Veterans and their Inherent Cybersecurity Preparedness: Myth or Reality?

Marc Dupuis
Computing and Software Systems
University of Washington
Bothell, Washington, USA
marcjd@uw.edu

Maximilian Weiss
Computing and Software Systems
University of Washington
Bothell, Washington, USA
mjweiss@uw.edu

***Abstract*—Increasingly, the cybersecurity job market is lacking in qualified talent. Although lack of available workers with the proper skills is part of it, it is primarily due to the increasing breadth of the cyber domain. To combat this, many companies and government agencies are looking to train combat veterans in the necessary skills to be effective and capable in the domain of cybersecurity. Combat veterans, who have experience with risk and adapting to difficult situations and unknown threats, are believed to be better suited than the civilian population to deal with the threat landscape of cybersecurity. The purpose of the research is to examine this preconceived notion through four overarching research questions: 1. Do combat veterans make better cybersecurity professionals? 2. How much does their experience with risk and threat assessment come into play? 3. Do veterans make better cybersecurity professionals for other reasons? 4. Or is the notion that vets make better cybersecurity professions flawed because the required skills are so technical in nature? As a precursor to a comprehensive study, a large-scale survey was conducted to see what differences, if any, there are between individuals with combat experience and those that do not have such experience. These results are discussed. Future research will employ a mixed methods design consisting of a general survey (phase I) followed by interviews with Chief Information Security Officers (CISOs) (phase II), and finally interviews with Veterans and non-Veterans (phase III). The phased approach will allow us to make the most efficient use of our time by using the information learned in one phase to help inform subsequent phases. This will result in a richer set of data and more meaningful results.**

***Index Terms*—cybersecurity, professionals, military, veterans, risk, skills, mixed method, survey, interviews, combat experience, privacy**

I. Introduction

Increasingly, the cybersecurity job market is lacking in qualified talent [13]. Although a lack of available workers with the proper skills is part of it, it is primarily due to the increasing breadth of the cyber domain. To combat this, many companies and government agencies are looking to train combat veterans in the necessary skills to be effective and capable in the domain of cybersecurity [6]. Or, educational programs are being developed with veterans in mind [18], [21]. Combat veterans, who have experience with risk and adapting to difficult situations and unknown threats, are believed to be better suited than the civilian population to deal with the threat landscape of cybersecurity [7]. The purpose of this research is to examine this preconceived notion through four overarching research questions: 1. Do combat veterans make better cybersecurity professionals? 2. How much does their experience with risk and threat assessment come into play? 3. Do veterans make better cybersecurity professionals for other reasons? 4. Or is the notion that vets make better cybersecurity professions flawed because the required skills are so technical in nature?

There are several studies linking the exposure to combat with a higher propensity for risk-taking behavior and self-destructive behavior [11], [12], [19]. Additionally, studies which have examined the link between attitude and security [1], [2], [9], [16], have found a direct correlation between personality traits, perceptions of risk, the environment, and cybersecurity behavior.

Where the research is lacking is in bridging the gap and linking the psychological changes veterans undergo in service with their attitudes and behavior in the arena of cybersecurity. What differences in attitudes towards cybersecurity do veterans have? How does their perception of risk for cybersecurity activities differ from non-veterans, and what are the security and behavior implications of this? Information about such a link (or lack thereof) between veterans and changes in cybersecurity behavior will give better insight into the relationship between veterans, risk behavior at a broad general health level, and what ramifications there are for combat and stress in the cybersecurity sector.

In the next part of our research, we will employ a mixed methods design consisting of a general survey (Phase I) followed by interviews with Chief Information Security Officers (CISOs) (Phase II), and finally interviews with veterans and non-veterans (Phase III) [20]. The phased approach will allow us to use the information learned in one phase to help inform subsequent phases. This will result in a richer set of data and more meaningful results. The preliminary results obtained and discussed in the current paper, will help inform the launch of this phased approach.

