2019-08-01

A Methodology to Measure the Impact of Diversity on Cybersecurity Team Effectiveness

Caralea May Cornel
Brigham Young University

A Methodology to Measure the Impact of Diversity on Cybersecurity Team Effectiveness

Caralea M. Cornel

A thesis submitted to the faculty of
Brigham Young University
in partial fulfillment of the requirements for the degree of

Master of Science

Dale C. Rowe, Chair
Justin Giboney
Bonnie Anderson

School of Technology

Brigham Young University

ABSTRACT

A Methodology to Measure the Impact of Diversity on Cybersecurity Team Effectiveness

Caralea M. Cornel
School of Technology, BYU
Master of Science

In recent years, the definition of cybersecurity professional has been diluted to include more individuals, particularly women, to be included. Depending on the definition used, women currently comprise between 11% and 25% of the cybersecurity workforce. While multiple studies have indicated the benefits to diverse teams, research in the cybersecurity area is lacking.

This research proposes a framework that uses a modified escape-the-room gamified scenario to measure the effectiveness of cybersecurity teams in technical problem-solving. The framework presents two routes, incident response and penetration testing, the participants can choose. In a preliminary study, this framework is used to show the combination of gender diversity and prior cybersecurity experience and/or cybersecurity knowledge, particularly in women, are found to be significant in reducing the time taken to solve cybersecurity tasks in the incident response, and penetration testing domains.

In conclusion, opportunities for extending this research into a large-scale study are discussed, along with other applications of cybersecurity escape-rooms.

Keywords: gender diversity, cybersecurity teams, framework, effectiveness, team effectiveness

ACKNOWLEDGEMENTS

I would like to give a giant thank you to Dr. Rowe for your guidance, support, and technical expertise in completing this thesis. Thank you to my friends, especially Cj Cornel, Andrew Thomas, Rachel Adams, Anna Guthrie, and Amin Haq, who have provided valuable aid in the building and finishing of this project. Furthermore, my gratitude goes out to my committee members, Professor Giboney and Professor Anderson, for your advice in bettering my thesis. Thank you to my parents, godparents, family, and friends for your love and support in this large endeavor.

I would also like to express my appreciation to Red Sky Security Conference for allowing me to host an initial stage of my thesis. Thank you to all those who participated in my research experiment.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION

1.1 Nature of the Problem

A leading cybersecurity vendor, Palo Alto, defines cybersecurity as “a set of techniques used to protect the integrity of networks, programs and data from attack, damage or unauthorized access”[1]. Along the same lines, the National Initiative for Cybersecurity Careers and Studies (NICCS) defines cybersecurity as “The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation” [2]. This term has not only become pertinent to those with a cybersecurity career, but also for the rest of the world. Cybercrime is remarkably costly. For example it was reported in a 2019 study, that the average cost for companies in cybercrime in 2018 was $13M [3]. In a 2018 Gallup study, Americans were presented with a survey inquiring about how often they worry about becoming the victim of different crimes. The results indicated that the public worry more about crimes surrounding cybersecurity than other types listed [4][5]. More specifically, results show that 71 percent of Americans are extremely worried about “Having [their] personal, credit card or financial information stolen by computer hackers” and 67 percent about “Being the victim of identity theft.” Whereas each of the other statements related to violent crimes, such as “Your home being burglarized when you are not there” and “Getting mugged” were each below 40 percent [5]. From this we can understand how significant cybersecurity is in the daily lives of everyday people.

Cybersecurity is a growing field and we are facing a shortage of cybersecurity professionals. Frost & Sullivan released a report indicating there will be a global deficit of 1.8 million information security workers by 2022 [6]. In addition to this shortage, the reports indicate that diversity is lacking. In particular, studies of gender diversity show that women constitute just 11% of the global cybersecurity workforce, with 14% in North America being the highest percentage in comparison to other regions [6]. A more recent article [7] completed by a collaborator from the last group, the International Information System Security Certification Consortium $(ISC)^2$, indicates that women make up a greater percentage of cybersecurity professionals than what has been stated. This increase in the number of women in the field has only been achieved by redefining the role of a cybersecurity professional to include a wider variety of supporting roles.

Various disciplines, such as research and development [8] and business [9], have demonstrated the advantages of diverse teams. Although this is the case, studies on diversity in specific cybersecurity skill areas, such as incident response or forensics, are lacking in technical depth and rigor in regards to the impact of diversity. This has led to conflicting statements about the value of diversity in specific circumstances. A formal study focusing on technical capabilities will provide more insight in defining and measuring the difference in effectiveness from gender-diverse cybersecurity teams.

How can cybersecurity team effectiveness be defined? Existing research is limited, for example, discussing how effectiveness can be measured, but lacking a definition for this [10]. To better understand this idea of team effectiveness in the technical cybersecurity space, a suitable definition is needed.

Should gender-diverse cybersecurity teams be shown to be more effective, then the deficit of cybersecurity professionals in the workplace could be better mitigated by further studies in the recruitment and retention of women and other diversity groups.

1.2 Purpose of the Research

The purpose of the research is to:

1. Establish a definition of effectiveness with respect to cybersecurity teams.
2. Select key technical and non-technical skills in cybersecurity that can be measured in support of (1).
3. Construct a framework capable of delivering a series of representative cybersecurity challenges with associated measurements for the skills described in (2).
4. Perform a validation study of the framework using homogeneous and heterogeneous teams.
5. Review the findings of the proposed framework.

This framework will allow the measurement of team effectiveness in the technical cybersecurity space. These measurements will help to better understand existing research in identifying whether mixed gender teams are more effective than same gender teams in cybersecurity, and thus allow more effective targeting of cybersecurity candidates.

1.3 Research Questions and Hypotheses

The following are questions and hypothesis regarding this research:

- Q1. What is an appropriate definition of team effectiveness in the cybersecurity domain?
- Q2. What subdomains of cybersecurity are practical for these research purposes?
- Q3. How can effectiveness be measured in cybersecurity teams involved in technical problem-solving?
- H1: In line with other disciplines, gender-diversity is beneficial to cybersecurity team effectiveness in tasks that require problem-solving or innovation.
- H2: A robust method for measuring technical cybersecurity team effectiveness can be used to determine the impact of gender diversity within cybersecurity teams.

1.4 Defining Effectiveness

After review of the literature (see section 2.7), the following definitions were found to be the most suitable [11]:

- Team performance: "the outcomes of the team's actions regardless of how the team may have accomplished the task" [12]
- Team effectiveness: A "holistic perspective in considering not only whether the team performed (e.g., completed the team task) but also how the team interacted (i.e., team processes and teamwork) to achieve the team outcome" [12]

- Team cognition: “the cognitive structures and processes within teams, which are inherently important to teams’ functioning and thus may correlate to their performance and effectiveness” [13]

1.5 Additional Definitions

- Penetration testing: “An evaluation methodology whereby assessors search for vulnerabilities and attempt to circumvent the security features of a network and/or information system” [14]
- Incident response: A method whereby a person “responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats” and also involves “investigat[ion] and analyzation” of “all relevant response activities” [2]
- Honeypot: systems altered to be used as decoys with the purpose of “gather[ing] information regarding human threats” [14]

2 LITERATURE REVIEW

2.1 Cybersecurity

Both the significance and awareness of cybersecurity has continued to grow, the creation of the United States' National Cybersecurity Awareness Month in 2004 being one of such indicators. This initiative focuses on providing resources for informing the public how to stay cyber safe and aware, especially spreading the awareness during the month of October [15].

In line with these fears, it is troubling that in the cybersecurity space, there is a significant shortage of professionals to help combat these concerns. In a 2018 study, the global shortage of these workers was reported to be three million [7]. In the same study, 59 percent of participants reported the companies they work for "are at moderate or extreme risk of cybersecurity attacks" because of having an inadequate amount of staff working in cybersecurity [7].

2.2 Cybersecurity Subject Areas

Cybersecurity is a broad field and is continually growing. It includes many subject areas such as incident response and penetration testing.

Incident response is a method whereby a person "responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats" and also involves "investigat[ion] and analyzation" of "all relevant response activities" [2]. It includes enacting a defined plan in response to an incident.

Penetration testing is assessing how secure the given defenses are by playing the role of malicious threats in order to identify vulnerabilities and potential weaknesses that could be used in a real world scenario [14].

2.3 Suggested Factors in Gender Diversity

Although the focus of this study is to measure the effectiveness of team diversity, some studies have investigated why gender diversity is of particular interest in different environments. It would be reasonable to suggest that the different thought processes in male and female subjects may have an impact in team effectiveness. The following is a short review of studies that seemed relevant to this suggestion.

2.3.1 Learning Difference Between Genders

Neurobiological studies have shown the human visual cortex as two systems. One system being used to identify 'what' an object is; responding to questions of color and texture. The second system has to do with 'where' it is going; how fast is it moving and in what direction [16] [17]. In his book, *Girls on the Edge*, author Leonard Sax M.D., Ph.D. presents a series of studies that extend the visual system into learning preferences; emphasizing that females are more naturally tended to 'what' learning, whereas males tend to benefit more from 'where' learning [18].

The natural tendency of a gender to prioritize either the 'what' or 'where' provides insight into the studies on gender diversity in the workplace. This reinforces the finding that mixed gender teams are more effective in understanding cybersecurity threats. Accordingly, these teams should be more proficient at understanding and articulating both the ‘what’, and ‘where’ of threats: “What attacked us?” and “Where did it come from?”

A pertinent question on the root cause surrounding the gender composition of cybersecurity professionals could be derived from studies of educational environments: Does the school system cater to the ‘what’ learning preferences of women in computing disciplines?

Dr. Sax states that when schools teach STEM topics in a manner more suited to the ‘what’ brain, adolescent females perform noticeably better and gain self-confidence at a faster rate. As most schools focus on the ‘where’ aspects of STEM topics, then it is possible that the current delivery of STEM education places young women at an innate disadvantage versus their male peers. One must then wonder to what extent this affects the workplace, and consequentially, whether some women who have completed a computing education at college have misguided expectations in a career setting. Stated differently: Are some women in cybersecurity careers thinking more like men, and potentially losing some of their natural abilities to perceive the ‘what’ due to educational methods? If so, this could potentially have an impact on the effectiveness of a mixed-gender cybersecurity team.

2.3.2 Societal Factors

Society may also factor in for why there is less gender diversity. In a 2015 study by the Information Systems Audit and Control Association (ISACA), 75% of women reported to have never heard, from guidance counsellors nor teachers, a suggestion for a career path in cybersecurity [19]. Furthermore, a 2017 study investigated the impact of stereotypes and technical experience for girls. They hypothesized the reason for the gender gaps in the "motivation to pursue computer science and engineering" to be due to cultural stereotypes and the different experiences due to gender. For example, elementary school girls reported smaller interest and self-efficacy in comparison to boys when it comes to technology [20].

The method in a 2017 study involved a setting where participants were randomly chosen for a group: programming a robot, storytelling without technology, and a "no-activity" group [20]. The latter 2 groups acted as the control groups. The study reports a boost in technology motivation among females after programming a robot. They held more motivation for programming and robot self-efficacy than the girls who had been in the control groups. The study also observed "stereotype threat" in female participants who viewed boys as "better than girls at robots and programming" and thus "reported lower self-efficacy".

2.4 Team Diversity

The relationship between gender diversity and team productivity is one of much discussion among researchers. Most studies conclude that, under most conditions, diversity leads to a competitive advantage [21], improved decision making [22] and radical innovation [8]. In Information Technology, a 2014 study showed that diverse teams are more productive, innovative, more able to stay on schedule, and under budget [23]. Although this research is less mature in the cybersecurity domain, indications are that gender diversity leads to a better understanding of threats [24], [25].

While several studies have been performed on team diversity, most of these focus on the soft-skills or non-cybersecurity technical skills of teams using subjective measurements [26]. For example, studies in management show diverse organizations perform better (26% increased shareholder return in six years if there is woman on the board) [19]. In a Harvard review of team-diversity studies, researchers show that diverse teams are typically more effective in a variety of ways, such as being better at decision making or being innovative [27]. Other research adds that not only does diversity have a tendency to enhance team creativity and insight, but also to introduces disruption into existing teams [28]. One could posit that a certain amount of disruption or perturbation could lead to increased communication and discussion of possible solutions. For example, threat assessment and risk mitigation demand a frank, open and innovative process that may be facilitated by team perturbation. Such disturbances to the normal thought process of a team can encourage lateral thinking and enhance problem solving if personal conflict is avoided. Objective studies that consider technical problem solving, rather than just soft-skills may provide more insight into these findings.

Another article highlights the significance of having gender diversity in cybersecurity. It supports the idea that diversity can help better combat cybersecurity threats [19]. A point is made; in order for one to adapt to the constantly changing cyber threats, it is necessary for a more diverse set of skills of which is a homogenous group would not be able to suitably represent. The article continues to suggest, besides having the technical knowledge, that those in the cybersecurity profession need to be able to "think critically, manage projects, be adept at planning and communicate effectively".

Another paper published in 2000 that calls for further research across disciplines to determine the precise benefits of diverse teams [29]. This paper claims that while heterogeneous teams are typically more effective, the level of efficacy may not in fact be significant under certain conditions. Although this article may be older and there have been studies in other fields, there is limited research, if any, studying the impact of gender diversity in the cybersecurity domain. More specifically, research on this is needed to gauge the effects of diversity on cybersecurity teams.

2.5 Cybersecurity Teams

One study evaluated the capabilities of cybersecurity incident response teams (CSIRTS) in comparison of efficiency to other similar fields, such as military response (MR) and emergency medical systems (EMS). From the comparative results, the authors suggested how to improve CSIRTS, focusing on problem solving, communication, trust, and shared team knowledge [10].

2.6 Gamification and Cybersecurity

In a 2011 study, the conclusion of a study suggested that gamification can be defined as the implementation "of game design elements in non-game contexts" [30]. In cybersecurity, gamification has been included in different events such as Capture the Flag (CTF) competitions and Cyber Defense Competitions. Gamification is implemented by integrating ideas such as turning the activity into a competition and including point systems. After analyzing multiple security events that have gamification involvement, such as those mentioned, one study published in 2019, observes that they have multiple commonalities; They have been known to impact participants' by resulting in their "enjoyment and satisfaction" for "competing," "increased motivation to learn about cybersecurity, improved practical knowledge of theoretical aspects of cybersecurity," and gained awareness of where they lack the knowledge [31]. Another study in 2017 tested the importance of story inclusion to their cybersecurity course. The course involved participants working on multiple security tasks. For each task, they would unlock parts of the given story. The results indicated that the story had increased their participants' engagement and the outcome of how well they did [32].

2.7 Team Effectiveness

The goal of a 2016 study was to figure out a method for how team effectiveness could be assessed in cybersecurity, specifically in the case of defense exercises [11]. In a 2005 research paper focused on teamwork it states that: team effectiveness "takes a holistic perspective in considering not only whether the team performed (e.g., completed the team task) but also how the team interacted (i.e., team processes and teamwork) to achieve the team outcome" [11], [12]. The study concluded, for the assessment of team effectiveness, both "technical performance measurements and behavioral assessment techniques" would be required [11].

2.8 Summary of Significant Literature Elements

The literature review revealed the following significant elements that are suitable for consideration in designing this study:

- Team effectiveness consists of cognition and performance.
- Immersive and engaging environments can be created by gamification.
- Experiments can be designed that allows teamwork to influence the measured outcomes.
- Overlapping and complimentary skillsets can impact team performance.
- Related studies outside of cybersecurity suggest that gender diversity may lead to a better understanding of threats.

3 METHODOLOGY

3.1 Overview

The steps of this research will be conducted as follows (from section 1.2):

1. Establish a definition of effectiveness with respect to cybersecurity teams.
2. Select key technical and non-technical skills in cybersecurity that can be measured in support of (1).
3. Construct a framework capable of delivering a series of representative cybersecurity challenges with associated measurements for the skills described in (2).
4. Perform a validation study of the framework using homogeneous and heterogeneous teams.
5. Review the findings of the proposed framework.

A framework was created with a series of technical challenges, designed to measure team effectiveness in an immersive gamified environment. The scenario was based on two domains within the Certified Information Systems Security Professional (CISSP) Common Body of Knowledge (CBK) defined by $(ISC)^2$: Security and Risk Management, Asset Security, Security Architecture and Engineering, Communications and Network Security, Identity and Access

Management, Security Assessment and Testing, Security Operations, and Software Development Security.

Penetration Testing falls under the "Security Assessment and Testing" domain, while incident response falls under the "Security Operations" domain [33].

3.2 Selection Rationale

Selecting two complimentary opposing sides of cybersecurity (offensive and defensive) allows for technical skills to be measured in different domains. While there is some technical overlap between these domains, they require different approaches and training to navigate. The defensive side selected was incident response, and penetration testing was selected to represent the more offensive field. These domains each had a series of challenges based on them. The challenges were presented in a gamified scenario to increase participation and motivation.

The challengers were assessed on their cybersecurity skills based on technical skills [10], team performance [12], and team cognition [11] [13].

3.3 Framework Requirements

The framework is designed to measure team effectiveness as defined in section 1.4. This is to say that it "takes a more holistic perspective in considering not only whether the team performed (e.g., completed the team task) but also how the team interacted (i.e., team processes and teamwork) to achieve the team outcome [12]". Team effectiveness is composed of team performance and team cognition (see definitions from Section 1.4).

After reviewing existing research and given the above definition of team effectiveness, requirements have been established for creating the framework to measure the impact of diversity on cybersecurity team effectiveness.

- Immersive/Engaging [realistic]
- Structured ability to measure [performance]
- Encourage teamwork [effectiveness]
- Different skills are complimentary [cognition]
- Adaptable [cognition][performance]

3.3.1 Immersive/Engaging

In order to create an immersive/engaging environment, gamification was identified as an effective approach. As indicated in section 2.6, gamification leads to an increase in engagement. Therefore, the method used to measure team effectiveness should incorporate gamification elements in the given challenges and overall experience. The objective of this is to have participants communicate, cooperate and work together realistically as they would to solve real-world problems.

3.3.2 Structured Ability to Measure

The environment needs to have enough structure to allow the measurement of a team's performance. Logging of events and progress will facilitate measurement and allow the measurement of time-to-completion of various steps, as well as what activities led to a challenge's completion and what hints or training material was provided to the team.

