For Your Information Security

Addressing the Need for Cybersecurity Awareness throughout the Military

Amy Owens

Comp116 Final Paper

December 10, 2019

Abstract

Traditional demonstrations of "hard power," or national combat arms branches that are strategically integrated, include joint operations of armed forces, naval fleets, and air power. Within the last decade, the United States military established a force for a new domain of hard power - cyberspace. Compared to previous domains, the cyber domain presents a unique challenge due to the difficulty of preemptively identifying threats and dangerous actors. Additionally, while other domains have limited fighting arenas, cyberspace is vast and has undefined boundaries. Members of the military who are not a part of cyber warfare forces may be undertrained and may disregard cybersecurity as unnecessary. These individuals could be vulnerabilities for their units on the tactical, operational, or strategic level. This paper will explore the need for every individual in the military to have some level of cybersecurity training through an evaluation of current required training and the cyber skill.

Introduction: State of the Military

Since World War 1, the branches of the United States' great military power fought in three domains: land, sea, and air. These domains have been well established, with clear rules of engagement agreed between actors. The U.S. spends 15% of federal funds to strengthen, sustain, and build the Army, Navy, and Air Force. In fact, the U.S. spends more on defense than Russia, China, and Saudi Arabia combined ("U.S. Defense Spending"). In the early 2000s, a new warfare domain emerged: cyberspace. U.S. Army commands had been managing their own network security systems in the late 20th century. Yet, self-management of network systems led to vulnerabilities and incapability that impeded the effectiveness of military cyber power ("Timeline of Army Cyber"). By 2010, the Army, Navy, and Air Force all established a special force for cyber operations, although the Air Force team is provisional ("Officials Detail Scope", Strickland). As the Army is the largest branch among the armed forces, this paper will mainly focus on the Cyber force of the U.S. Army

To the Community: Discrepancies between Physical Security and Cyber Security Understanding

Headlines such as “US opens national security investigation on Tik Tok” and “Using FaceApp to age your photos may be fun, but you could be giving up your privacy” all play on the public fear of losing what they value: privacy (Alley, Snider). However, these articles, posted on mainstream news outlets similar to CNBC and USA Today, usually lack detailed explanations of cyber security vulnerabilities. These headlines exploit the ignorance of the public by creating alarm towards losing privacy and safety. Yet many people do not educate themselves on the basics of cyber security. They skim or ignore the Terms of Service and other necessary precautions for protection. While many people understand the necessity of locking their doors and windows to protect their house, owning a safe for extreme valuables, and other aspects of physical safety, they neglect provisions of information and network security. This ignorance is exemplified in the U.S. Army, as the current required cyber training is sparse and hands-off, while concepts of physical security such as patrol base operations or gun safety are harbored consistently.

Problems with Cybersecurity Training in the Army

Presently, the minimum mandatory cyber security training is an online course taken individually and required annually. This format of training, when forced into it, is non-engaging and can be taken passively. Users can ignore the training videos by muting them and then guessing through the follow-up questions. In fact, one can use a search engine in the background to find answers. It is easy to achieve the certification and often the only supervision is a checkup to ensure personnel achieve the certificate.

This training for fiscal year 2020, “Cyber Awareness Challenge 2020,” is designed to tackle the information awareness requirements outlined in DoD (Department of Defense) 8570.01-M Information Assurance Workforce Improvement Program (“Cyber Awareness Challenge”). In DoD 8570.01-M, it is outlined that every personnel are required to complete the training before accessing a DoD IT (information technology) system. The minimum topics, outlined in chapter 6 of the document, that must be covered are:

- The crucial reliance on information and information systems (IS),
- Required commitment to protect previously mentioned, including personal identifiable information (PII),
- Present threats, vulnerabilities, and risks to operating IS,
- Consequences of inadequate protection, and
- The essential role of DoD employee (Department of Defense, 45).

However, there are several topics that "shall" be addressed yet are not required. This list is extensive and non-exclusive, but they include topics that are necessary to know for entry level civilian jobs in cyber security. Additionally, they are common security mishaps that one must be able to recognize and react to. Some topics that are necessary for foundational understanding of cybersecurity are:

- The relevant laws, policies, and procedures, and how they impact users of DoD IT systems,
- Present external threats such as hackers or actors of foreign countries/terrorist groups,
- Present internal threats such as incompetent/malicious users,
- Understanding malicious code including how they attack and how users can reduce impact, and
- Impact of distributed denial of service attacks and how to mitigate them (Department of Defense 45-47).