Since human participants will be involved, IRB approval will be sought and obtained prior to conducting any research with human participants. Special consideration will be given to the primary population being explored, veterans. We are sensitive to having veterans in a research study and will ensure all appropriate measures are taken to minimize any possible distress.

II. Objectives

In studying veterans, we wish to find what cybersecurity traits, risks, and behaviors they exhibit which differ from the general population and what implications this may have for veterans and cybersecurity. The information gleaned from this research may lead to better psychological evaluation and treatment for veterans and their health, as well as provide valuable insight into how those who have dealt with risk approach cybersecurity in their daily lives. This in turn will help security and IT professionals by providing deeper insight into a specific user subset. By comparing and contrasting the nature of veterans skills with cybersecurity, we open the door to new assessments of the psychology of veterans, the relationship between generalized risk assessment and analogous threat modeling in other domains, as well as the relationship between risk propensity and effectiveness in jobs dealing with risk assessment.

Such research may also lead to tailored applications and approaches for protecting and defending IT infrastructure in high risk and stress-related environments—not merely combat zones, but in law enforcement workspaces, hospitals, and other high-stress areas which are known to produce many of the same mental health and behavioral outcomes which afflict combat veterans. Indeed, being able to map the causal effects of stress and trauma from the psychological starting point, to risk and health behavior, over to cybersecurity behavior and attitudes, has the potential to dramatically increase the effectiveness of security solutions. Such a map would provide the means to make cybersecurity inferences based solely on health and behavior research, which would allow for more directed and productive research in the future.

For example, Hartley et al (2013) found that women and men develop PTSD based on different factors—women are more prone to developing it by repeated traumatic exposure, whereas men are more likely to develop it due to the intensity of specific traumatic events [8]. However, it is not known how this information could be used to generate a hypothesis about cybersecurity behavior. By providing an evidence-based link from veterans to cybersecurity, all future research into both arenas may benefit, and a variety of new research opportunities may present themselves.

As a result of the survey and behavioral study, we will be able to gain specific discrete data about the correlative links between veterans, cybersecurity awareness, and actual cybersecurity behavior. This data will help define what other areas of research are needed. Future research that is enabled by the data provided by this study may have extremely useful repercussions. As an example, this data may help to reduce instances of breach and misuse of computer systems deployed in combat and high-stress environments, such as hospitals, where security issues can have life-and-death consequences.

Moving to the psychological and behavioral side, the research may help to guide the creation of applications and systems that are more intuitive and user-friendly for veterans and those with PTSD. It may also shed light on issues within organizations, such as the insider threat [4]. In short, this research will form a framework for a wide breadth of future research by providing specific links between the many facets which are intertwined with stress, health, risk behavior tendencies, security awareness, and security behavior. This may have implications in health and psychology in addition to cybersecurity, as certain security behaviors may be correlated with health and risk behaviors and beliefs, which may lead to more informed diagnoses and treatment of mental health issues.

III. Methods

In order to obtain some initial data examining differences between combat-veterans and others, a large-scale survey was employed. Amazon's Mechanical Turk (MTurk) was used to recruit survey participants. MTurk provides researchers with a relatively low-cost and quick turnaround platform for participant recruitment [3], [17]. Participants generally represent a broader cross-section of the population than other methods often employed, such as college sophomores in an introductory psychology class [15]. IRB approval was on file prior to collecting data and informed consent obtained. Participants were compensated with $2 for their participation in the study. Two quality control questions were used. If participants failed either quality control question, the survey would conclude with an explanation of why it has concluded.

We used the Qualtrics survey platform. A total of 1,002 responses were collected. Participants were asked at the end of the survey how the effort and time required to complete the survey compared to similar work offered through the MTurk platform. Most participants indicated that it was either easier (21.5%) or comparable (69.1%) to other projects with a small number indicating more effort was required (9.4%). Of note, a pilot study consisting of 50 participants was employed beforehand to check for any issues with the survey, including survey logic and question wording problems, as well as the same question noted above. The compensation was subsequently adjusted from the pilot study ($1.50) to better reflect a comparable amount of time and effort for research participants. Thus, we believe we accomplished this given the above results from this question in the final survey.