3.3.3 Encourage Teamwork

Promoting teamwork can be done by encouraging participants to participate in team sizes of at least two or more. To encourage participants to work with one another, a team goal should be established to encourage completing the given activity together. Multiple challenges based on teamwork should also be included to discourage individual participation. One framework for the gamification of teamwork situations suggests, in order to have a cooperative team, the design of the activity should promote interdependence of game goals and dependent interaction [34].

3.3.4 Complimentary Skillsets

As well as being designed to require teamwork, the challenges should be designed such that complimentary skillsets of individual team members can be utilized. Although the focus is on technical skills, teams often consist of mixed skills which can work synergistically together. The challenges should allow these team cognitive processes to be seen and measured.

3.3.5 Adaptable

Initial discussions indicated the possibility of inherent difficulties in measuring different levels of proficiency between teams. As all teams are not the same, the challenges should have an adaptive level of difficulty. Many teams learn together on various projects. The environment should provide training and assistance to teams that are making slower progress and allow teams to progress, even if the overall difficulty is beyond their initial capability. This flexibility will allow a greater range of participants. Surveys should normalize for a team’s experience and capability to allow an unbiased comparison of performance of teams possessing similar technical capabilities.

3.4 The Immersive Cybersecurity Experience (ICE)

The Immersive Cybersecurity Experience (ICE) simulator is an escape room, a popular story-based extracurricular activity designed with the requirements of solving puzzles in order to "escape" the room. However, instead of trying to escape, the goal is to survive. It was initially designed to include a variety of technical challenges that are catered to instruction provided to participants at a series of cybersecurity workshops during a summer camp. ICE is set on a starship, where not only must challenges be solved, but they must operate their ship, such as by steering the ship and monitoring fuel intake.

3.4.1 ICE History

The ICE was designed in 2016 by the Cybersecurity Research Lab (CSRL) for the Girls Cybersecurity Camp (GCC) as a means for measuring how engaging the immersive cybersecurity experiences are. In a 2017 study, it was reported that a survey was given to the GCC participants immediately after participating in the ICE. Results indicated that 100% of the participants agreed with the following statement "The Escape Room experience was engaging", with 56.52% strongly agreeing, 32.61% agreeing and 10.87% somewhat agreeing. The question was formed on a Likert scale consisting of different levels of agreement and disagreement. None of participants held any level of disagreement for this question [35]. Furthermore, a question, that was also formed using the Likert scale, asked about their interest in Cybersecurity, specifically, "How likely are you to continue with cybersecurity education?" The results of the survey were: 48.84% extremely likely, 32.56% moderately likely, and 13.95% likely. None of the answers in regards to neutral (i.e. Neither likely nor unlikely) or disagreement (i.e. Slightly unlikely) were selected for this query.

An overview of the flow through ICE is shown in Figure 3.1.

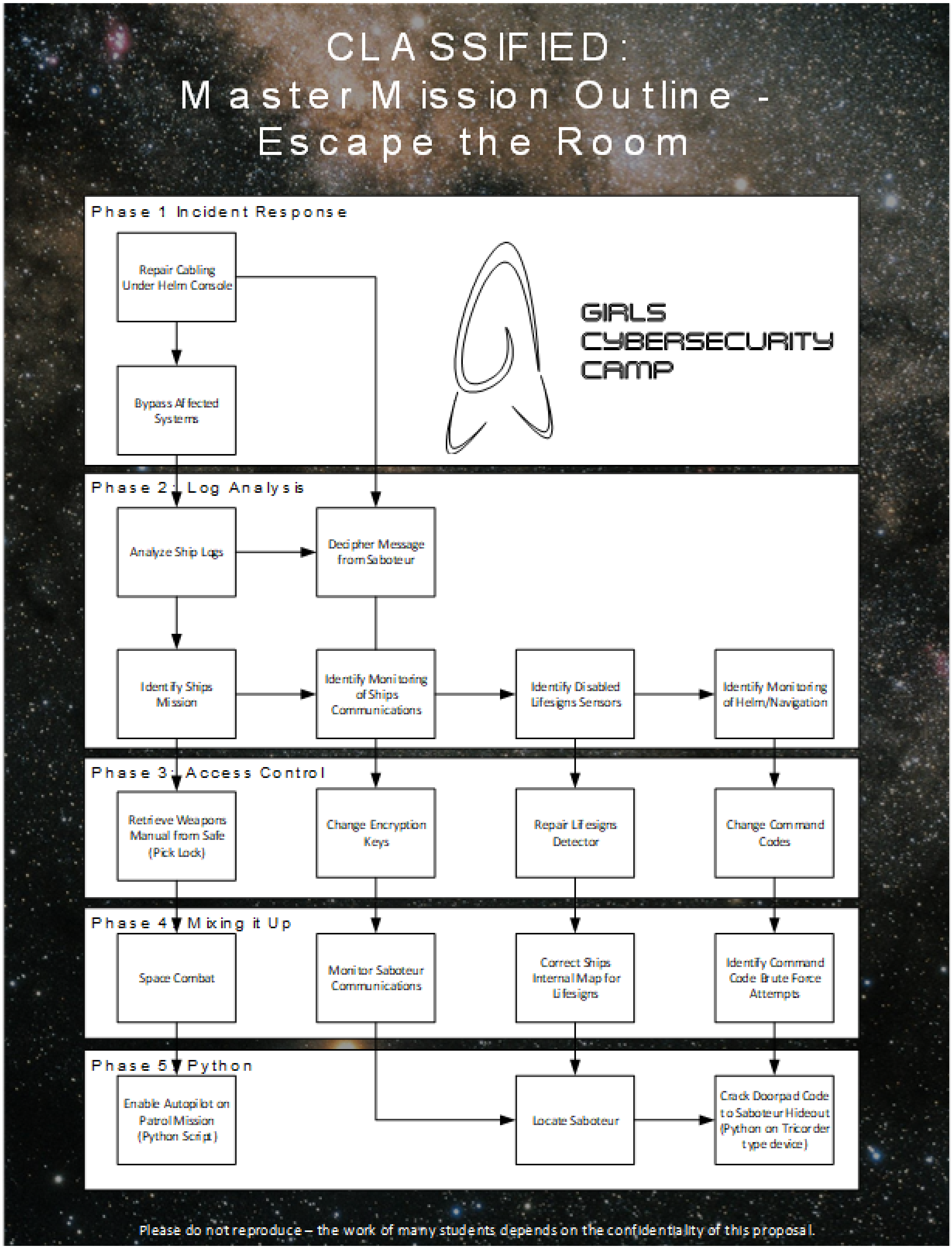
3.4.2 Applicability

ICE has been operating since 2016 and been through multiple iterations and provides an established approach to the benefits of combining cybersecurity and hands-on gamification. ICE covers all the requirements for the method of measurement provided in Section 3.3. It is engaging, as indicated in the survey results in 3.4.1. Also, there is a structured ability to measure performance by including a timer and observation room and finally, it is a team activity, thereby encouraging, and at times, requiring teamwork. Individuals that have participated in ICE have been seen to contribute and work with one another.

ICE was designed to be adaptable and allow the difficulty of challenges to be altered in real-time for different skill levels. Although the ICE has already been established, it does not have the ability to travel to different conferences to encourage diverse participants. The Mobile Immersive Cybersecurity Experience (m-ICE) was created for this reason and based on the same idea as the ICE.

3.5 Mobile Immersive Cybersecurity Experience (m-ICE)

The Mobile ICE platform was built around a more structured series of interchangeable tasks as shown in Figure 3.2. The mobility aspect was implemented in order to persuade a more targeted audience to participate in the study. For example, targeted cybersecurity professionals seemed more likely to take part in the m-ICE if it was easily accessible to them, rather than traveling to a farther location to participate. The idea to bring the m-ICE to them, rather than persuading professionals to come to where the m-ICE was stationed, was therefore created.



CLASSIFIED:
Master Mission Outline -
Escape the Room

Phase 1 Incident Response

Repair Cabling Under Helm Console

Bypass Affected Systems

GIRLS CYBERSECURITY CAMP

Phase 2: Log Analysis

Analyze Ship Logs

Decipher Message from Saboteur

Identify Ships Mission

Identify Monitoring of Ships Communications

Identify Disabled Lifesigns Sensors

Identify Monitoring of Helm/Navigation

Phase 3: Access Control

Retrieve Weapons Manual from Safe (Pick Lock)

Change Encryption Keys

Repair Lifesigns Detector

Change Command Codes

Phase 4: Mixing it Up

Space Combat

Monitor Saboteur Communications

Correct Ships Internal Map for Lifesigns

Identify Command Code Brute Force Attempts

Phase 5: Python

Enable Autopilot on Patrol Mission (Python Script)

Locate Saboteur

Crack Doorpad Code to Saboteur Hideout (Python on Tricorder type device)

Please do not reproduce – the work of many students depends on the confidentiality of this proposal.

Figure 3.1 - Immersive Cybersecurity Experience (ICE) Challenge Flow [35]

The mobility factor considers a couple aspects of human behavior. One study observed that people are less likely to travel far because, in general, “people move periodically within a bounded region” [36]. Another behavior is in accordance with Zipf’s principle of least effort (PLE), which is the idea that people tend to select the path of “least effort” in order to complete “tasks” [37]. The PLE can be seen in the location placement of retail stores, as location can be the most important element in determining their success [38]. In considering all of these behaviors, it may be suggested that an activity, such as the m-ICE, being hosted 45 minutes away from where the ideal participants are convening for a conference, would be less likely for the same participants to travel to the hosted location. It would then be better for the m-ICE to be at the conference or where the targeted subjects are.

3.5.1 Technical Topics

m-ICE consisted of two tracks central to cybersecurity: Incident response and penetration testing. A small subset of technical skill tests was included that can be expanded for future studies. All tracks required the participant to focus on the instructions and the team’s ability to process clues and indicators were also measured. The initial skills measured as part of the challenge include:

1. Penetration Testing
    a. Command line tool usage (Kali Linux)
    b. Reconnaissance (discovery of dictionary file)
    c. Password attacks (dictionary)
    d. Web vulnerability assessment

   e. SQL injection
   f. Web-site reconnaissance
2. Incident Response
   a. Command line tool usage (Linux)
   b. Review of log files (command line)
   c. Web compromise investigation (defacement)
   d. Physical compromise investigation (malicious dropbox)
   e. Firewall configuration
   f. Attack containment

Each subtask was measured by its binary completion, number of incorrect attempts, team communication (measured by the team's overall approach to problem solving and manual observation), number of hints provided and the delta time to complete since the last successful task completion. An observer will take notes on team dynamics during the exercise. A copy of the observer log can be found in Appendix C.

3.5.2 Network and Platform

The network should be portable and allow for the easy replacement of failed systems. Network range(s) used should be chosen from less likely to be used ranges to avoid overlap with externally connected systems. The edge router should use Network Address Translation (NAT) to avoid interference when connected to external networks.

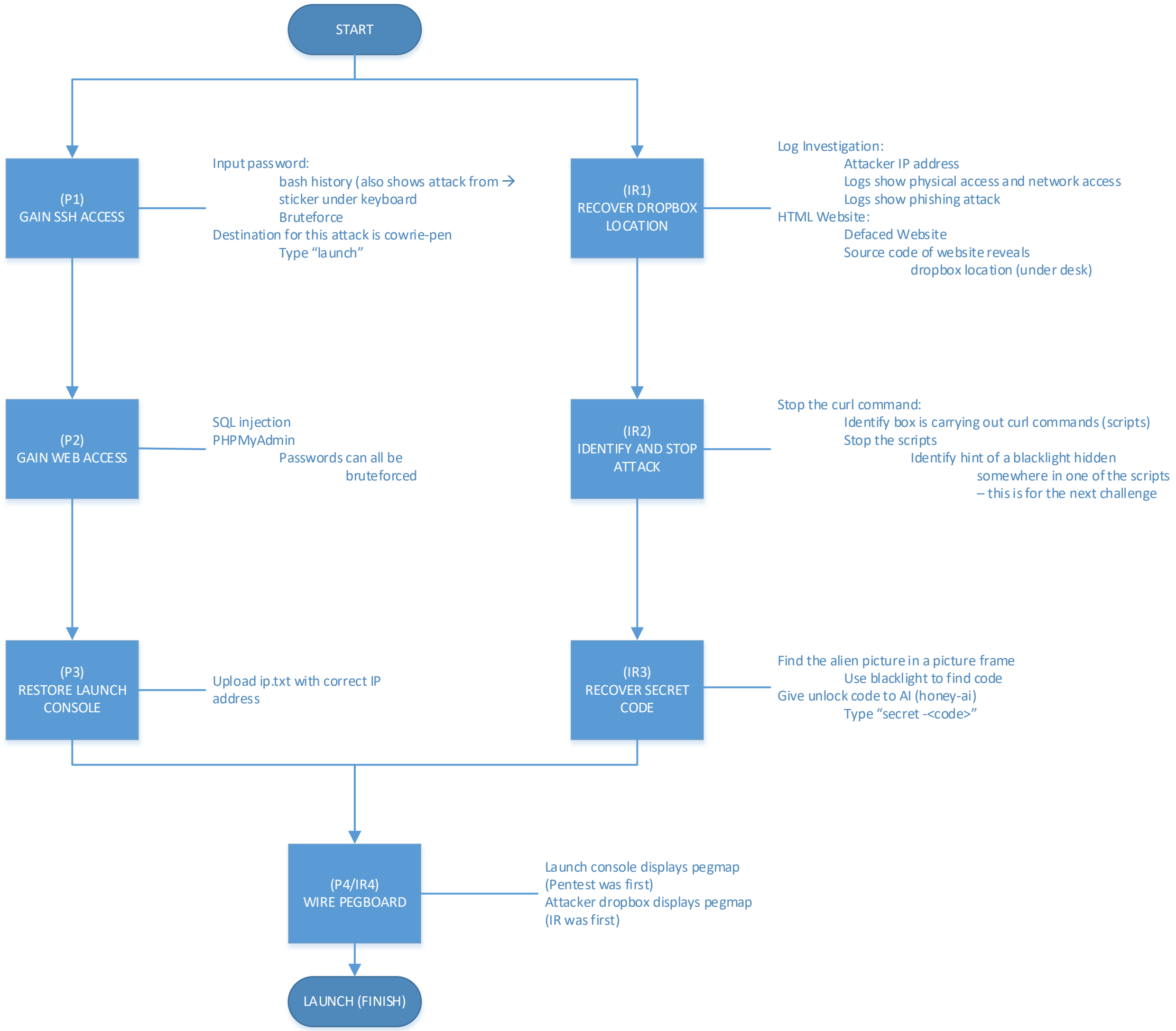

START
(P1)
GAIN SSH ACCESS
Input password:
bash history (also shows attack from →
sticker under keyboard
Bruteforce
Destination for this attack is cowrie-pen
Type "launch"
(IR1)
RECOVER DROPBOX LOCATION
Log Investigation:
Attacker IP address
Logs show physical access and network access
Logs show phishing attack
HTML Website:
Defaced Website
Source code of website reveals
dropbox location (under desk)
(P2)
GAIN WEB ACCESS
SQL injection
PHPMyAdmin
Passwords can all be
bruteforced
(IR2)
IDENTIFY AND STOP ATTACK
Stop the curl command:
Identify box is carrying out curl commands (scripts)
Stop the scripts
Identify hint of a blacklight hidden
somewhere in one of the scripts
– this is for the next challenge
(P3)
RESTORE LAUNCH CONSOLE
Upload ip.txt with correct IP
address
(IR3)
RECOVER SECRET CODE
Find the alien picture in a picture frame
Use blacklight to find code
Give unlock code to AI (honey-ai)
Type "secret -<code>"
(P4/IR4)
WIRE PEGBOARD
Launch console displays pegmap
(Pentest was first)
Attacker dropbox displays pegmap
(IR was first)
LAUNCH (FINISH)

Figure 3.2 - m-ICE Conceptual Scenario

Raspberry Pi devices are used extensively in ICE and are suitable to be used in m-ICE. If possible, these should be stateless (network boot from a shared image) to allow for easy swap outs in the event of failure.

3.5.3 Design Methodology

Rapid Application Development is a 4-stage cyclic process that produces quick prototypes to allow for user feedback at early stages of development. Although initially proposed in 1991, it is compatible with modern agile development methodologies [39]. The primary rationale for the creation of RAD was to combat the issue of the requirements changing at the conclusion when using other methods [33]. It is a common approach to tackling research problems within the BYU Cybersecurity Research Laboratory.

Rapid application development (RAD) was primarily used to develop ICE and has been found to be a robust method for developing the platform. RAD uses a rapid prototyping iterative process consisting of 4 main steps (Figure 3.3).

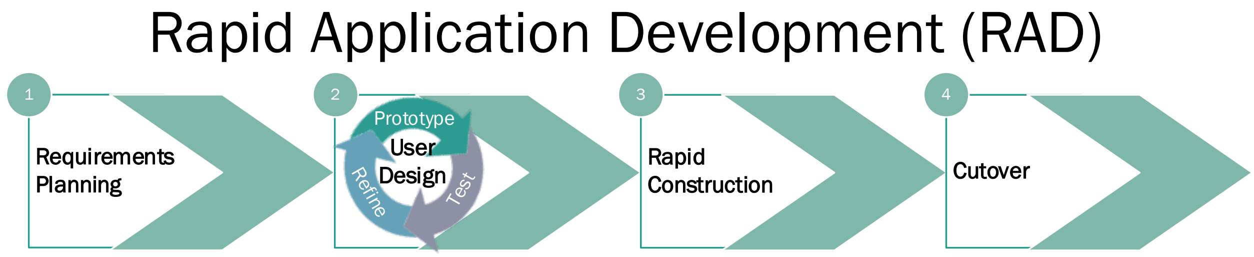


Figure 3.3 - Rapid Application Deployment Lifecycle

The first step, requirements planning, is comprised of the project creators working with the clients to identify the problem being addressed by the project and its requirements. Examples of such requirements can be defining the scope or possible uses of the project. The second step, user design, is a cyclic process where a prototype is created, tested, and updated to include feedback. It is repeated as necessary. The third step, rapid construction, is the building of the final prototype, where the bugs are ironed out. Similar to the second step, the third step considers feedback and then fixes it accordingly but can also be repeated as needed. The fourth step, cutover, is the last stage and implements the final alterations. Step four transitions the project to a live environment, permitting the testing of all elements of the project [40], [41]. RAD allows for the system to be developed in a short timeframe, tested, and then redesigned in accordance with feedback, bug discovery and performance.

