate the complete impact of individuals' potential removal from the team, but provides merely a proxy value for that impact. The true importance of that first person, however, is not captured when *only* they are removed; it is found when they are removed in conjunction with every combination of other team members.

Competency Metric Importance: Due to the fact that the metrics used were not proprietarily selected for the purpose of completing this analysis, normalizing these specific metrics (in this analysis) such that each variable carries the same amount of weight in determining resilience is impossible. While all efforts were made to normalize using percentages of original blue teams, the inherent characteristics of the competency metrics as they were collected prevent true equal weighting. For instance, comparing the percentages in step 2a/2b of cyber security knowledge and number of specific certifications held is imbalanced because of the total number of options that fall within each metric. Individuals have the opportunity to correctly answer 6 questions in the cyber security knowledge section, whereas they have the opportunity to "correctly" possess 368 unique certifications. The inherent assumption that separates these two competency metrics is that all 6 of the cyber security knowledge questions were predetermined to be theoretically relevant to proficiency, whereas that assumption does not hold for all 368 of the unique certifications. The original intent of collecting data on these 368 metrics was to aid in the determination of which were actually relevant (read: significant) in predicting team proficiency; thus there was bound to be extraneous, irrelevant certifications included with respect to this resiliency analysis. Further, it is far more reasonable for an individual to answer all of the cyber security knowledge questions correctly than for an individual to possess all 368 certifications; there is more effort required, and perhaps more relevant knowledge required, for an individual or team to achieve 100% on certifications than security knowledge.

While each of the metrics in the suite that holistically describes team resiliency (step 5) reveals important information about each team, the average index difference is the most comparable across teams. The lower the number, the more resilient the team.

Table 2 shows that teams 1, 14, and 27 have the lowest three average index difference values when comparing each theoretical team composition to the original blue team. This pattern indicates that these teams could be qualified as the "most resilient" according to our assessment method.

Table 2 Single metrics describing team resiliency (abridged; derived in step 5).

Team	Number of Team Members	TOTAL SUM INDEX DIFFERENCE:	AVERAGE INDEX DIFFERENCE:	TOTAL SUM INDEX DIFFERENCE / # of team members:
1	8	-127.97	-3.55	-16.00
2	8	-187.13	-5.20	-23.39
3	14	-471.78	-4.49	-33.70
4	11	-308.13	-4.67	-28.01
5	9	-188.46	-4.19	-20.94
…	…	…	…	…
14	11	-226.99	-3.44	-20.64
…	…	…	…	…
27	3	-23.83	-3.97	-7.94
…	…	…	…	…
30	12	-362.13	-4.64	-30.18

4. DISCUSSION

Formulating a single value that represents team resiliency without conducting real-world experiments required ample theoretical foundation and creative problem solving. In this hypothetical removal analysis, we are able to assess predicted team resiliency without the time, management, or monetary costs of conducting true experimentation, but using data collected during a red team-blue team training exercise.

A number of factors must be considered when viewing the results of this analysis:

1. The competency metrics selected in this analysis were chosen from a pre-existing dataset that was not proprietarily designed for resiliency analysis. In future analyses, desired individual characteristics will be determined prior to data collection. This is not to say, however, that the competency metrics used in this analysis are not appropriate; for instance, certifications provide insight into overall team qualifications for certain cyber realms, and thus should be included as a metric in future data collection. Further, these variables are not necessarily the optimum metrics for quantifying the characteristics key to defining team resilience in cyber defense teams. It is reasonable to assume that education, knowledge, and certifications/trainings contribute to team resilience (i.e., robustness), but other observable and unobservable characteristics that are not captured by these metrics are likely to be relevant. Further, other metrics might better describe education within the context of team resilience. We recommend that surveys completed in conjunction with Cyber Shield and other defense team training exercises capture more metrics

specifically hypothesized to contribute to team resilience. There is the opportunity with Cyber Shield to pair the collected data with team proficiency, which can lead to meaningful analysis determining the most important characteristics that lead to more resilient teams.