The primary purpose of this initial survey was to see if there were any differences with respect to risk behavior in general, and cybersecurity behavior in particular. For the former, we asked participants a series of six questions related to risk decisions. They included the following:

1) Do you get flu shots?
2) Do you require a call-back from your bank to verbally confirm any money transfers?
3) Do you use LifeLock or another identity theft monitoring service?

4) Do you have pre-prepared earthquake or natural disaster emergency kits/food storage?
5) Do you have AAA or another emergency roadside assistance provider?
6) Do you have a home security system such as Nest, Ring, ADT, or others?

The goal was to assess the extent to which survey participants took measures to mitigate various types of risk. We also asked survey participants whether they used the following measures related to cybersecurity: password manager, virtual private network (VPN), backup data, anti-malware software, and two-factor authentication.

Finally, we also asked participants about their past experiences related to cybersecurity threats. These nine questions assessed whether they believe they have ever had the following activities occur to them:

To the best of your knowledge, have you ever...

1) received a notice that your social security number had been compromised?
2) received a notice that other sensitive personal information, such as your account number, had been compromised?
3) noticed fraudulent charges on your debit or credit card?
4) had someone take over your email account without your permission?
5) had someone take over your social media account without your permission?
6) had someone attempt to open a line of credit or apply for a loan using your name?
7) had someone attempt to receive a tax refund using your name?
8) had personal belongings stolen?
9) lost money or data from a phishing attack?

These questions were asked along with demographic questions and other cybersecurity questions that are not a part of the current study.

IV. Results

Out of 1,002 survey responses, only 15 identified themselves as having had combat experience in the past 20 years. Thus, the sample is quite limited with respect to the primary population of interest. This will be addressed in the comprehensive study to ensure a large enough sample size of veterans with combat experience is obtained.

Nonetheless, we did find some interesting initial results. For the first series of questions related to a general willingness to try and mitigate various types of risk, participants with combat experience were more likely to have enacted various protective measures ($p < 0.01$).

Additionally, out of the five cybersecurity protective measures we asked participants about, there was a statistically significant difference for only one of them (VPN usage). Participants with combat experience were more likely to use a VPN than those without such experience ($p < 0.05$). This was true regardless of platform, such as laptop/desktop or smartphone/tablet.

Finally, we also found that participants with combat experience were more likely to have experienced various cybersecurity threats than those without such experiences ($p < 0.01$). It is possible that these experiences may be related to something entirely different than combat experience, such as having to move greater distances on a more regular basis than the average civilian. This may create greater opportunities for various cybersecurity threats to be realized. This is something that will also be explored in greater depth in the comprehensive study.

V. Looking Ahead

Future research will employ a mixed methods design [20]. The purpose is to have one method inform one or more subsequent methods employed in a research design.

Research on health-risk behaviors and attitudes towards risk have traditionally been survey-driven with predefined characteristics used as risk assessment measures. Thomsen et al. (2011), whose research focused on the effect of combat on risky and self-destructive behavior, gathered demographic information, deployment history, and certain behavior actions; they had predefined eight actions as risky behavior [19]. This allowed the researchers to directly correlate combat deployment with risk behavior.

Ion, Reeder, and Consolvo (2015) focused their research on the security beliefs of experts versus non-experts in cybersecurity and conducted their research by asking a series of open-ended questions about computer-associated risk beliefs, followed by several narrow questions about specific cybersecurity-related behavior [10]. This allowed them to link knowledge and attitudes with likelihood of engaging in specific cybersecurity-related behaviors.