3.5.4 Architecture and Code Management

Since starting in 2016, ICE has become increasingly complex with live development taking place over a period of years on various elements of the environment. The creation of m-ICE addressed this by a more efficient and consistent model. At the core of this will be an event-driven architecture orchestrated by a central server. All code will be managed using Git version control.

3.5.5 Survey-based User Feedback

Participants were asked to complete two surveys distributed through the Qualtrics platform. To decrease bias, one survey was given to the participants before taking part in the m-ICE, and the other was given after to gauge their thoughts and feelings on the m-ICE.

The initial survey, found in Appendix A, includes questions on demographics, cybersecurity experience, familiarity between team members, and whether or not they consider themselves cybersecurity experts. The post survey, see Appendix B, inquiries about whether they enjoyed working with their team, their experience with each of the challenges, and whether they enjoyed the m-ICE. The surveys were used to help answer the question, (Q3) “How can effectiveness be measured in cybersecurity teams involved in technical problem-solving?”, and address both hypotheses, (H1) “In line with other disciplines, gender-diversity is beneficial to cybersecurity team effectiveness in tasks that require problem-solving or innovation” and (H2) “A robust method for measuring technical cybersecurity team effectiveness can be used to determine the impact of gender diversity within cybersecurity teams.” A diagram similar to the data collection model [11] has been created and is shown in Figure 3.4.

The observation notes were logged using a template called the Observation Log (see Appendix C). The Observation Log was specifically catered towards observing communication and collaboration among teams per challenge.

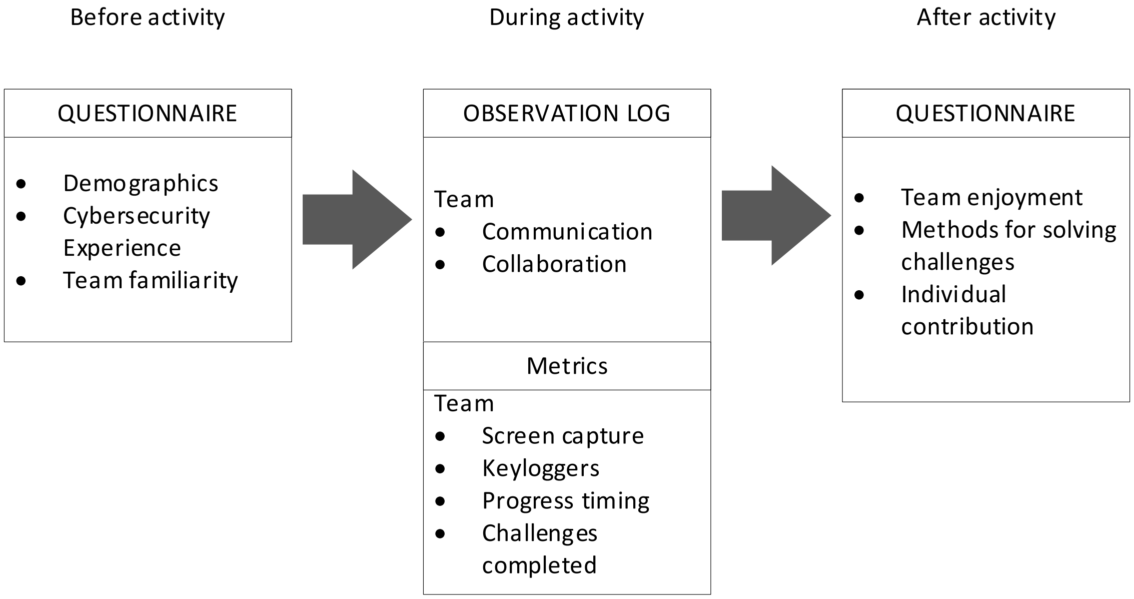


Figure 3.4 - Data Gathering Model

3.5.6 Experiment Metrics

From section 3.5.1 the following metrics will be gathered to investigate team effectiveness:

- Completion of each challenge

- Number of incorrect attempts
- Team collaboration
- Number of hints provided
- Delta time to complete since last successful task completion (for each challenge)
- Observations of team communications (see Observation Log in Appendix C)

3.5.7 Institutional Review Board (IRB) Approval

Gathering of data from human subjects was reviewed by the BYU Institutional Review Board “A Formal Methodology to Measure the Impact of Diversity on Cybersecurity Team Effectiveness”. The IRB number is #E19146. Exempt status under category 2(i)(ii) was granted through May 2020

4 EXPERIMENT AND DATA GATHERING

4.1 Overview

This section discusses the implementation and data gathering of the methodology presented in Chapter 3.

4.2 m-ICE Introduction

As mentioned in Section 3.5, m-ICE was created based off the same idea as ICE. The m-ICE was created to be portable to increase participation and, therefore, increase the amount of gathered data.

The m-ICE consisted of two main tracks, penetration testing and incident response. These tracks each contained 3 challenges, and shared the 4th challenge. The m-ICE allowed for the participants to choose which track they would like to take, similar to an escape room process. For the m-ICE, a story line was involved to gamify the experience to increase appeal and engage participants. A time limit of 25 minutes to complete the escape room was also given and to create a sense of urgency and allow the rotation of teams throughout the experiment.

4.3 Storyline

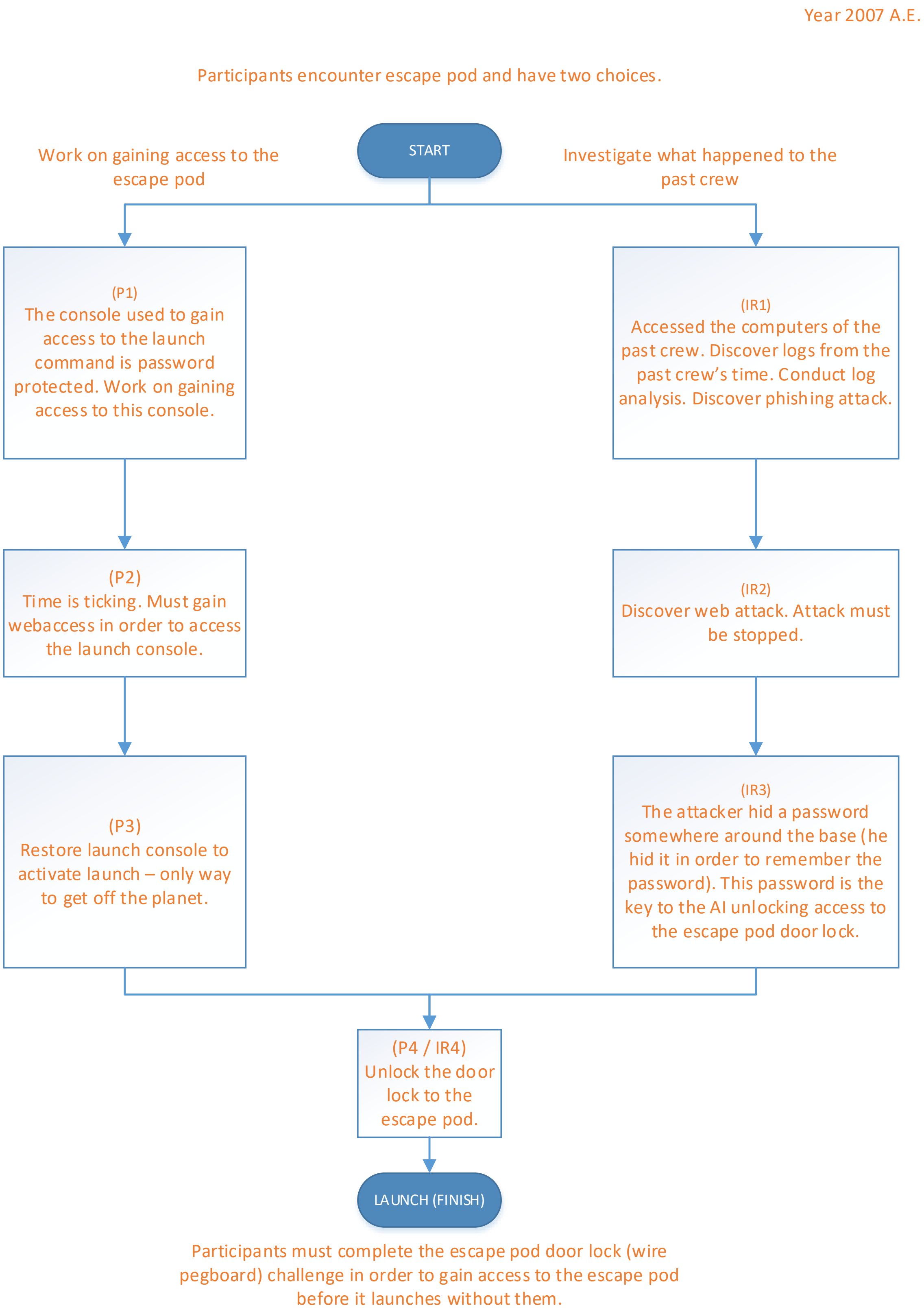
A storyline was integrated into the design to increase engagement as research shows in Section 2.6. The story takes place on another planet that people now inhabit. The year is 2007 After Earth (A.E.) and a mysterious and urgent event has forced the participants to be among the last survivors. They are recommended to find their way to an escape pod, but upon discovering one, find that it is not fully functional. To gain access to the escape pod, they must choose to either break in (pen testing) or investigate (incident response).

Integration of the storyline involved assigning a story to each route and challenge (Figure 4.1), designing the physical aspect of the m-ICE with a futuristic theme, and including informational videos that gave a background of what scenario the participants are in during the experience.

4.4 Challenge Design

4.4.1 Penetration Testing Challenges

The penetration (pen) testing route focused on brute force and vulnerability identification. In the first challenge (P1), their objective was to use a locked down Kali Linux machine to gain Secure Shell (SSH) access to another system, which was a honeypot designed as a Linux machine. Access could be achieved through physically locating a password or brute-forcing the password. The goal of P2 was to gain web access, done through SQL Injection or brute-forcing passwords through PHPMyAdmin. P3 focused on restoring and fixing the given file, which



Participants encounter escape pod and have two choices.

Work on gaining access to the escape pod

Investigate what happened to the past crew

(P1)
The console used to gain access to the launch command is password protected. Work on gaining access to this console.

(P2)
Time is ticking. Must gain webaccess in order to access the launch console.

(P3)
Restore launch console to activate launch – only way to get off the planet.

(IR1)
Accessed the computers of the past crew. Discover logs from the past crew's time. Conduct log analysis. Discover phishing attack.

(IR2)
Discover web attack. Attack must be stopped.

(IR3)
The attacker hid a password somewhere around the base (he hid it in order to remember the password). This password is the key to the AI unlocking access to the escape pod door lock.

(P4 / IR4)
Unlock the door lock to the escape pod.

Participants must complete the escape pod door lock (wire pegboard) challenge in order to gain access to the escape pod before it launches without them.

Figure 4.1 - m-ICE story map

contained an incorrect IP address, on a web portal. The solution requires the incorrect IP address to be changed to the correct IP address.

The fourth challenge (P4) focused more on the “fun” aspect. They wired a pegboard (Figure 4.2) using a given mapping (Figure 4.3) provided in the room. The mappings listed where to connect the wires e.g. ‘Black 4 -> Red 7’. One end of a wire would be plugged into the hole indicated as black ‘4’, and the other, plugged into the hole labeled as a red ‘7’.

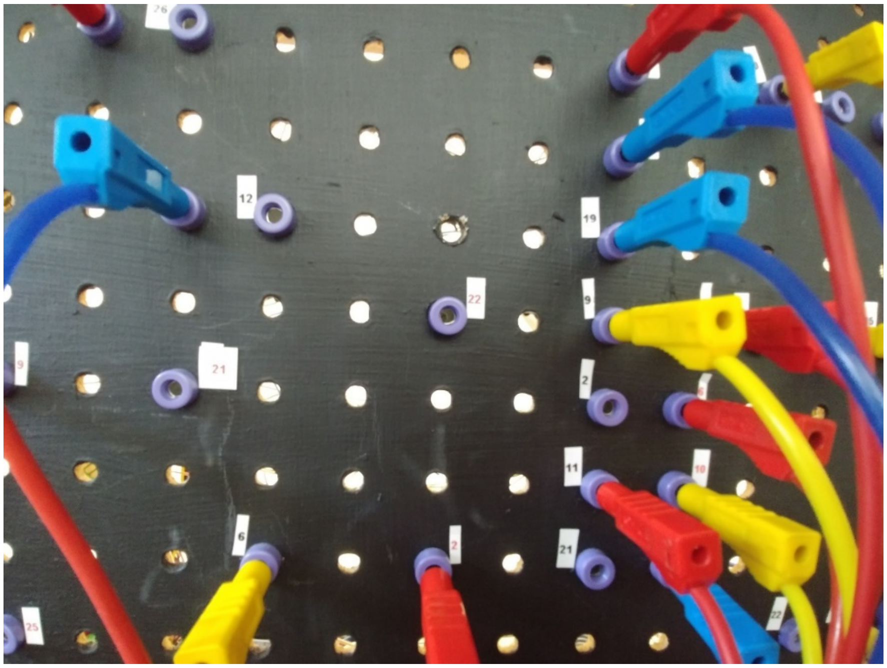
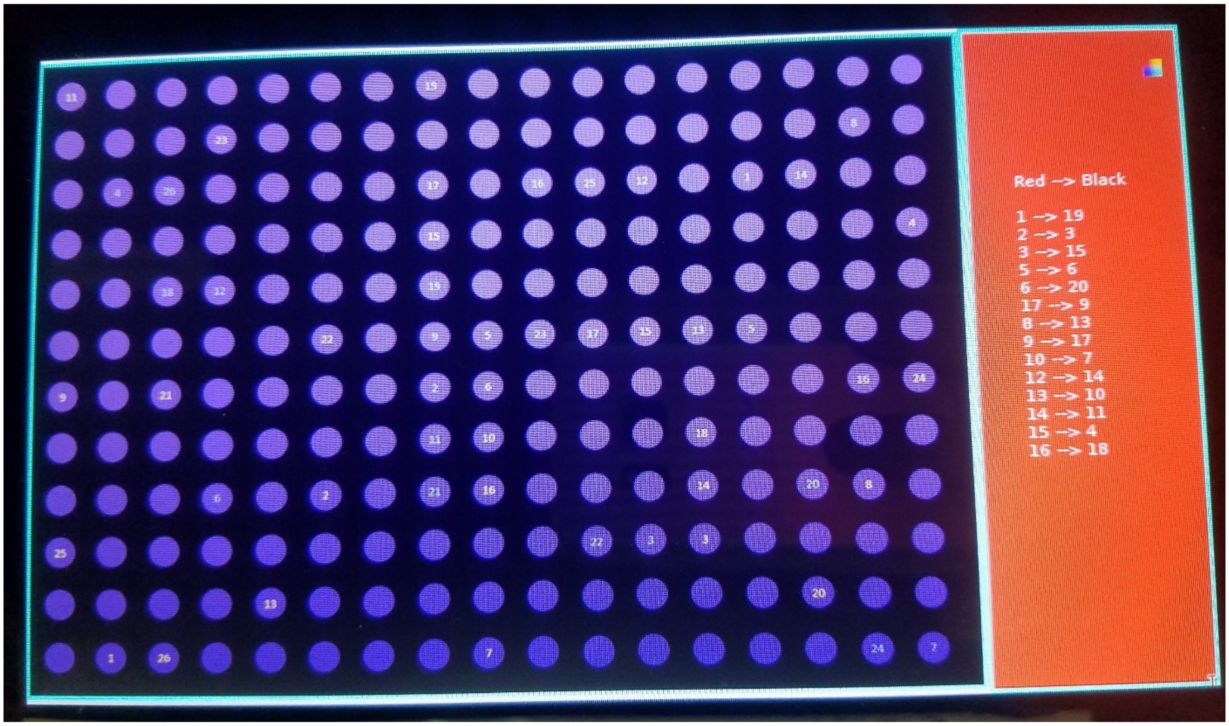


Figure 4.2 - Pegboard with wires plugged in

This challenge was taken from the original ICE experiment as it has been an excellent test of team cooperation, requiring a minimum of two team-members to complete.



```
Red --> Black

1 --> 19
2 --> 3
3 --> 15
5 --> 6
6 --> 20
17 --> 9
8 --> 13
9 --> 17
10 --> 7
12 --> 14
13 --> 10
14 --> 11
15 --> 4
16 --> 18
```

Figure 4.3 - Pegboard map

4.4.2 Incident Response Challenges

The incident response route consisted of three challenges with the fourth being shared with the pen testing route, see Section 4.1.2. The first task, IR1, requires recovering the location of the ‘dropbox’, which was a Raspberry Pi device with a screen on it. Completing the incident response challenge can be done through log investigation, identifying there has been an attack, and locating a Uniform Resource Locator (URL) of a defaced website. Viewing the source page of the website shows the location of the ‘dropbox’. IR2 entails identifying and stopping an attack, which consisted of identifying and stopping a curl attack coming from the ‘dropbox.’IR3 necessitates recovering a secret code. The secret code is hidden in a drawn picture and can only be revealed using a black light.

4.5 Room Design

The mobile room was created in a 10x20 tent, as conferences do not always have rooms available. The tent contains 4 analyst consoles, each of which has a monitor and keyboard powered by a Raspberry Pi device. It has been designed (Figure 4.4) with the storyline in mind. The desks for each of the analyst consoles were positioned next to each other to promote team work. The TV is used to show the introductory and background videos. Visually, the room also has LEDs running on the desks to help participants identify progress and challenge location.