2. In certain situations, the removal of one or two team members could increase the total index for the team in the permutation. This might happen when either of the two knowledge scores are averaged when that person or combination of people are removed from the team. If the individual's score is lower than the current team average, then the team value for that competency metric will increase once removed; depending on the effect felt by the other competency metrics, this could increase the overall resilience index. It may be difficult to rationalize a team being "better" once a team member is removed. The metrics selected may also be being analyzed incorrectly such that the analysis overemphasized the weight an individual metric carries in determining predicted team resiliency and devalues the holistic contribution that the individual has to the team. This method condenses the entire influence that a person has down to a few metrics which may pose a threat to internal validity.

Taking into consideration the caveats associated with the ongoing development of this resiliency analysis paradigm, there are still important and poignant conclusions that may be drawn from the results.

Inherent in team resilience is team size. Looking at the heat maps, the teams degrade very quickly when they only have a few people, while larger teams result in a much smoother gradient of index percentages. Teams with more people can understandably maintain performance more readily and for a longer period of time when threatened with the removal of one or more team members. As the number of people increases in the team, the index percentage becomes more and more steady (i.e., less variable) among the removal of the different people (see team histograms). When there are fewer people, index percentages become much more stochastic. In short, teams with more people can afford to lose team members more easily. Further, the magnitude average index difference, which represents team resilience as a single number, is partially a function of the number of people on the team; because the total sum index difference rises with the number of individuals on the team, it follows that the average of the sum index differences across all team permutation.

Team resilience is fundamentally difficult to evaluate. Predictive analysis surrounding potential team composition (and the characteristics embedded in that composition) is difficult to evaluate without conducting experimental evaluations on specific teams. Without conducting performance tests on every possible team composition, team resilience and proficiency must be predicted using known factors; even in such an experimental environment, one must take into account maturation effects and other threats to internal validity such as learning artifacts resulting from repeated trials of the same task. It is even harder to generalize resilience assessments on specific characteristics. To truly evaluate the impact that the possession of a specific characteristic will have on team resilience, identical teams would have to be formed except for the characteristic being evaluated, and intricate experiments must be conducted. This analysis, however, begins to evaluate team resilience as well as possible given the confines of the existing data set as well as the experimental and quasi-experimental constraints.

The importance of individual characteristics depends on how common the characteristic is for the team. While expertise is obviously important to the performance of a DCOE, it is not the inherent characteristics of metrics that are important in a discussion of resilience. A competency metric could objectively be the most important skill for an individual to possess, but if every person on a team possesses that metric (breadth of coverage of a skill), that particular metrics will not be as important to team resilience; if an individual with that characteristic leaves the team, the impact will be minimal because many other people on the team have the characteristic. Ultimately, an interaction between expertise importance and appearance frequency on team will represent overall importance to team resilience.

Future Research and Conclusions

The main goal of future iterations of this research will be to expand upon the analytical framework proposed here and to determine the specific individual characteristics that are most influential in determining resiliency.

To improve similar analyses in the future, we must standardize the competency metrics such that they are all presented in the same units and easily comparable across individuals and teams. In this paper, percentages were used to compare metrics such as specific certifications held by team members, average knowledge scores, and number of individuals holding an IT degree – this technique was used in an attempt to overcome the problem that the unit of analysis was not consistent across metrics. If future work preemptively determines which metrics are of specific concern to team resilience, the positive effect will be twofold: (1) there will be greater control over units of analysis and (2) characteristics that are truly of interest will be evaluated rather than already collected characteristics that must be repurposed and shoehorned to fit into this analysis.

Further, a goal of future research will be to better evaluate individual impact on team resilience. By collecting individual characteristics of potential team members prior to team assembly, the hypothetical contribution of each individual can be calculated. This would allow leadership who is assembling a team to craft a team that is minimally impacted by the removal of any individual team member as quantified through compositional analysis. This evaluation, being more comprehensive than the analysis completed here, will require a look at every possible team permutation; as described above, time and resource limitations prevented this level of analysis to completed for this report.

BIBLIOGRAPHY

Deckard, GM, and Camp, LJ, "Measuring efficacy of a classroom training week for a cybersecurity exercise." 2016 IEEE International Symposium on Technologies for Homeland Security (HST), IEEE, pp 1-6.

Durkin, J., & Bekerian, D. A. (2000). Psychological resilience to stress in firefighters. *University of London, UK*, 3-6.