Our research methodology will use both approaches in order to get a broad measure of risk belief and risk behavior in general health terms as well as gather significant new data narrowed to the realm of cybersecurity specifically. This will allow us to not just gather new data in cybersecurity, but to make the relevant connections between risk belief and behavior more broadly and its relationship with cybersecurity beliefs and behaviors. We expect to be able to use this data to find links that may be useful in further research relating health and risk behaviors and beliefs with cybersecurity behaviors and beliefs.

A. Phase I: Survey

First, a survey will be employed that explores what differences, if any, may exist between veterans and non-veterans. Several factors will be explored during this stage, including psychological factors (e.g., personality, trait affect); information on perceptions and behavior related to risk (both cybersecurity and non-cybersecurity); cybersecurity knowledge, attitudes, and behavior; and demographics (including occupation). Prior efforts involving comprehensive data collection have been fruitful in the context of understanding social networking behavior [5]. While this research is focused on veterans, the occupation question will also allow us to capture

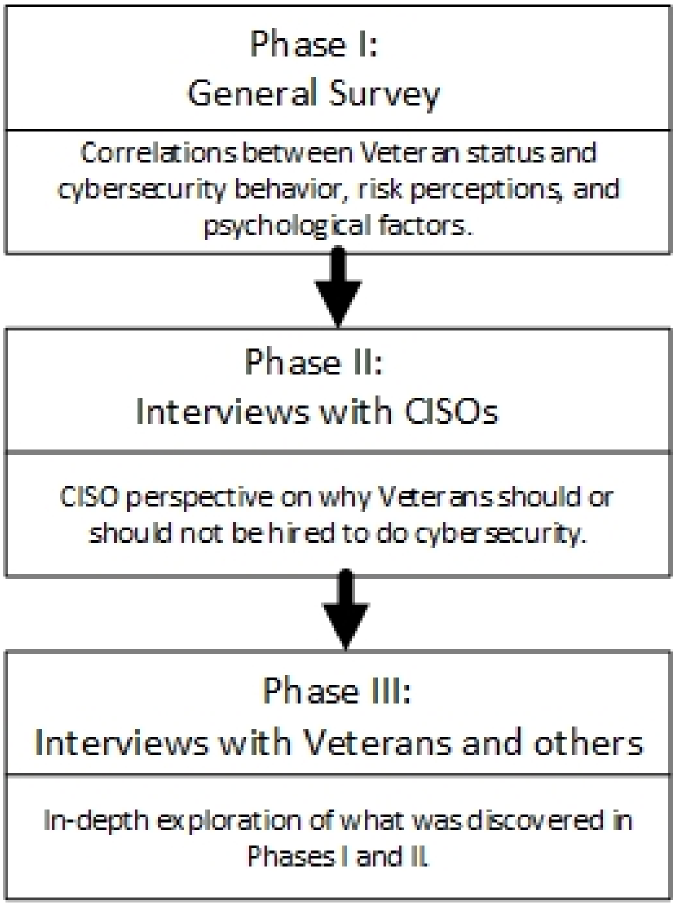
Phase I:
General Survey
Correlations between Veteran status and cybersecurity behavior, risk perceptions, and psychological factors.
Phase II:
Interviews with CISOs
CISO perspective on why Veterans should or should not be hired to do cybersecurity.
Phase III:
Interviews with Veterans and others
In-depth exploration of what was discovered in Phases I and II.

Fig. 1. Mixed-Method Phased Research Design

information on other possible occupations that may have similar perceptions and behavior from a risk standpoint. This includes such occupations as police officers and firefighters, among others.

This exploratory survey will be developed using Qualtrics and administered using Amazons Mechanical Turk (MTurk). MTurk provides a good value proposition with a quick turnaround time, high quality, high anonymity between the participants and the PI, and low cost [3], [17]. Approximately 1,000 responses will be collected for this survey with the goal of obtaining at least 500 veterans and 500 non-veterans. Qualifying questions will be used to develop a large enough pool of veterans with combat experience given the results obtained in the preliminary data discussed earlier.