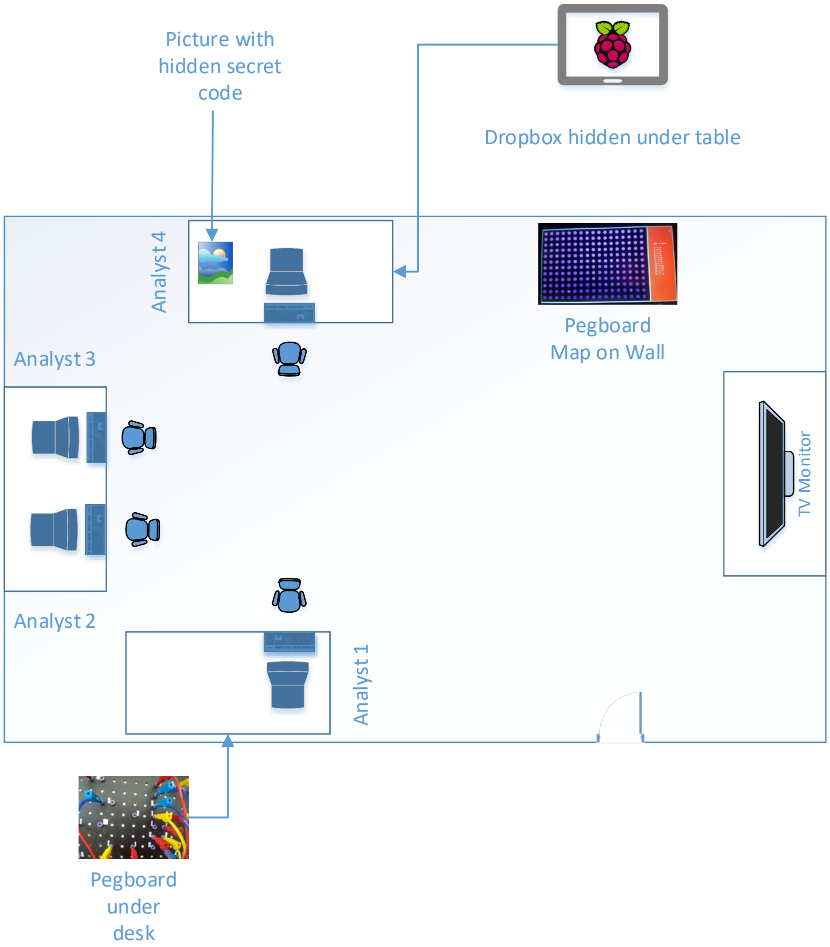


Figure 4.4 - Room design

4.6 m-ICE Architecture

The architecture, as shown in the network map (Figure 4.5) involves many different technologies. Hardware included Raspberry Pi devices, an Intel Next Unit of Computing (NUC), DELL Desktop, and a router were used as well as LED lighting, matrix display panels and sound-effect generation. The software used in the study included honeypots (Cowrie SSH/Telnet Honeypot), Python, ProjectSend (a vulnerable application derived from Damn Vulnerable Pi (DV-Pi)), Kali Linux, Raspbian, Message Queuing Telemetry Transport (MQTT), and GitLab were used. The participants, or the analysts, used Raspberry Pi devices as their consoles (Figure 4.4).

Table 4.1 - Platforms and Use

Platform	**Use**
Cowrie	Honeypots for SSH challenges (log analysis, launch subsystem).
Kali Linux	Finding dictionary file and launching password attack.
Raspbian-Desktop	Analyst desktops.
Raspbian-Lite	IOT devices (LED, Pinboard, Timer).
MQTT	Eventhub service.
ProjectSend	Run on VM for performance. SQLi and launch website. Rewritten, themed and integrated to MQTT signaling.
Python 2.7/3.7	Used for all development. Flask used for all websites except DVPi. Tkinter used for surveys and modal displays.
BASH scripts	Used for analyst console lockdown and hardening.
Asus AC86 Router	Edge router and Hotspot
Netgear POE switch	POE to Raspberry Pi devices and network connectivity (wired)

Table 4.1 Continued

Intel NUC	ESXi Server 1
Dell Desktop	ESXi Server 2
GitLab	Source code management.

Extensive egress filtering was used on the Kali box to prevent participants from attacking network infrastructure. One network was setup with multiple honeypots to discourage hacking the whole network. The particular honeypot used can be seen as a limited Linux system where activities, such as Linux commands, do not carry over outside of the environment.

MQTT was used as an eventhub to communicate between machines and set off the actions as indicated in Table 4.2.

Table 4.2 - MQTT Eventhub Topics

MQTT Topics	**Used by (Roles)**	**Description**
audit/[mac]	All	Audit logs (CSV Timestamped, generated by publogger function)
mgmt	None	All management subtopics
mgmt/[role]	All	See below:
mgmt/analyst	Analyst Consoles	Global analyst channel
mgmt/analyst/#	Analyst Consoles	Analyst desktop Pi's. Opens URL in Kiosk mode if known, or browser mode if unknown [STRING]

Table 4.2 Continued

mgmt/av1	Media Players	TV/Sound system - plays provided filename (absolute path) [STRING]
mgmt/mac	All	Topics to join. Global ROLE is set to last-provided role.
mgmt/mastercommander	All	Receives expected strings (soft-reset, hard-reset, heartbeat)
mgmt/matrix	Matrix Display	Matrix control - triggers start/stop/pause/resume [STRING]
mgmt/register/mac	All	Registration channel to request 'role'
mgmt/time	Matrix Display, Timer Visuals	Matrix library - provides 10s countdowns [INT]
mgmt/vote	Analyst Consoles	Vote initiation (NAME;Question;Response1;Response2) [CHAR;STRING;STRING;STRING]
score/reset	Analyst Consoles	Resets if '0' received.

4.7 Network Design

An overview of network design is shown in Figure 4.5. All devices using the ‘ice-agent’ were allocated using DHCP and communicated via the MQTT eventhub server using predefined topics. This allows ‘drop-in’ replacement of Raspberry Pi devices without changing the network architecture. The network range used was 172.16.31.0/24.

The central Raspberry Pi imaging and stateless PXE boot configuration meant that the entire environment can be reset within 2 minutes to its initial state, even if participants have compromised a local device.

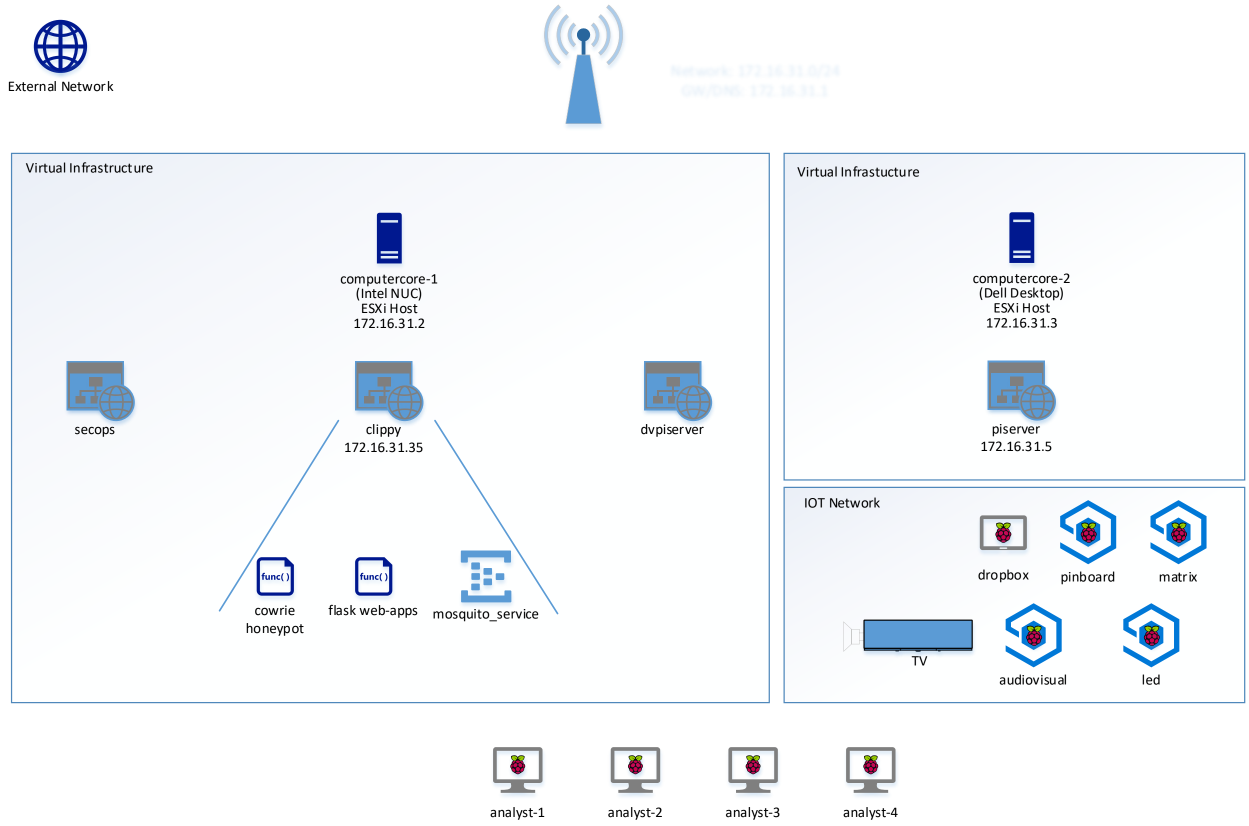


Figure 4.5 - Network Design

4.8 Experiments

After initial development and testing, three experiments were performed. The first experiment, conducted as a proof of concept, was done at a security conference, and attracted many professionals, although only one female participant. The second and third experiments were performed at a college and drew the attention of college students and non-college students consisting of both those not in cybersecurity and those that were.

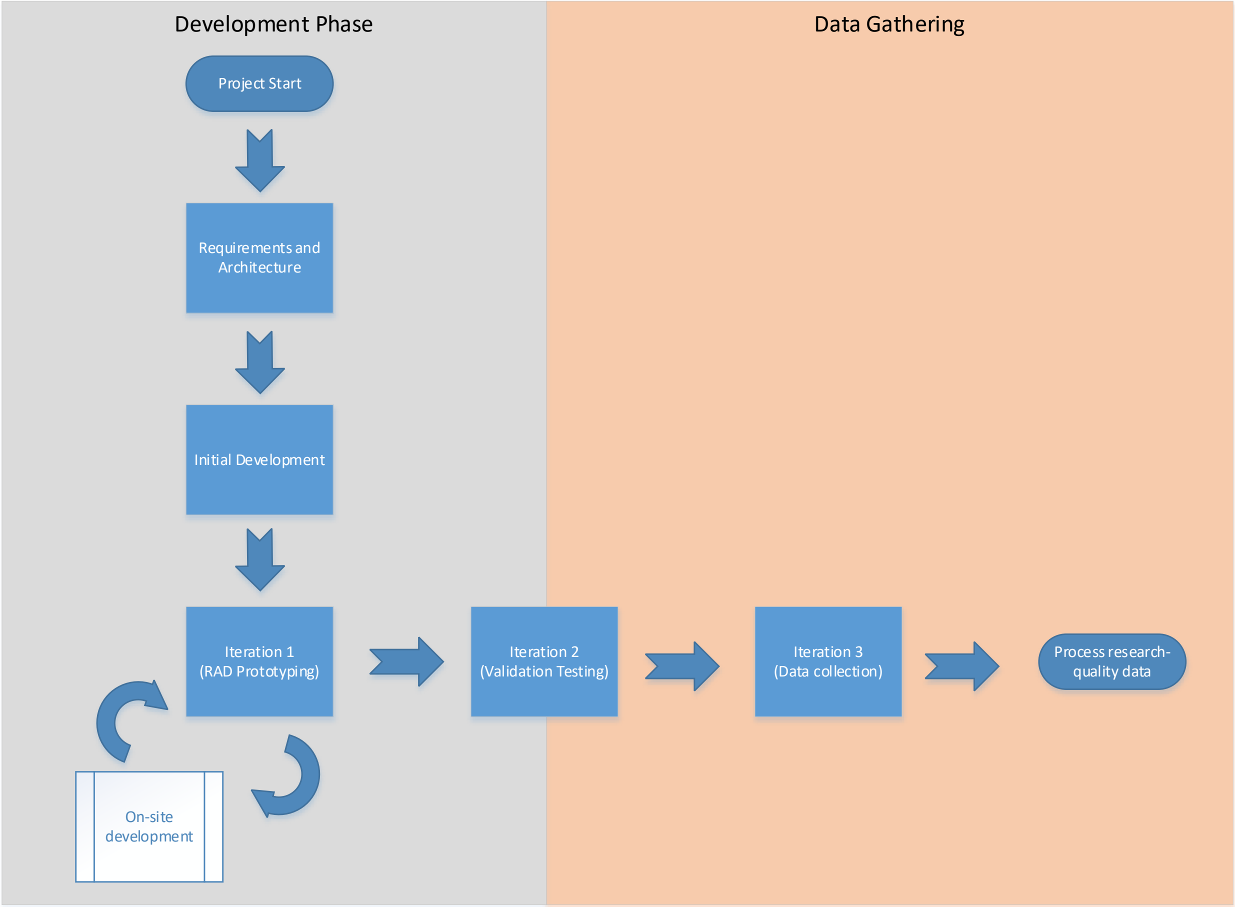

Development Phase
Data Gathering
Project Start
Requirements and Architecture
Initial Development
Iteration 1 (RAD Prototyping)
On-site development
Iteration 2 (Validation Testing)
Iteration 3 (Data collection)
Process research-quality data

Figure 4.6 - Approach to Research (Scope of Study)

4.8.1 Iteration 1

In order to perform a test of feasibility for this idea, it was decided to set up the m-ICE at the Red Sky Security conference. A signup sheet with times and team numbers was offered to attendees via a booth. These volunteers were then given the choice to take on the penetration testing route or the incident response route. For this iteration, cybersecurity professionals were targeted. Seven teams, each person with a background or interest in cybersecurity, participated in the m-ICE. Team sizes consisted of 3-4 people.

4.8.2 Issues Encountered and Refinements

The primary issue for the first iteration was overall readiness. Setting up the mobile environment took several hours longer than anticipated and the relocation introduced some anomalies into the network topology. Addressing these caused a loss of the day one of data collection meaning only eight teams instead of the expected 20 were able to participate. The majority of the participants were male with one female among the 32 total participants.

Bugs encountered in transitions were expected at this stage, and development occurred onsite between challenges.

Initially, it was attempted to have two tracks ready for the initial experiment but ran into the problem that the incident response challenges were not connecting to each other. There were no technical triggers to set off the incident response challenges following one another. Another problem faced concerned the inexperience of the participants. Many of the participants were unfamiliar with hydra or SQL injection, and did not completely understand the launch console challenge (P3). Bugs in the penetration testing route meant that timing had to be manually advanced.

When testing the IR route, we found that the challenges were not well integrated technologically and lacked narrative cohesiveness. This caused some confusion among participants. For the first challenge (IR1), they had trouble locating the crew logs. They also had trouble identifying that the logs indicated a phishing attack. The defaced website had also not been attached to the challenge. Since the IR route was not technically connected, the majority of the participants were only able to choose one route to go through (penetration testing).

When the participants were observed to be struggling a person was set up in the tent with the participants, acting as the “Artificial intelligence” or “AI” of the base. They were to give hints to the team in the m-ICE whenever they struggled for too long. After a number of teams went through the m-ICE, it was observed that the given hints tended to vary from team to team and needed to be more uniform to address bias and for the experiment to be consistent.

4.8.3 Iteration 2

The second iteration had fifteen teams participate and their team sizes ranged from 2-4 people. Of these, twelve teams provided complete data. For the teams with incomplete data, technical issues occurred and thus the data gathered was considered to be incorrect and/or inconsistent. The audience came from the local area, college students and employees, as the experiment was conducted on a college campus. The second iteration involved testing the implementation of the second route, incident response as well as multiple enhancements and bug fixes. This iteration allowed participants to choose which route they would like to take for the m-ICE, pen testing or incident response. This iteration involved a more refined pen testing route (Figure 4.7).

The challenges revised, as show in Figure 4.7, were P1 and P2. In P1, there were two possible methods laid out for participants, (P1a) locating the password found on a sticky note under one of the keyboards or (P1b) brute-forcing the password using a dictionary attack via hydra. The goal for the second challenge was to gain web access. To do this, they could (P2a) perform a SQL Injection, (P2b) use default credentials, or (P2c) brute-force the passwords.

Incident Response (IR) enhancements included implementing triggers, automation and testing into the process with some enhancements (Figure 4.8).