Gillespie, B. M., Chaboyer, W., Wallis, M., & Grimbeek, P. (2007). Resilience in the operating room: Developing and testing of a resilience model. *Journal of advanced nursing*, *59*(4), 427-438.

Gomes, J. O., Borges, M. R., Huber, G. J., & Carvalho, P. V. R. (2014). Analysis of the resilience of team performance during a nuclear emergency response exercise. *Applied ergonomics*, *45*(3), 780-788.

Gutzwiller, R. S., Fugate, S., Sawyer, B. D., & Hancock, P. A. (2015, September). The human factors of cyber network defense. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 59, No. 1, pp. 322-326). Sage CA: Los Angeles, CA: SAGE Publications.

Mjelde, F. V., Smith, K., Lunde, P., & Espevik, R. (2016). Military teams–A demand for resilience. *Work*, *54*(2), 283-294.

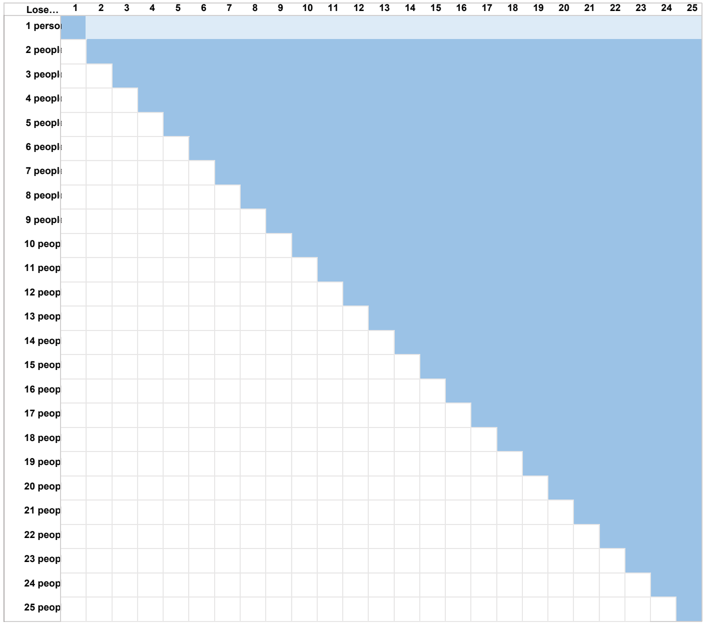
Morgan, P. B., Fletcher, D., & Sarkar, M. (2013). Defining and characterizing team resilience in elite sport. *Psychology of Sport and Exercise*, *14*(4), 549-559.

Paton, D., Violanti, J. M., Johnston, P., Burke, K. J., Clarke, J., & Keenan, D. (2008). Stress shield: a model of police resiliency. *International Journal of Emergency Mental Health*, *10*(2), 95-107.

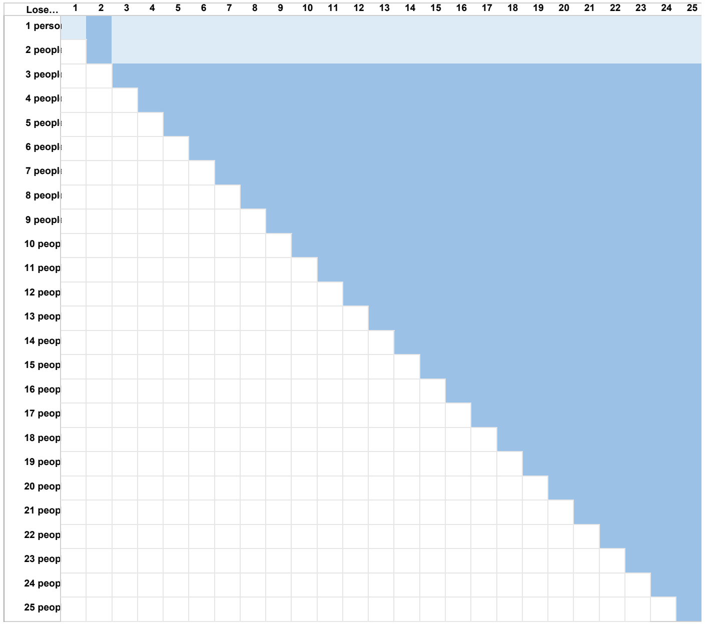
Rodríguez-Sánchez, A. M., & Vera Perea, M. (2015). The secret of organisation success: a revision on organisational and team resilience. *International Journal of Emergency Services*, *4*(1), 27-36.