Data analysis will be conducted using SPSS and SmartPLS. SPSS will be employed for initial data analysis and examine possible correlations and other relationships between variables. Depending on the results found, some initial exploratory data modeling will take place using structural equation modeling via Smart PLS, version 3.0 [14]. The goal of the survey is to collect a large data set so that any relationships present may be explored in much greater depth through interviews.

B. Phase II: Interviews with CISOs

During phase II, interviews will be conducted with Chief Information Security Officers (CISOs) to better understand what they look for when hiring individuals into cybersecurity positions. CISOs from across the country will be chosen by using the professional networks available to the team. Based in large part on the results from the survey, as well as other research and anecdotal information, the goal will be to understand the decision making process of the CISO, including how this may differ when hiring a veteran. This will help us move one step closer to better understanding the role veterans play in this profession, including possible answers to the question of why a veteran?. Ten CISOs in total will be interviewed for this phase. Participants will be compensated with a $20 Amazon gift card.

The interviews will be recorded and subsequently sent to a transcription service. The transcripts will be analyzed and coded using ATLAS.ti. Concepts and themes will be identified that helps us better understand the role of veterans in the cybersecurity space. These results and those obtained from the survey will help inform the interview schedule for phase III.

C. Phase III: Interviews with Veterans and Non-Veterans

Based on the research conducted thus far, including information gleaned from the general survey as well as the interviews with CISOs, an interview schedule will be developed. While this phase could have occurred first, it would likely have resulted in a missed opportunity to ask more salient questions based on what had been learned from phases I and II. Thus, this final phase will allow us to focus our attention solely on the real and perceived differences between veterans and non-veterans. While the focus is on veterans, we are including a control group of non-veterans to help ensure the differences are based on the data gathered and not just the views of veterans.

A representative sample of veterans to interview will be identified. Likewise, non-veterans will be identified and interviewed as well. Twenty veterans and 20 non-veterans will be interviewed in total. As noted in phase II, the interviews will be recorded and subsequently transcribed. Data analysis will occur using ATLAS.ti. Participants will be compensated with a $20 Amazon gift card.

VI. Conclusion

This paper identified a need to research a preconceived notion involving veterans, especially those with combat experience. The underlying premise is that those with such experience may be better able to identify risk and handle risk-involved situations, including cybersecurity types of risk. Thus, they may be better suited to helping fill the cybersecurity workforce shortage than others. However, we do not know to what extent this premise is true. Or perhaps if they are found to be more suited, there may be other reasons for this.

Some preliminary data was discussed. We then laid out a plan for a more comprehensive study. Understanding the answers to the questions raised in this paper may help us better understand the role of veterans in the cybersecurity workforce, as well as begin to identify the specific traits needed to be successful in the cybersecurity domain.

References

[1] Marc Dupuis and Robert Crossler. The compromise of ones personal information: Trait affect as an antecedent in explaining the behavior of individuals. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*. IEEE, 2019.

[2] Marc Dupuis, Robert Crossler, and Barbara Endicott-Popovsky. The information security behavior of home users: Exploring a users risk tolerance and past experiences in the context of backing up information. In *The Dewald Roode Information Security Workshop*, 2012.

[3] Marc Dupuis, Barbara Endicott-Popovsky, and Robert Crossler. An analysis of the use of amazons mechanical turk for survey research in the cloud. In *Proceedings of the International Conference on Cloud Security Management*, Oct 2013.

[4] Marc Dupuis and Samreen Khadeer. Curiosity killed the organization: A psychological comparison between malicious and non-malicious insiders and the insider threat. In *Proceedings of the 5th Annual Conference on Research in Information Technology*, page 3540. ACM Press, 2016.

[5] Marc Dupuis, Samreen Khadeer, and Joyce Huang. i got the job!: An exploratory study examining the psychological factors related to status updates on facebook. *Computers in Human Behavior*, 73:132140, 2017.