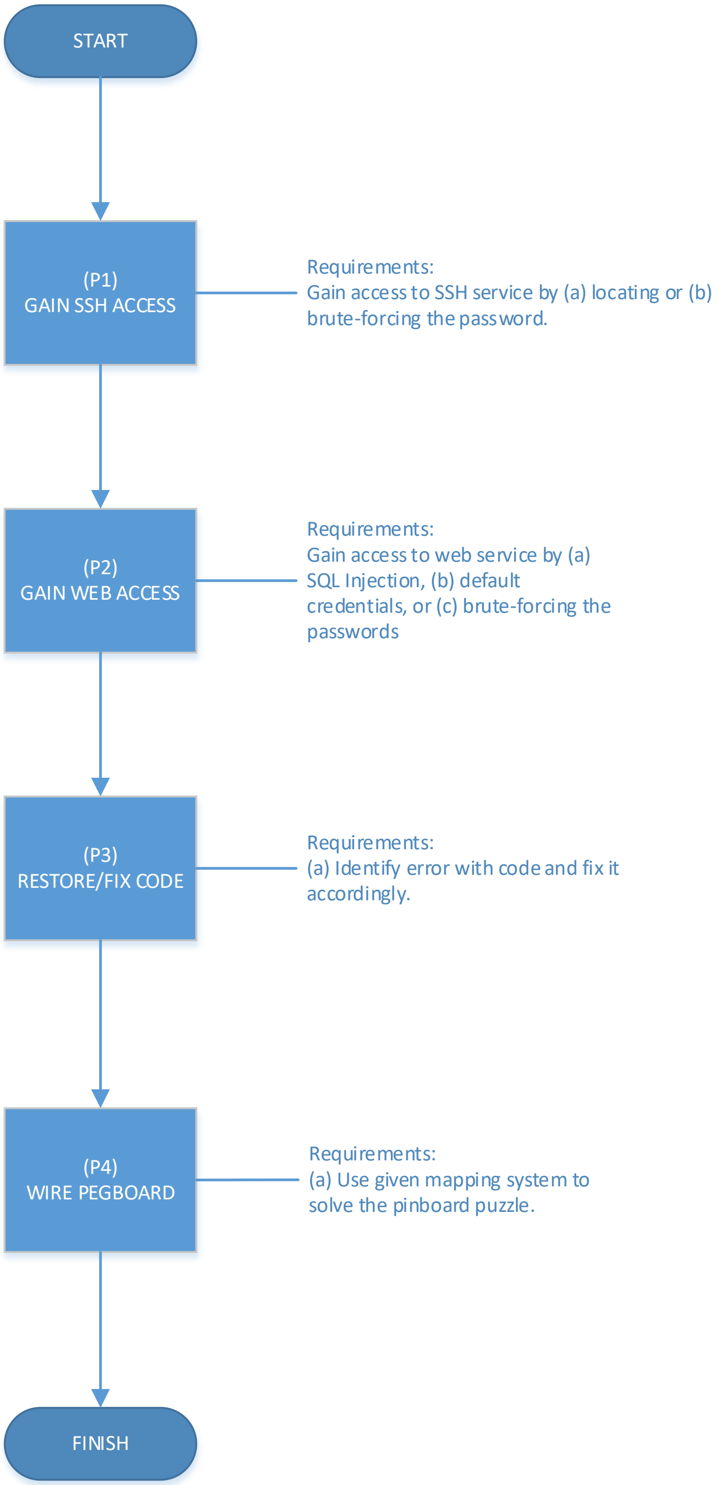

START
(P1)
GAIN SSH ACCESS
Requirements:
Gain access to SSH service by (a) locating or (b) brute-forcing the password.
(P2)
GAIN WEB ACCESS
Requirements:
Gain access to web service by (a) SQL Injection, (b) default credentials, or (c) brute-forcing the passwords
(P3)
RESTORE/FIX CODE
Requirements:
(a) Identify error with code and fix it accordingly.
(P4)
WIRE PEGBOARD
Requirements:
(a) Use given mapping system to solve the pinboard puzzle.
FINISH

Figure 4.7 - Iteration 2: Revised Penetration Testing Scenario

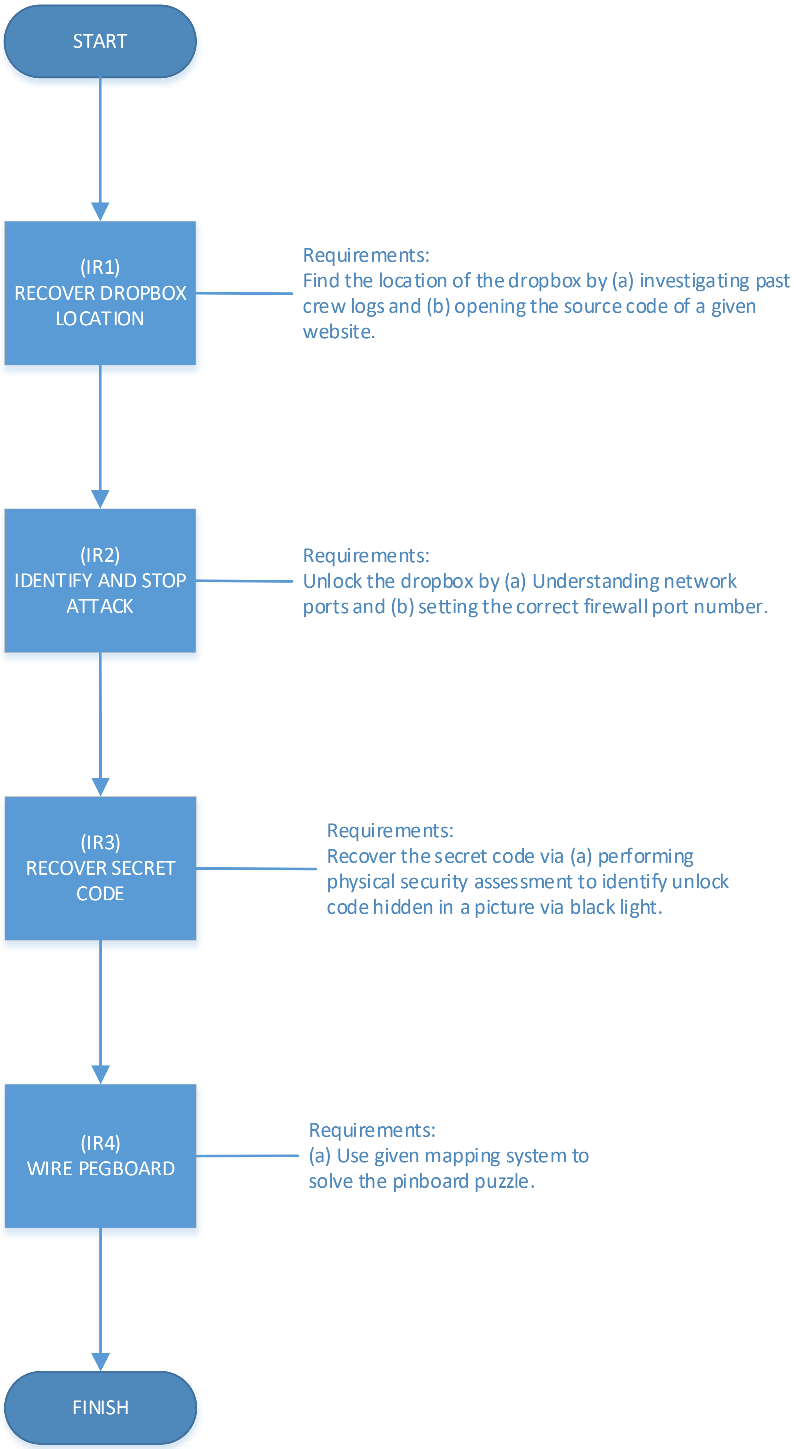

START
(IR1)
RECOVER DROPBOX LOCATION
Requirements:
Find the location of the dropbox by (a) investigating past crew logs and (b) opening the source code of a given website.
(IR2)
IDENTIFY AND STOP ATTACK
Requirements:
Unlock the dropbox by (a) Understanding network ports and (b) setting the correct firewall port number.
(IR3)
RECOVER SECRET CODE
Requirements:
Recover the secret code via (a) performing physical security assessment to identify unlock code hidden in a picture via black light.
(IR4)
WIRE PEGBOARD
Requirements:
(a) Use given mapping system to solve the pinboard puzzle.
FINISH

Figure 4.8 - Iteration 2: Revised Incident Response Scenario

4.8.4 Iteration 2 Refinement

This iteration appeared to attract many non-cybersecurity people. Due to this, while the participants were completing challenges, a need for more hints, and especially tutorial-like hints, were identified. Some limitations in sandboxing were identified to reduce the possibility of participants having access outside of the project scope at times when it was not conducive to solving problems. For example, one participant accessed their social media account during the experience. After each challenge, the IR route would be refined to better incorporate immersion and storyline.

4.8.5 Iteration 3

The final iteration of m-ICE included all the fixes and enhancements discussed so far. The platform had been completed to a mobile readiness and initial data collection had begun. A complete systems architecture diagram is shown in Figure 4.9. The figure shows the front end and the back end of the m-ICE.

The third iteration included twenty-five teams whom participated and their team sizes ranged from 2-4 people. Of these teams, only twenty-three provided complete data. Participants included college students interested in cybersecurity or in the idea of an escape room as well as college employees or local residents in the area.

Iteration 3 was performed as a more verified method. It consisted of another round of experimentation with more fleshed out elements from iteration 1 and 2. Automation of the platform had been greatly enhanced. Challenges and triggers for each challenge had been incorporated in the m-ICE and a more fleshed out mapping (Figure 4.11) had been created. This mapping includes the triggers, challenges, requirements, and storyline. The triggers help automate the challenges to follow one after another. The voting system had been fully integrated. More hints had been implemented as tutorials to be show on the TV in the room. Tutorials such as (Figure 4.10) were implemented as a last resort if participants were unable to solve the challenge in a reasonable time frame. These tutorials gave participants a step by step guide or examples for how they can solve the given challenges. For those who had received the tutorial, they appreciated the guide or only had to glance at it to know what direction they should have been heading instead.

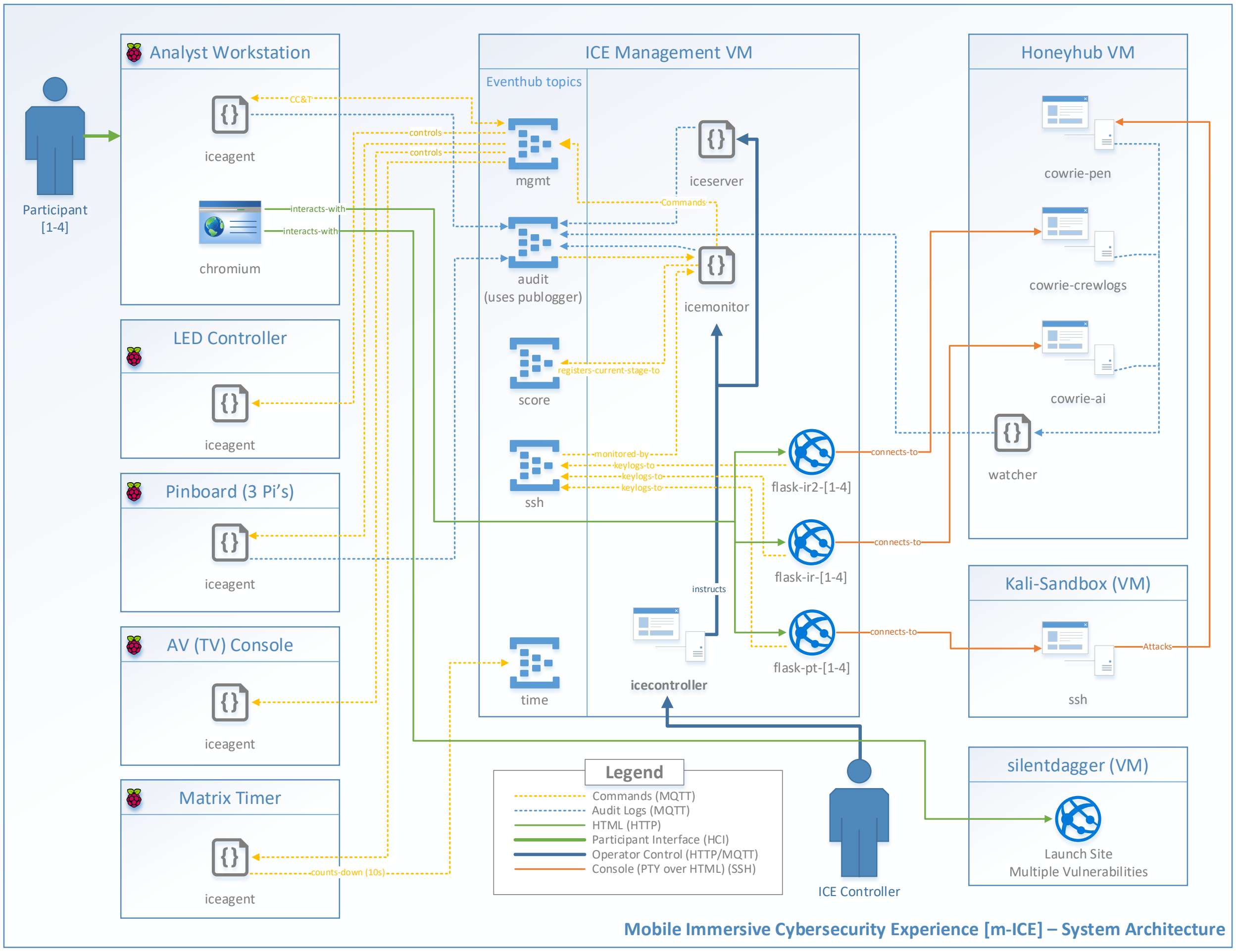
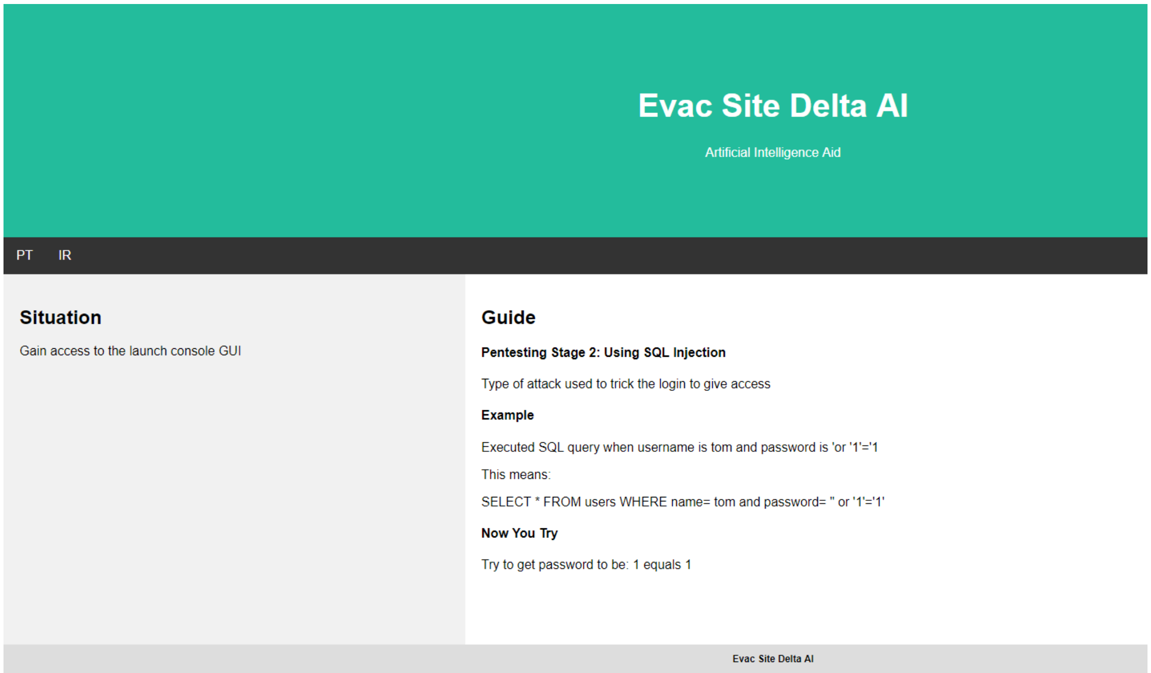


Figure 4.9 - Final Systems Architecture



Evac Site Delta AI

Artificial Intelligence Aid

Situation

Gain access to the launch console GUI

Guide

Pentesting Stage 2: Using SQL Injection

Type of attack used to trick the login to give access

Example

Executed SQL query when username is tom and password is 'or '1'='1

This means:

SELECT * FROM users WHERE name= tom and password= '' or '1'='1'

Now You Try

Try to get password to be: 1 equals 1

Evac Site Delta AI

Figure 4.10 – Tutorial for P2

4.8.1 Iteration 3 Refinements

The refinements for iteration 3 centered around automating data gathering and parsing the results from data gathering. This was seen as a worthwhile investment towards having more consistent data that could then be analyzed.

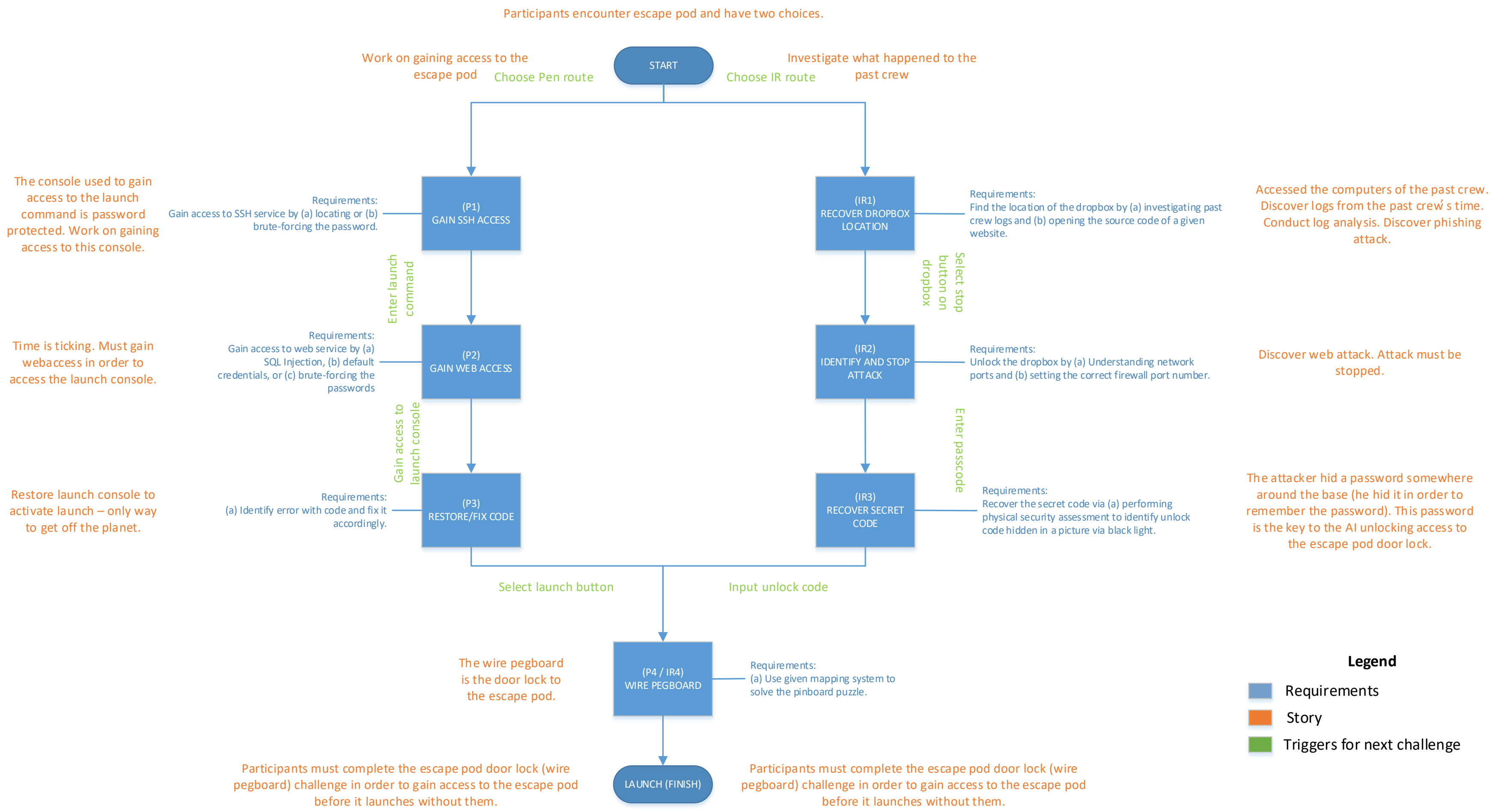

Participants encounter escape pod and have two choices.
START
Work on gaining access to the escape pod
Choose Pen route
Choose IR route
Investigate what happened to the past crew
The console used to gain access to the launch command is password protected. Work on gaining access to this console.
Requirements: Gain access to SSH service by (a) locating or (b) brute-forcing the password.
(P1) GAIN SSH ACCESS
(IR1) RECOVER DROPBOX LOCATION
Requirements: Find the location of the dropbox by (a) investigating past crew logs and (b) opening the source code of a given website.
Accessed the computers of the past crew. Discover logs from the past crew's time. Conduct log analysis. Discover phishing attack.
Enter launch command
Select stop button on dropbox
Time is ticking. Must gain webaccess in order to access the launch console.
Requirements: Gain access to web service by (a) SQL Injection, (b) default credentials, or (c) brute-forcing the passwords
(P2) GAIN WEB ACCESS
(IR2) IDENTIFY AND STOP ATTACK
Requirements: Unlock the dropbox by (a) Understanding network ports and (b) setting the correct firewall port number.
Discover web attack. Attack must be stopped.
Gain access to launch console
Enter passcode
Restore launch console to activate launch – only way to get off the planet.
Requirements: (a) Identify error with code and fix it accordingly.
(P3) RESTORE/FIX CODE
(IR3) RECOVER SECRET CODE
Requirements: Recover the secret code via (a) performing physical security assessment to identify unlock code hidden in a picture via black light.
The attacker hid a password somewhere around the base (he hid it in order to remember the password). This password is the key to the AI unlocking access to the escape pod door lock.
Select launch button
Input unlock code
The wire pegboard is the door lock to the escape pod.
(P4 / IR4) WIRE PEGBOARD
Requirements: (a) Use given mapping system to solve the pinboard puzzle.
Legend
🟦 Requirements
🟧 Story
🟩 Triggers for next challenge
Participants must complete the escape pod door lock (wire pegboard) challenge in order to gain access to the escape pod before it launches without them.
LAUNCH (FINISH)
Participants must complete the escape pod door lock (wire pegboard) challenge in order to gain access to the escape pod before it launches without them.