APPENDIX A

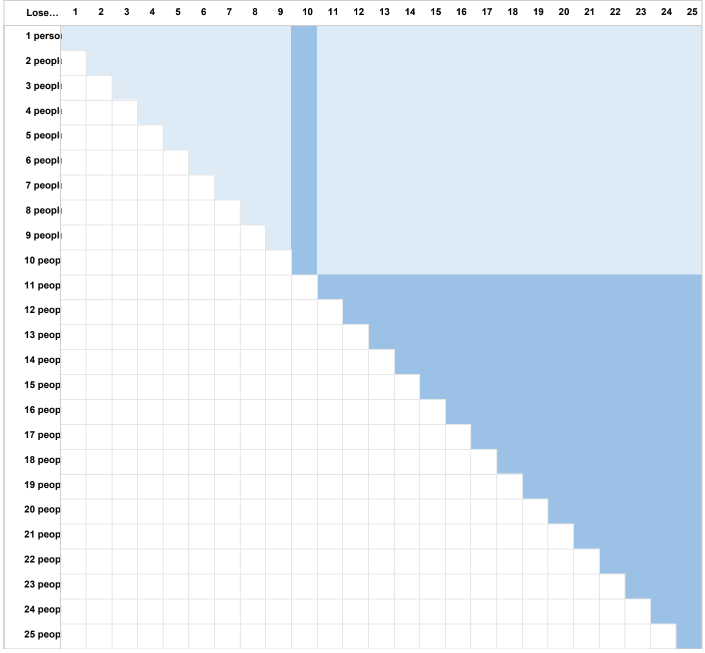
All cells in which person 1 is removed from the team



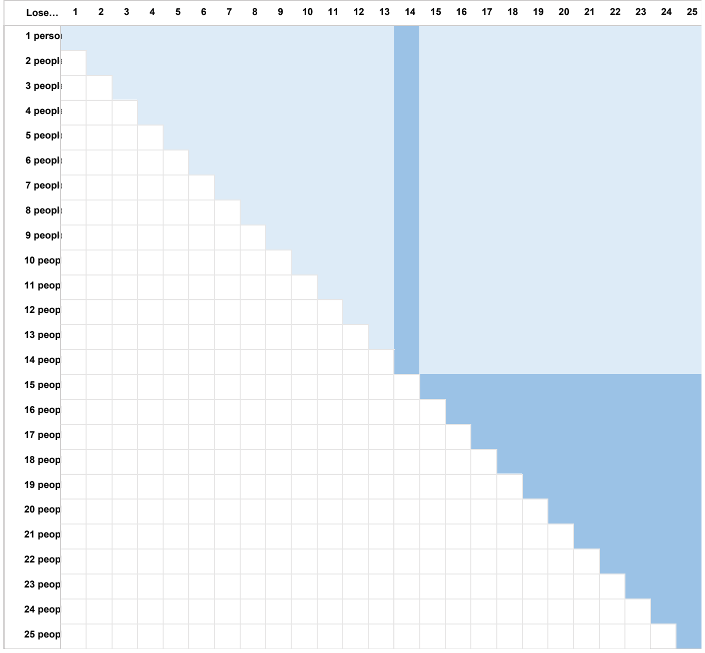
All cells in which person 2 is removed from the team



All cells in which person 10 is removed from the team



All cells in which person 14 is removed from the team



Author Contact Information

Brad Lufkin
130 M St NE, Apt. 1120, Washington, DC 20002
Email: Brad.Lufkin@gmail.com
Phone: 260-494-7325

Diane S. Henshel
Associate Professor, Indiana University
School of Public and Environmental Affairs
1315 E 10th Street, Bloomington, IN 47405
Email: dhenshel@indiana.edu
Phone: 812 855-4556

Gary Deckard
Atterbury-Muscatatuck Center for Complex Operations
Camp Atterbury, Indiana, USA 46124
Email: gary.m.deckard.civ@mail.mil