[6] Brian R. Gattoni. *From FOB to NOCa pathway to a cyber career for combat veterans*. PhD thesis, Naval Postgraduate School, Jun 2014.

[7] Nigel Guenole, Jeff Labrador, Trevor Pons, and Sheri Feinzig. *High-Stakes Hiring: Selecting the Right Cybersecurity Talent to Keep Your Organization Safe*. Number 30018130-USEN-01 in IBM Talent Management Solutions. IBM, Dec 2018.

[8] Tara A. Hartley, Khachatur Sarkisian, John M. Violanti, Michael E. Andrew, and Cecil M. Burchfiel. Ptsd symptoms among police officers: Associations with frequency, recency, and types of traumatic events. *International journal of emergency mental health*, 15(4):241253, 2013.

[9] Adele E. Howe, Indrajit Ray, Mark Roberts, Malgorzata Urbanska, and Zinta Byrne. The psychology of security for the home computer user. In *Proceedings of the 2012 IEEE Symposium on Security and Privacy*, page 209223. IEEE, May 2012.

[10] Iulia Ion, Rob Reeder, and Sunny Consolvo. ...no one can hack my mind: Comparing expert and non-expert security practices. In *Proceedings of the Eleventh Symposium on Usable Privacy and Security*, page 327346. USENIX Association, Jul 2015.

[11] Lisa M. James, Thad Q. Strom, and Jennie Leskela. Risk-taking behaviors and impulsivity among veterans with and without ptsd and mild tbi. *Military Medicine*, 179(4):357363, Apr 2014.

[12] William D. S. Killgore, Amanda Kelley, and Thomas J. Balkin. So you think youre bulletproof: Development and validation of the invincibility belief index (ibi). *Military Medicine*, 175(7):499508, Jul 2010.

[13] Martin C. Libicki, David Senty, and Julia Pollak. *H4cker5 Wanted: An Examination of the Cybersecurity Labor Market*. Number RR-430. RAND Corporation, 2014.

[14] Christian M. Ringle, Sven Wende, and Jan-Michael Becker. Smartpls 3. bnningstedt: Smartpls. *Retrieved from http://www.smartpls.com*, 2015.

[15] David O. Sears. College sophomores in the laboratory: Influences of a narrow data base on social psychologys view of human nature. *Journal of Personality and Social Psychology*, 51(3):515, 1986.

[16] Jordan Shropshire, Merrill Warkentin, and Shwadhin Sharma. Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, 49:177191, Mar 2015.

[17] Zachary R. Steelman, Bryan I. Hammer, and Moez Limayem. Data collection in the digital age: Innovative alternatives to student samples. *MIS Quarterly*, 38(2):355378, 2014.

[18] Tracy Thompson, Marc Dupuis, Bryan Goda, Yan Bai, Charles Costarella, and Morgan Zantua. Systems thinking pedagogical design: Developing a veteran-centric masters degree in cybersecurity and leadership. *Special Edition of The Colloquium for Information Systems Security Education: Educational Approaches To Transition Former Military Personnel into the Cyber Security Field*, Jun 2015.

[19] Cynthia J. Thomsen, Valerie A. Stander, Stephanie K. McWhorter, Mandy M. Rabenhorst, and Joel S. Milner. Effects of combat deployment on risky and self-destructive behavior among active duty military personnel. *Journal of Psychiatric Research*, 45(10):13211331, Oct 2011.

[20] Viswanath Venkatesh, Susan A. Brown, and Yulia W. Sullivan. Guidelines for conducting mixed-methods research: An extension and illustration. *Journal of the Association for Information Systems*, 17(7):435, 2016.

[21] Morgan Zantua, Marc Dupuis, and Barbara Endicott-Popovsky. Re-engineering the cybersecurity human capital crisis. *Special Edition of The Colloquium for Information Systems Security Education: Educational Approaches To Transition Former Military Personnel into the Cyber Security Field*, Jun 2015.