Figure 4.11 - Expanded Scenario

5 ANALYSIS AND FINDINGS

5.1 Introduction

The data collection of the research incorporated 35 teams. Although most of this data was gathered from iteration 3, there were twelve teams from iteration 2 that provided usable data and were thus included.

Each team consisted of 2-4 participants, with 109 total participants, 74 males and 36 females. There was a total of 23 teams that contained gender diversity. Of the same gender teams, there was one female team of size two, with the remaining eleven teams being all-male. Proficiency (see Initial Survey) was rated across four categories where participants were asked to rank their knowledge on a 5-point scale. Half (37) of all male participants self-assessed as 'Moderately Knowledgeable' or higher in one or more categories versus 7 (19%) females. Although only limited significant conclusions were found due to the sample size, the existing data seemed to suggest that heterogenous teams are more effective than homogenous teams, in particular when the woman has prior cybersecurity experience, certifications or knowledge.

5.2 Findings

Figure 5.1 observes the relationship between challenges completed and the gender diversity in teams, with reference to the team cyber experience. The 'challenges completed' is referring to the number of challenges completed by the teams. The challenges included for this are the first three challenges from each route. The fourth challenge was not considered due to the low number of teams that completed it, proving insignificant to the data. The 'Gender Diversity' refers to if the teams are homogenous (0) or heterogenous (1). Homogenous teams were those with all members of the same biological sex. Heterogenous were teams with all members of differing biological sex. The 'Team Cyber Experience' is a binary value equated through answers from questions in the initial survey, whether at least one member of the team held any cybersecurity history (Q23), considered themselves a cyber professional (Q19), or held any cybersecurity qualifications/certifications (Q14).

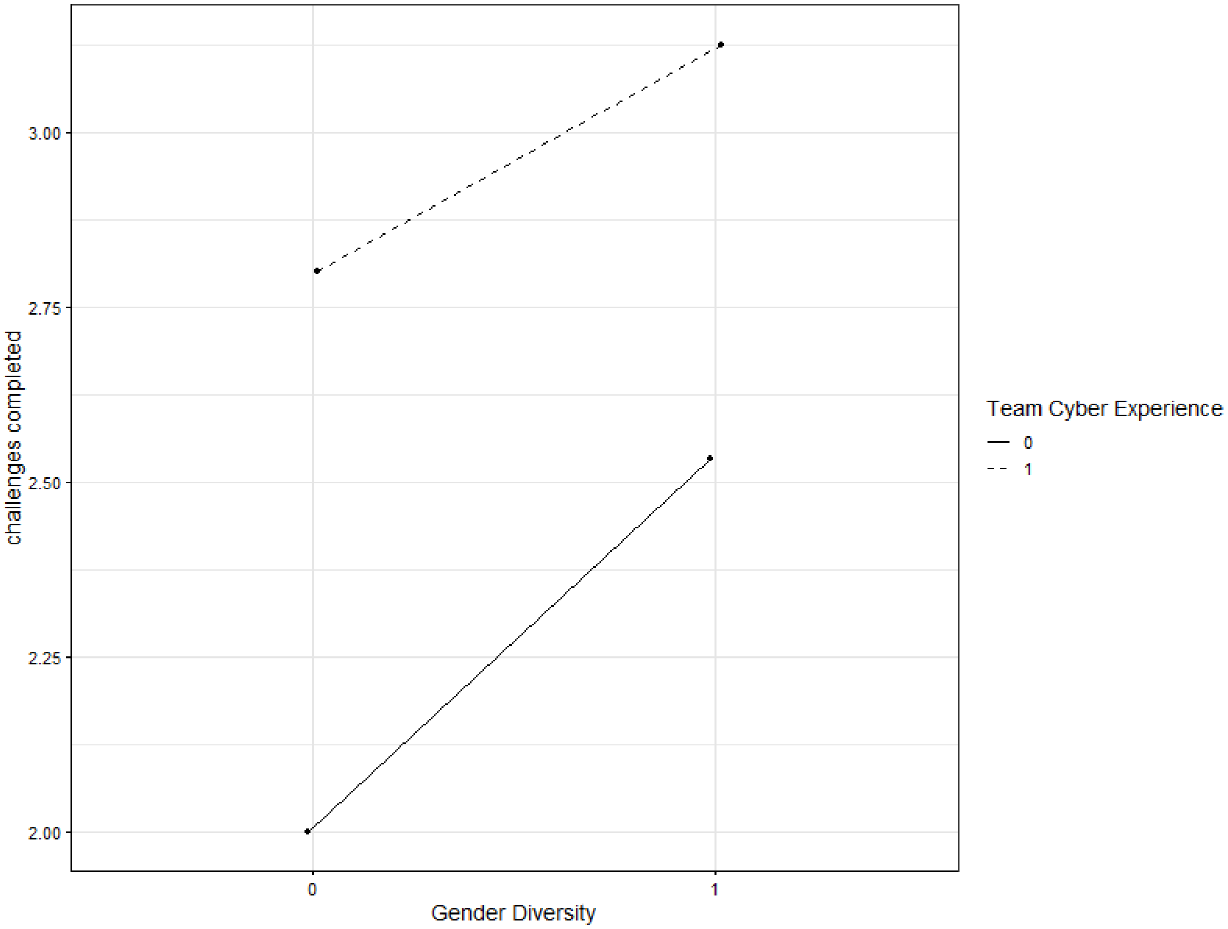


Figure 5.1 Relationship between Gender Diversity and Challenges Completed with Respect to Team Cyber Experience

Figure 5.1 details that both the teams with no cyber experience and with cyber experience completed more challenges with heterogenous teams rather than homogenous teams. This data suggests heterogenous teams may help increase the amount of challenges that are solved.

Figure 5.2 details the relationship between gender diversity and challenges completed, with reference to Team Cyber Proficiency. In this figure, the fourth challenge is included. The 'Team Cyber Proficiency' refers to whether at least one team member on a team answered 'Moderately knowledgeable', 'Very knowledgeable', or 'Extremely knowledgeable' in any of the given fields (Q11) in the initial survey. These fields included: 'Penetration Testing / Pen Testing / Ethical Hacking', 'Incident Response', 'Cybersecurity Management', and 'Security Analytics'. In analyzing Figure 5.2, the homogenous teams with no cyber proficiency appeared to complete fewer challenges than the heterogenous teams of the same cyber proficiency. Heterogenous teams with cyber proficiency tended to complete more challenges than the homogenous teams with cyber proficiency. This supports H1.

Figure 5.3 visualizes the relationship between gender diversity and the time to complete challenges, with respect to the team cyber experience. The "Time to Complete" refers to the total amount of time it took for the teams to complete all four challenges. The time was determined as a score due to the time limit given. If any challenges were not completed, teams would receive a time penalty. The following formula was used to calculate the time for each team:

Time to Complete (s) = 1500s + (375s * #challenges not completed)

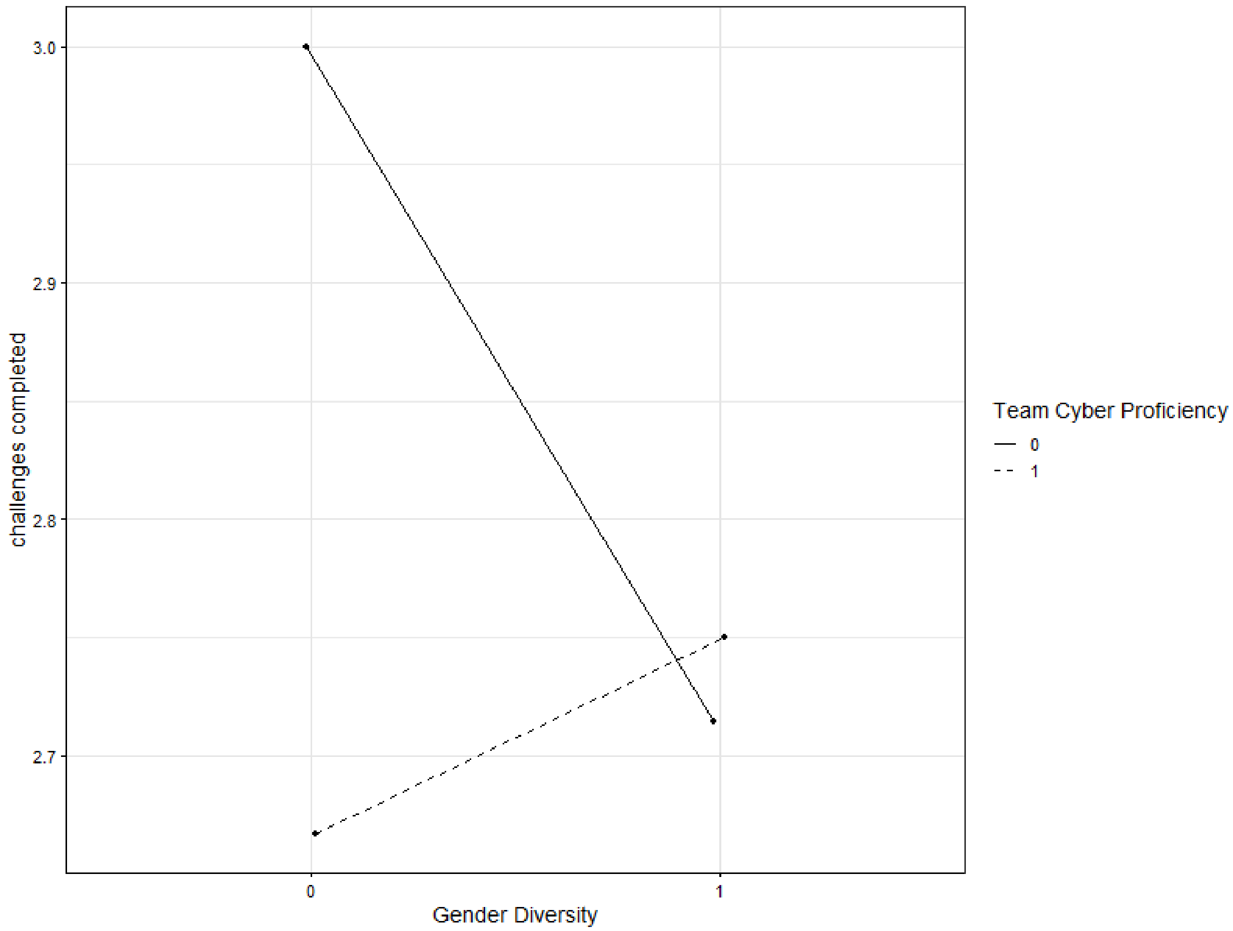


Figure 5.2 Relationship between Gender Diversity and Challenges Completed with Respect to Team Cyber Proficiency

The time limit given for each team was 25 minutes, or 1500s. The penalty time, 375s, was calculated based on dividing the total time given, 1500s, divided by the total number of challenges given, 4.

In Figure 5.3, the homogenous teams without cyber experience were observed to perform slower than the heterogenous teams. The homogenous teams with cyber experience also performed slower than the heterogenous teams. The data suggests heterogenous teams may complete challenges quicker than homogenous teams.

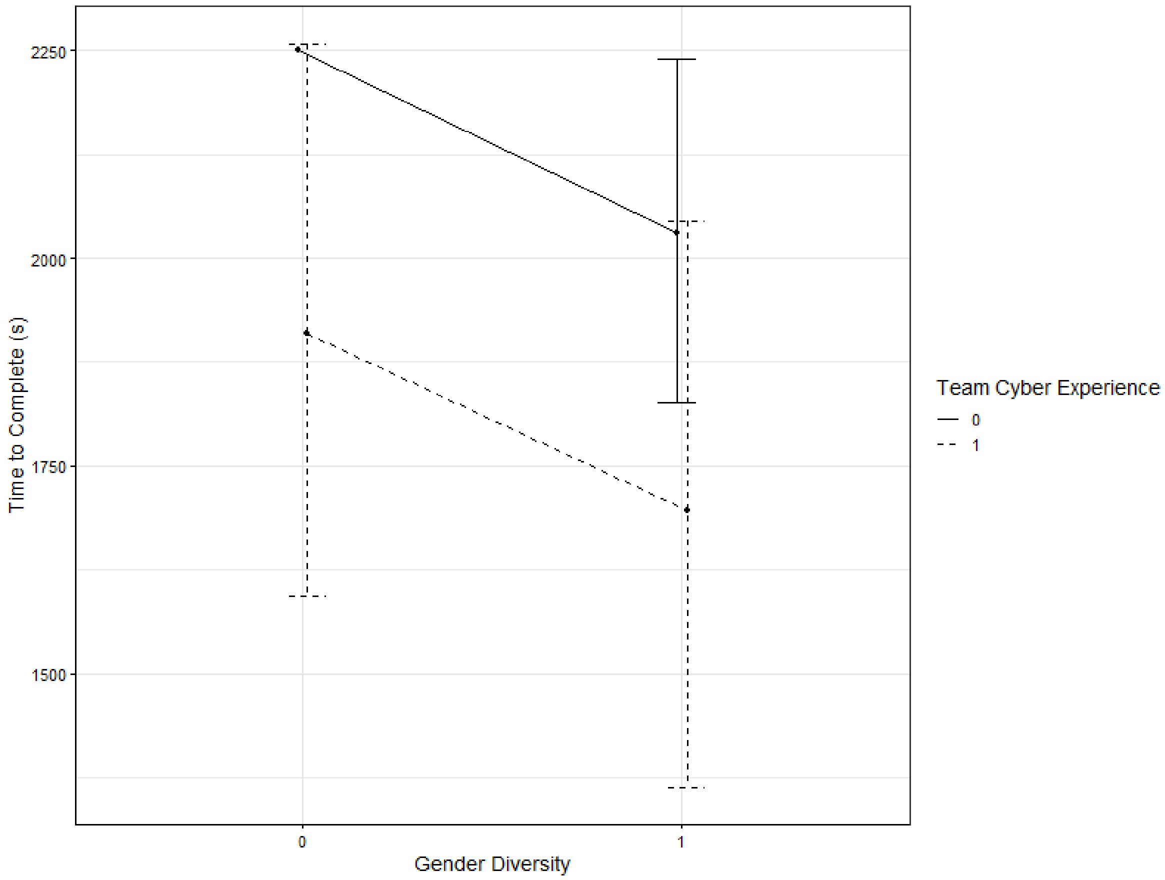


Figure 5.3 Relationship between Gender Diversity and Time to Complete with Respect to Team Cyber Experience

Figure 5.4 observes the relationship between gender diverse teams, and the time to complete the challenges with respect to the team cyber proficiency. The homogenous teams with no cyber proficiency completed fewer challenges than the heterogenous teams. The homogenous teams with cyber proficiency completed more challenges than the heterogenous teams. As proficiency was measured as a team factor, it cannot be determined from this chart if both genders had proficiency. It was noticed that if female team members did not have proficiency, males would slow down their progress in order to teach their other teammates.

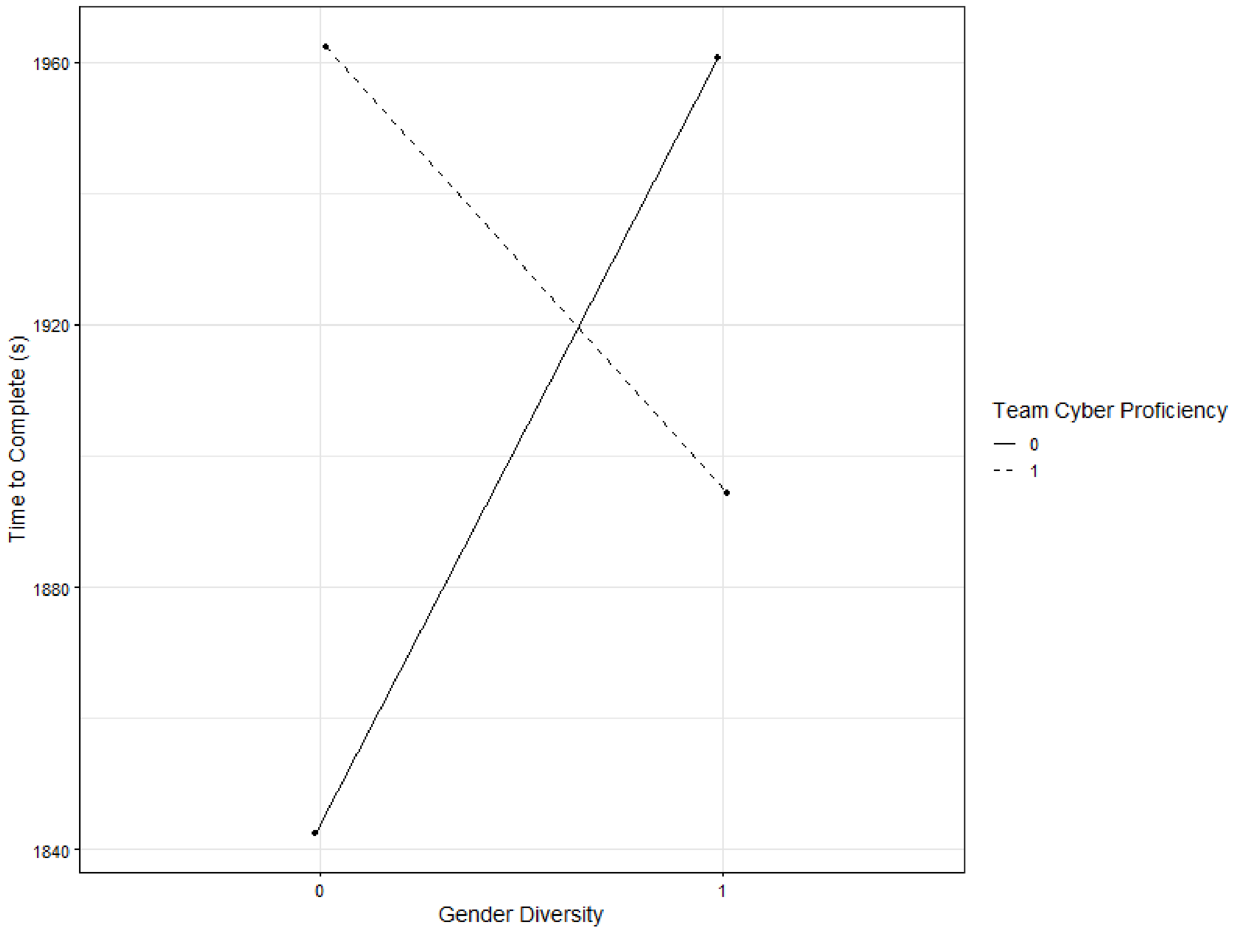


Figure 5.4 Relationship between Gender Diversity and Time to Complete with Respect to Team Cyber Experience

5.3 Anecdotal Observations

5.3.1 Communications

There was one particular team of members who knew each other prior to the m-ICE activity, that chose to participate together. They did not communicate to each other at all until the last challenge, where one of the teammates spoke out loud, that they should probably talk to each other. During the first three challenges, only one person solved it and did not let his/her teammates know. The other teammates seemed to not know or care how or why the challenges were progressing and just accepted it.

Many teams had tunnel vision, or worked individually without being aware of surroundings and other people, when working on the challenges. They would not see the hints given or would gloss over them and deem them as unimportant despite strong audio cues to their presence. Due to this tunnel vision, many of the teams seemed to struggle for a longer amount of time, and became aware of this only after the event when the notifications and clues were shown to them.

5.3.2 Diversity of Experience

One particular team, consisting of three technical people and one non-technical person, decided to work on the penetration testing route. During the second challenge, it was the non-technical person whom figured out how to use SQL injection. This offers the idea that having a different perspective is great to have on a cybersecurity team.

5.4 Significance of Findings Using Multiple Linear Regression

When considering both routes through the first three challenges, females with cyber experience is a significant factor in reducing the time to solve challenges when considering gender diversity, male experience and female experience.

```
Call:
glm(formula = time_to_c4 ~ route + sex_num + femalecyberstuff + 
    malecyberstuff + MaleCyberProficiency + FemaleCyberProficiency, 
    data = dat)

Deviance Residuals: 
    Min       1Q   Median       3Q      Max
-221.15   -64.89   -46.27    81.92   212.73


Coefficients:
                       Estimate Std. Error t value Pr(>|t|)
(Intercept)            1048.578    272.975   3.841  0.00396 **
route                   149.450    173.286   0.862  0.41083
diversity                24.238    123.619   0.196  0.84891
femalecyberstuff1      -932.586    301.753  -3.091  0.01292 *
malecyberstuff1        -142.977    154.457  -0.926  0.37877
MaleCyberProficiency      9.032     11.651   0.775  0.45808
FemaleCyberProficiency   66.855     32.757   2.041  0.07165 .
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1
```

Raw findings are listed in the Appendix. However, for all cybersecurity challenges 1-3 (C1-C3), females with cyber experience were shown to reduce the total time taken with statistical significance. This remains true in the incident response challenges. In the penetration testing challenges, the indicators show the same patterns but there were not a sufficient number of female participants to provide significance.

5.5 Limitations

While attempts were made to recruit more women into participating for this experiment, they seemed reluctant or had no interest to attempt it during the first iteration. The women who did approach the booth at the conference for registration for the m-ICE seemed somewhat intimidated at the technical aspect included. There were more women, who did not have a technical background, who participated at the later iterations. This was possibly due to these iterations being hosted in a more casual setting, so much so that participants usually turned it into a date night, a friend’s activity, or a family night. In these cases, some women were participating because their gender counterpart was interested in the escape room and had little-to-no cybersecurity experience.

There were problems gathering the correct sample from targeted cybersecurity professionals. This could have been due to the small sample size and problem with generating enough interest, especially for women. Women cybersecurity professionals did not seem as interested in the m-ICE as men. There was only one female homogenous team whom participated in all three iterations. The rest of the homogenous teams were male. In the future, the recommendation would be to setup the m-ICE at an event where women with an interest in cybersecurity are known to be. This would provide better representative data.

5.6 Review: Purpose of the Research

In an attempt to address the purposes of the research (refer to section 1.2), the following sub sections have been provided.

5.6.1 Definition of Team Effectiveness

Through reviewing the literature review, an appropriate definition of ‘team effectiveness’ with respect to cybersecurity teams has been identified. Team effectiveness is a “ holistic perspective in considering not only whether the team performed (e.g., completed the team task) but also how the team interacted (i.e., team processes and teamwork) to achieve the team outcome” [11][12].

5.6.2 Key Technical and Non-Technical Skills

The key technical skills focus primarily on penetration testing and incident response. These key technical skills both share Linux command line as the consoles they primarily used are Linux based. Penetration testing focuses on reconnaissance, password attacks, web vulnerability assessment, SQL injection, and Web-site reconnaissance. Incident response focuses on the forensics of review of log files, web compromise investigation, physical compromise investigation, firewall configuration, and attack containment.

5.6.3 Construction of a Framework

The m-ICE was created as the framework for delivering representative cybersecurity challenges with the skills mentioned in section 2.2. As mentioned in section 3.5, the m-ICE incorporates two tracks, penetration testing and incident response, that deliver a total of four challenges, each sharing the fourth one. The m-ICE incorporates all of the requirements for the framework listed in section 3.3, with the additional effect of mobility. This framework was created to help easily measure the technical and non-technical skills mentioned in section 5.6.2.

5.6.4 Validation Study of the Framework

A validation study of the framework (section 0) was conducted using homogenous and heterogeneous teams in three iterations. Although an attempt at using homogeneous and heterogeneous teams was made, there was only one gender diverse team that volunteered and the number of females in the cybersecurity profession was found lacking at iteration 1. At iteration 2, more non-cybersecurity professionals took an interest and took part in the m-ICE. This might support the idea that there are not many women in cybersecurity. As several approached the room but did not sign up, it may also support the idea that women hold more self-efficacy problems in participating in something targeting STEM. Although with iteration two, there were more gender diverse teams taking part in the experiment.

5.7 Responses to Research Questions and Hypotheses

This section addresses the questions and hypotheses created for this study.

- Q1. What is an appropriate definition of team effectiveness in the cybersecurity domain?

  Team effectiveness: A " holistic perspective in considering not only whether the team performed (e.g., completed the team task) but also how the team interacted (i.e., team processes and teamwork) to achieve the team outcome [11][12]."

- Q2. What subdomains of cybersecurity should be targeted for this study?

  As mentioned in section 3.1, the subdomains were decided based on the Certified Information Systems Security Professional (CISSP) Common Body of Knowledge (CBK) defined by the $(ISC)^2$. The subdomains chosen are penetration testing, which falls under the "Security Assessment and Testing" domain, and incident response, from the "Security Operations" domain [33]. Informal feedback during post-event discussions indicated that participants were happy with this choice, with most having a predisposition to one or the other track.

- Q3. How can effectiveness be measured in cybersecurity teams involved in technical problem-solving?

  Effectiveness was measured in cybersecurity teams through a combination of performance metrics, team observation and normalized with survey data. A framework, as mentioned in section 3.3, was created to help create a setting where team effectiveness could be measured. This was created by an immersive gamified scenario that included real-world cybersecurity problems with extensive monitoring and measurements. The environment was derived from a prior project but involved extensive adaptations to create a portable, mobile environment that can gather data in various locations. Over time, this framework should provide data from a variety of locations that host cybersecurity professionals.

- H1: In line with other disciplines, gender-diversity is beneficial to cybersecurity team effectiveness in tasks that require problem-solving or innovation.

  The research necessitated the design and validation of a framework suitable for collecting this data, as no suitable mechanism was identified in existing research.

  Although there were no significant results found marking diverse teams as beneficial, it was found that teams with one or more female members with cybersecurity experience/knowledge was a significant factor in reducing the time taken to solve the challenges. Thus, it could be expected that if the study were limited to cybersecurity professionals, diversity itself may become more significant.

  The impact of diversity (sex_num) was considered to be one of the leading variables when the gathered data was analyzed using Principle Component Analysis (see Figure 5.5). Other significant factors included team familiarity (TeamFamiliarityScore), team enjoyment (team_enjoy), and ~~certification~~ team size (team_size).

- H2: A method for measuring technical cybersecurity team effectiveness can be used to determine the impact of gender diversity within cybersecurity teams.

  Although a method, m-ICE, has been proposed, as noted, it was not possible to collect significant data related to the impact of gender diversity within cybersecurity teams. Future research is proposed to further study gender diversity. This method has several possible future applications and does not have to be only applied to identifying the impact of gender diversity, but to all kinds of team diversity types.

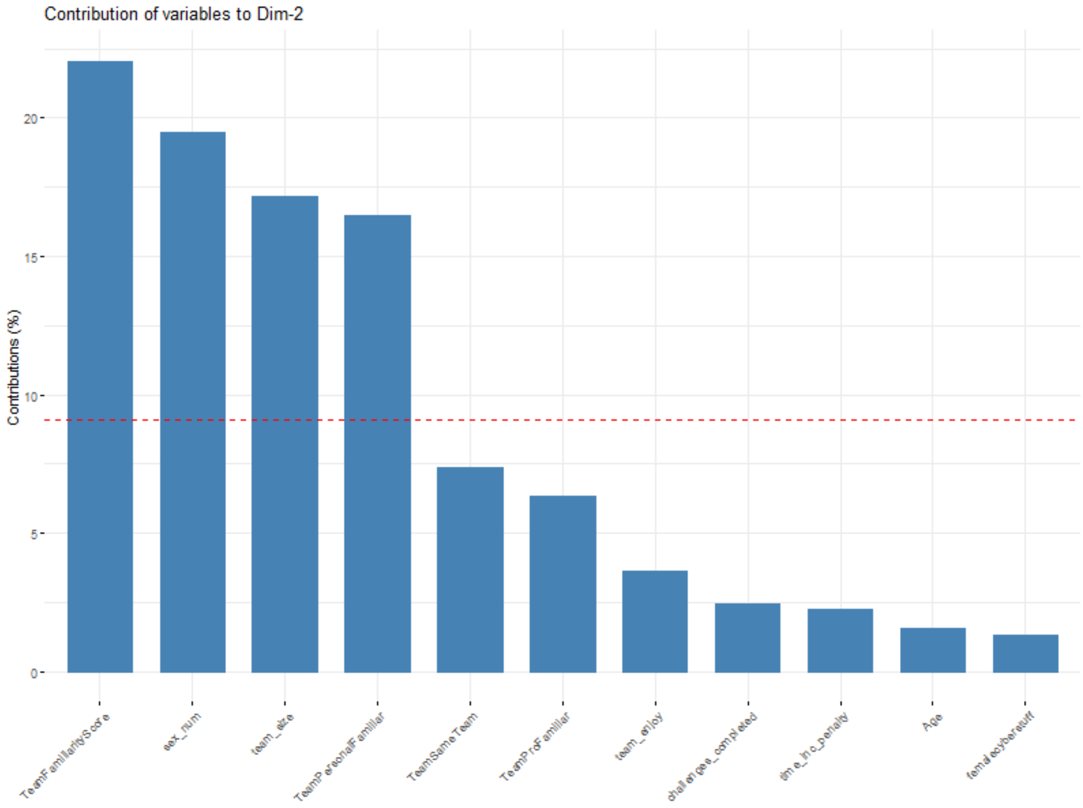


Figure 5.5 Principle Component Analysis Results

5.7.1 Further Findings

Through observing participants and reviewing the data gathered, the suggested and adapted mobility aspect of the m-ICE has increased the opportunities of use for this methodology. Iterations have supported that this framework works and can attract multiple audiences, such as cybersecurity professionals or everyday people.

It was also observed to be an effective tool in enhancing skill development in both previous research (ICE) and the research discussed in this study. Further research is recommended to validate m-ICE's suitability as an educational tool.

5.8 Research Contribution:

The following is a summary of the research performed:

1. Identified a problem (lack of women in cyber).
2. Identified a lack of research in cybersecurity technical team effectiveness.
3. Identified there are challenges with measuring technical team effectiveness.
4. Identified criteria for a mobile environment to measure team effectiveness:
   a. Immersive/engaging
   b. Structured ability to measure (consistently and at a technical level).
   c. Environments to measure this should encourage teamwork.
   d. Team performance should be optimal when there are complimentary and overlapping skills.

   e. Adaptable, environment should normalize for the team as they progress and adjust difficult to compensate, focusing on the teams potential to be effective in a technical task.

   f. Normalized for bias in highly skilled or experienced individuals.

5. Identified a model (ICE) that may be useful for this study.

6. Identified issues with current model (ICE).

7. Proposed an adaptation of the current model (m-ICE).

8. Designed and constructed m-ICE.

9. Conducted a study with two experiments to validate that the model works.

10. Presented a refined final model suitable for data gathering.

5.9 Future Questions

There are many potential possibilities for what m-ICE can be used for. It could be used to increase awareness and interest in cybersecurity. It could also be used for a team building exercise.

1. What is the suitability of m-ICE as a learning platform?

2. What is the suitability of m-ICE as a team effectiveness enhancement (team-building) platform?

3. What is the suitability of m-ICE to recruit women and diverse groups into cybersecurity?

6 REFERENCES

[1] I. Palo Alto Networks, “What is Cybersecurity?,” *Palo Alto Networks, Inc.* [Online]. Available: https://www.paloaltonetworks.com/cyberpedia/what-is-cyber-security. [Accessed: 22-Apr-2019].

[2] National Initiative for Cybersecurity Careers and Studies, “Glossary | Explore Terms: A Glossary of Common Cybersecurity Terminology,” *National Initiative for Cybersecurity Careers and Studies*, 2018. [Online]. Available: https://niccs.us-cert.gov/about-niccs/glossary#C. [Accessed: 22-Apr-2019].

[3] K. Bissell, R. LaSalle, P. Dal Cin, and Ponemon Institute LLC, “Ninth Annual Cost of Cybercrime Study: Unlocking the Value of Improved Cybersecurity Protection,” 2019.

[4] J. Mason, “14 Most Alarming Cyber Security Statistics in 2019,” *TheBestVPN.com*, 2019. [Online]. Available: https://thebestvpn.com/cyber-security-statistics-2019/. [Accessed: 22-Apr-2019].

[5] M. Brenan, “Cybercrimes Remain Most Worrisome to Americans,” *Gallup, Inc.*, 2018. [Online]. Available: https://news.gallup.com/poll/244676/cybercrimes-remain-worrisome-americans.aspx. [Accessed: 22-Apr-2019].

[6] J. Reed, Y. Zhong, L. Terwoerds, and J. Brocaglia, “The 2017 Global Information Security Workforce Study: Women in Cybersecurity,” Santa Clara, 2017.

[7] International Information System Security Certification Consortium, “Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens,” 2018.

[8] C. Díaz-García, A. González-Moreno, and F. Jose Sáez-Martínez, “Gender diversity within R&D teams: Its impact on radicalness of innovation,” *Innovation*, vol. 15, no. 2, pp. 149–160, Jun. 2013.

[9] V. Hunt, D. Layton, and S. Prince J A N U A, “Why diversity matters,” 2015.

[10] J. Steinke *et al.*, “Improving Cybersecurity Incident Response Team Effectiveness Using Teams-Based Research,” *IEEE Secur. Priv.*, vol. 13, no. 4, pp. 20–29, Jul. 2015.

[11] M. Granåsen and D. Andersson, “Measuring team effectiveness in cyber-defense exercises: a cross-disciplinary case study,” *Cogn. Technol. Work*, vol. 18, no. 1, pp. 121–143, Feb. 2016.

[12] E. Salas, D. E. Sims, and C. S. Burke, “Is there a ‘Big Five’ in Teamwork?,” *Small Gr. Res.*, vol. 36, no. 5, pp. 555–599, Oct. 2005.

[13] N. J. Cooke, E. Salas, P. A. Kiekel, and B. Bell, “Advances in Measuring Team Cognition,” in *Team cognition: Understanding the factors that drive process and performance*, P. Eduardo Salas and P. Stephen M. Fiore, Eds. American Psychological Association, 2004, pp. 83–106.

[14] (ISC)^2, “The (ISC)^2 Cybersecurity Lexicon: An introduction to basic terminology and concepts.” (ISC)^2, 2018.

[15] Department of Homeland Security, “National Cybersecurity Awareness Month,” *Department of Homeland Security*, 2018. [Online]. Available: https://www.dhs.gov/national-cyber-security-awareness-month. [Accessed: 22-Apr-2019].

[16] M. A. Goodale and D. A. Westwood, "An evolving view of duplex vision: separate but interacting cortical pathways for perception and action," *Curr. Opin. Neurobiol.*, vol. 14, no. 2, pp. 203–211, Apr. 2004.

[17] K. Amunts *et al.*, "Gender-Specific Left-Right Asymmetries in Human Visual Cortex," *J. Neurosci.*, vol. 27, no. 6, pp. 1356–1364, Feb. 2007.

[18] L. Sax, *Girls on the Edge*. New York, New York, USA: Basic Books, 2010.

[19] M. J. Cobb, "Plugging the skills gap: the vital role that women should play in cyber-security," *Comput. Fraud Secur.*, vol. 2018, no. 1, pp. 5–8, Jan. 2018.

[20] A. Master, S. Cheryan, A. Moscatelli, and A. N. Meltzoff, "Programming experience promotes higher STEM motivation among first-grade girls," *J. Exp. Child Psychol.*, vol. 160, pp. 92–106, Aug. 2017.

[21] R. D. Austin and G. P. Pisano, "Neurodiversity as a Competitive Advantage," *Harv. Bus. Rev.*, vol. 95, no. 3, pp. 96–103, 2017.

[22] S. G. Rogelberg and S. M. Rumery, "Gender Diversity, Team Decision Quality, Time on Task, and Interpersonal Cohesion," *Small Gr. Res.*, vol. 27, no. 1, pp. 79–90, Feb. 1996.

[23] L. Barker, C. Mancha, and C. Ashcraft, "WHAT IMPACT DOES GENDER DIVERSITY HAVE ON BOTTOM-LINE PERFORMANCE?," 2014.

[24] B. Siwicki, "Why diverse cybersecurity teams are better at understanding threats, patient needs | Healthcare IT News," *Women in Health IT*, 2017. .

[25] M. Hasib, *Cybersecurity leadership : powering the modern organization*. Tomorrow's Strategy Today, LLC, 2014.

[26] M. Anwar, W. He, I. Ash, X. Yuan, L. Li, and L. Xu, “Gender difference and employees' cybersecurity behaviors,” *Comput. Human Behav.*, vol. 69, pp. 437–443, 2017.

[27] D. Rock and H. Grant, “Why Diverse Teams are Smarter,” *Harvard Business Review2*, 2016. .

[28] C. R. Fernandes and J. T. Polzer, “Diversity in Groups,” in *Emerging Trends in the Social and Behavioral Sciences*, Hoboken, NJ, USA: John Wiley & Sons, Inc., 2015, pp. 1–14.

[29] C. A. Bowers, J. A. Pharmer, and E. Salas, “When Member Homogeneity is Needed in Work Teams,” *Small Gr. Res.*, vol. 31, no. 3, pp. 305–327, Jun. 2000.

[30] S. Deterding, D. Dixon, R. Khaled, and L. Nacke, “From Game Design Elements to Gamefulness: Defining ‘Gamification,’” *MindTrek '11 Proc. 15th Int. Acad. MindTrek Conf. Envisioning Futur. Media Environ.*, pp. 9–15, 2011.

[31] T. Chothia, C. Novakovic, A.-I. Radu, and R. J. Thomas, “Choose Your Pwn Adventure: Adding Competition and Storytelling to an Introductory Cybersecurity Course,” in *Transactions on Edutainment XV*, Z. Pan, A. D. Cheok, W. Müller, M. Zhang, A. El Rhalibi, and K. Kifayat, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2019, pp. 141–172.

[32] T. Chothia, S. Holdcroft, A.-I. Radu, and R. J. Thomas, “Jail, Hero or Drug Lord? Turning a Cyber Security Course Into an 11 Week Choose Your Own Adventure Story,” *USENIX Work. Adv. Secur. Educ. (ASE 2017)*, 2017.

[33] M. Chapple, J. M. Stewart, and D. Gibson, *(ISC)2 Certified Information Systems Security Professional Official Study Guide*, 8th ed. Indianapolis, Indiana: SYBEX, A Wiley Brand, 2018.

[34] N. Vegt, V. Visch, H. de Ridder, and A. Vermeeren, “Designing Gamification to Guide Competitive and Cooperative Behavior in Teamwork,” in *Gamification in Education and Business*, Cham: Springer International Publishing, 2015, pp. 513–533.

[35] C. J. Cornel, D. C. Rowe, and C. M. Cornel, “Starships and Cybersecurity Teaching Security Concepts through Immersive Gaming Experiences,” 2017.

[36] E. Cho, S. A. Myers, and J. Leskovec, “Friendship and mobility: user movement in location-based social networks,” in *Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining - KDD ’11*, 2011, p. 1082.

[37] Y.-W. Chang, “Influence of the principle of least effort across disciplines,” *Scientometrics*, vol. 106, no. 3, pp. 1117–1133, Mar. 2016.

[38] R. M. Clarkson, C. M. Clarke-Hill, and T. Robinson, “UK supermarket location assessment,” *Int. J. Retail Distrib. Manag.*, vol. 24, no. 6, pp. 22–33, Jul. 1996.

[39] J. Martin and James, *Rapid application development*. Macmillan Pub. Co., 1991.

[40] Lucidchart Content Team, “4 Phases of Rapid Application Development Methodology | Lucidchart Blog,” 2018. [Online]. Available: https://www.lucidchart.com/blog/rapid-application-development-methodology. [Accessed: 06-Jun-2019].

[41] A. Powell-Morse, “Rapid Application Development (RAD): What Is It And How Do You Use It?,” 2016. [Online]. Available: https://airbrake.io/blog/sdlc/rapid-application-development. [Accessed: 06-Jun-2019].

APPENDIX A. INITIAL SURVEY

Initial Survey

Start of Block: Survey Info & Consent

Q16 My name is Cara Cornel, I am a graduate student at Brigham Young University and this research is being conducted under the supervision of Professor Dale Rowe, from the Department of Information Technology. You are being invited to participate in this research study, "A Formal Methodology to Measure the Impact of Diversity on Cybersecurity Team Effectiveness." I am interested in finding out about developing a framework to measure the impact of gender diversity on the effectiveness of technical cybersecurity teams.
Your participation in this study will require the completion of the attached survey. This survey should take approximately **5** minutes of your time. Your participation will be anonymous and you will not be contacted again in the future unless you provide contact information (as indicated in one of the questions of the survey). There is no payment involved for the participant in this study. With this in mind, your participation is completely voluntary. This survey involves minimal risk to you. The benefits, however may impact society by helping increase knowledge about cybersecurity teams.
Please keep in mind your participation in this study is optional and that you do not have to answer any question that you do not want to answer for any reason. We will be happy to answer any questions you have about this study. If you have further questions about this project or if you have a research-related problem you may contact me, Cara Cornel, at cara.cornel@byu.edu or my advisor, Professor Dale Rowe, at dale_rowe@byu.edu.
If you have any questions about your rights as a research participant you may contact the IRB Administrator at A-285 ASB, Brigham Young University, Provo, UT 84602; irb@byu.edu; (801) 422-1461. The IRB is a group of people who review research studies to protect the rights and welfare of research participants.
The completion of this survey implies your consent to participate. If you choose to participate, please complete the attached survey by July 7th. Thank you!

End of Block: Survey Info & Consent

Start of Block: Name

Over18 Are you over 18?

○ Yes (23)

○ No (24)

Skip To: End of Block If Over18 = 24

Q31 You will be provided both a team number and a team member number to answer these questions.

TeamNo Team Number

____

TeamMemberNo Team Member Number

____

End of Block: Name

Start of Block: Block 3

Display This Question:

If Over18 = 24

Under 18's are welcome to participate in the challenge when accompanied by a responsible adult. However we do not collect any survey data from under 18's. Please enjoy your experience!

Skip To: End of Survey If (1) Is Displayed

End of Block: Block 3

Start of Block: Demographics

X→

Sex Biological Sex

○ Male (1)

○ Female (2)

IdentifyasSex Do you identify as this gender?

□ Yes (23)

□ No (24)

Display This Question:

If IdentifyasSex = 24

GenderID Identified Gender

○ Male (1)

○ Female (2)

○ Other (3) ____

AgeRange Age

○ 18-24 (2)

○ 25-34 (3)

○ 35-44 (4)

○ 45-54 (5)

○ 55-64 (6)

○ 65+ (7)

Ethnicity How would you describe yourself? Select all that apply.

□ Hispanic or Latino (1)

□ American Indian or Alaska Native (2)

□ Asian (3)

□ Black or African American (4)

□ Native Hawaiian or Other Pacific Islander (5)

□ White (6)

□ Other (7) ____

CyberJobPast Have you ever held a job position where cybersecurity is your primary or secondary responsibility?

○ Yes (1)

○ No (2)

CurrentJobTitle What is your current or most recent job title?

____

____

____

____

____

CyberPro Do you consider yourself a cybersecurity professional?

○ Yes (40)

○ Unsure (41)

○ No (42)

CyberKnowledge Please indicate how knowledgeable you feel for each of the following four cybersecurity areas:

	Extremely knowledgeable (16)	Very knowledgeable (17)	Moderately knowledgeable (18)	Slightly knowledgeable (19)	Not knowledgeable at all (20)
Penetration Testing / Pen Testing / Ethical Hacking (1)	○	○	○	○	○
Incident Response (2)	○	○	○	○	○
Cybersecurity Management (3)	○	○	○	○	○
Security Analytics (4)	○	○	○	○	○

CyberCerts Do you hold any cybersecurity qualifications/certifications. Please select all that apply.

□ CompTIA Security+ (1)

□ Certified Information Privacy Professional (CIPP) (2)

□ Global Information Assurance Certification (GIAC) (3)

□ Certified Information Systems Security Professional (CISSP) (4)

□ Certified Information Systems Auditor (CISA) (5)

□ Certified Information Security Manager (CISM) (6)

□ Master's Degree (computing related field) (7)

□ Bachelor's Degree (computing related field) (8)

□ PhD (computing related field) (9)

□ Other certifications (please specify): (10)

____

KnowTeam Did you know any of your teammates participating in this simulation before this simulation?

○ Yes (1)

○ No (4)

Display This Question:

If KnowTeam = 1

KnowTeamDetails Please answer this question based on your relationship with your teammate(s).

	How many years have you known this teammate?	Context		For professional, do you work on the same team?	
	Amount of years: (1)	Professional (1)	Personal (2)	Yes (1)	No (2)
Team member 1 (1)		○	○	○	○
Team member 2 (2)		○	○	○	○
Team member 3 (3)		○	○	○	○
Team member 4 (4)		○	○	○	○

EmailProvided Would you be willing to provide your email for potential further follow up regarding this simulation? This is optional, by providing your email you agree that we may contact you regarding further information about your experience.

○ Yes (1)

○ No (2)

Display This Question:

If EmailProvided = 1

EmailAddress Email

____

End of Block: Demographics

APPENDIX B. POST SURVEY

Post Survey

Start of Block: Thesis Introduction

Q1 My name is Cara Cornel, I am a **graduate** student at Brigham Young University and this research is being conducted under the supervision of **Professor Dale Rowe**, **from the Department of Information Technology**. You are being invited to participate in this research study, "**A Formal Methodology to Measure the Impact of Diversity on Cybersecurity Team Effectiveness**." I am interested in finding out about **developing a framework to measure the impact of gender diversity on the effectiveness of technical cybersecurity teams**.

Your participation in this study will require the completion of the attached **survey**. This survey should take approximately **5 minutes** of your time. Your participation will be anonymous and you will not be contacted again in the future unless you provide contact information (as indicated in one of the questions of the survey). There is no payment involved for the participant in this study. With this in mind, your participation is completely voluntary. This survey involves minimal risk to you. The benefits, however may impact society by helping increase knowledge about **cybersecurity teams**.

Please keep in mind your participation in this study is optional and that you do not have to answer any question that you do not want to answer for any reason. We will be happy to answer any questions you have about this study. If you have further questions about this project or if you have a research-related problem you may contact me, **Cara Cornel**, at **cara.cornel@byu.edu** or my advisor, **Professor Dale Rowe**, at **dale_rowe@byu.edu**.

If you have any questions about your rights as a research participant you may contact the IRB Administrator at A-285 ASB, Brigham Young University, Provo, UT 84602; irb@byu.edu; (801) 422-1461. The IRB is a group of people who review research studies to protect the rights and welfare of research participants.

The completion of this survey implies your consent to participate. If you choose to participate, please complete the attached survey by **July 7th**. Thank you!

End of Block: Thesis Introduction

Start of Block: Block 1

Q5 Team Number

____

Q16 Team Member Number

____

End of Block: Block 1

Start of Block: Block 2

Q23 Did you enjoy working with your team composition?

○ Yes (37)

○ No (38)

Display This Question:

If Q23 = 38

Q24 Please give a few words or more explaining why you did not enjoy working with your team composition.

____

____

____

____

____

Display This Question:

If Q23 = 37

Q25 Please give a few words or more explaining why you enjoyed working with your team composition.

____

____

____

____

____

Q26 Did you find the overall simulation enjoyable?

○ Yes (5)

○ No (6)

Q34 Which route did your team choose?

○ Incident Response (Investigation Route) (1)

○ Penetration Testing / Pen Testing / Ethical Hacking (Breaking in route) (2)

X→

Q17 Which challenges did you work on? Please select all that apply.

□ Challenge 1 (1)

□ Challenge 2 (2)

□ Challenge 3 (3)

□ Challenge 4 (4)

Display This Question:

If Q17 = 1

Q15
For Challenge 1, please answer the following:

	Strongly agree (11)	Somewhat agree (12)	Neither agree nor disagree (13)	Somewhat disagree (14)	Strongly disagree (15)
The challenge was too difficult (1)	○	○	○	○	○
I helped solve this challenge (2)	○	○	○	○	○
My teammates helped solve this challenge (3)	○	○	○	○	○
This was a good team-based activity (4)	○	○	○	○	○
I enjoyed this challenge (5)	○	○	○	○	○
I learned something new (6)	○	○	○	○	○

Page Break

Display This Question:

If Q17 = 2

Q21
For Challenge 2, please answer the following:

	Strongly agree (11)	Somewhat agree (12)	Neither agree nor disagree (13)	Somewhat disagree (14)	Strongly disagree (15)
The challenge was too difficult (1)	○	○	○	○	○
I helped solve this challenge (2)	○	○	○	○	○
My teammates helped solve this challenge (3)	○	○	○	○	○
This was a good team-based activity (4)	○	○	○	○	○
I enjoyed this challenge (5)	○	○	○	○	○
I learned something new (6)	○	○	○	○	○

Page Break

Display This Question:

If Q17 = 3

Q22
For Challenge 3, please answer the following:

	Strongly agree (11)	Somewhat agree (12)	Neither agree nor disagree (13)	Somewhat disagree (14)	Strongly disagree (15)
The challenge was too difficult (1)	○	○	○	○	○
I helped solve this challenge (2)	○	○	○	○	○
My teammates helped solve this challenge (3)	○	○	○	○	○
This was a good team-based activity (4)	○	○	○	○	○
I enjoyed this challenge (5)	○	○	○	○	○
I learned something new (6)	○	○	○	○	○

Page Break

Display This Question:

If Q17 = 4

Q33 For Challenge 4, please answer the following:

	Strongly agree (11)	Somewhat agree (12)	Neither agree nor disagree (13)	Somewhat disagree (14)	Strongly disagree (15)
The challenge was too difficult (1)	○	○	○	○	○
I helped solve this challenge (2)	○	○	○	○	○
My teammates helped solve this challenge (3)	○	○	○	○	○
This was a good team-based activity (4)	○	○	○	○	○
I enjoyed this challenge (5)	○	○	○	○	○
I learned something new (6)	○	○	○	○	○

Page Break

Q9 What method(s) did you use to solve the challenge(s)?

____

____

____

____

____

Q10 What other method(s) did you think of to solve the challenge(s), but did not use?

____

____

____

____

____

Q6 Any further comments you would like to include?

____

____

____

____

____

Page Break

Q13 Would you be willing to provide your email for potential follow up regarding this simulation? This is optional, by providing your email you agree that we may contact you regarding further information about your experience.

○ Yes (1)

○ No (2)

Display This Question:

If Q13 = 1

Q14 Email

____

End of Block: Block 2

APPENDIX C. OBSERVATION LOG

Observation Log

Team # _____________

Date: _______________

Log File Name: __________________________________

Start time for Observation (Matrix Time): _______________

Route Chosen: Pen or IR

Did they talk as a team to decide which route should be chosen? Y N

How many people are in this team? 1 2 3 4

	Please Circle	
Member#1	M	F
Member#2	M	F
Member#3	M	F
Member#4	M	F

Reminder:

When writing notes, please take care to **refer to each person as their member#**.

Please record the **matrix time** for **each answer/note** taken.

CHALLENGE#1 Observation Notes (Please record the matrix time for each answer):

In the first 5 minutes of challenge 1, did all members of the team talk to each other? Y N

Did the team communicate with each other? Who and How?

How many hints were needed for this challenge?

Who solved this challenge (circle all member numbers this applies to):1 2 3 4

How? Did they work together or individually?

Any further observations?

CHALLENGE#2 Observation Notes (Please record the matrix time for each answer):

In the first 5 minutes of challenge 2, did all members of the team talk to each other? Y N

Did the team communicate with each other? Who and How?

How many hints were needed for this challenge?

Who solved this challenge (circle all member numbers this applies to):1 2 3 4

How? Did they work together or individually?

Any further observations?

CHALLENGE#3 Observation Notes (Please record the matrix time for each answer):

In the first 5 minutes of challenge 3, did all members of the team talk to each other? Y N

Did the team communicate with each other? Who and How?

How many hints were needed for this challenge?

Who solved this challenge (circle all member numbers this applies to):1 2 3 4

How? Did they work together or individually?

Any further observations?

CHALLENGE#4 Observation Notes (Please record the matrix time for each answer):

In the first 5 minutes of challenge 4, did all members of the team talk to each other? Y N

Did the team communicate with each other? Who and How?

How many hints were needed for this challenge?

Who solved this challenge (circle all member numbers this applies to):1 2 3 4

How? Did they work together or individually?

Any further observations?

Did they complete all four challenges? Y N

Did the team establish a leader among themselves? Y N

Did the they establish a common goal? Y N

Were there any roles assigned? Y N

Did the team ask each other follow up questions relating to their task(s)? Y N

Did the team hold each other accountable? Y N

Did they collaborate? Y N

Did the team share information with each other? Y N

Finish time for Observation (Matrix Time): _______________

Any further observations?