While these topics are taught in university level cyber security courses, many of them are not taught in the mandatory training. This training starts with a video on how in the future, every IS system is compromised, and it is up to the trainee to stop this future from becoming a reality. This introduction does not highlight the current reality of cyberattacks, nor does it create a true

sense of urgency. Then, the user is given the choice to test out of certain modules or to review all the material. To save time most would choose the former.

Figure A: Opening options to complete the Cyber Awareness Challenge.

This knowledge check option allows for the user to choose a module, and answer a few, usually three or less, questions about the topic. These questions do not prove greater understanding of these topics and are often simple enough to look up or guess. Again, this makes it easy for personnel to breeze through training without engaging or learning the material, which is necessary if this training is only required once a year.

Additionally, the topics included are not extensive. While the training does cover some of the extended topics, as the expected training time is only about 60 minutes. It is probable that the details covered in these topics are not enough to satisfy a university level education ("Cyber Awareness Challenge").

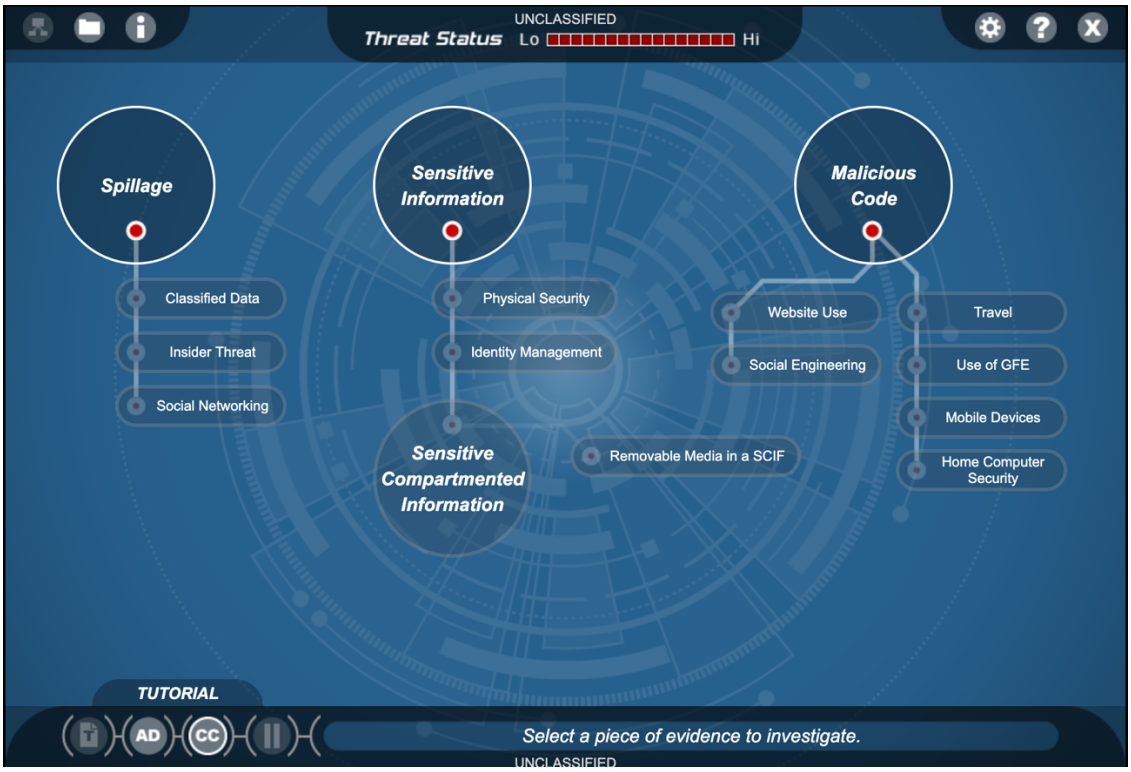

Figure B: Organization of Cyber Awareness Challenge modules.

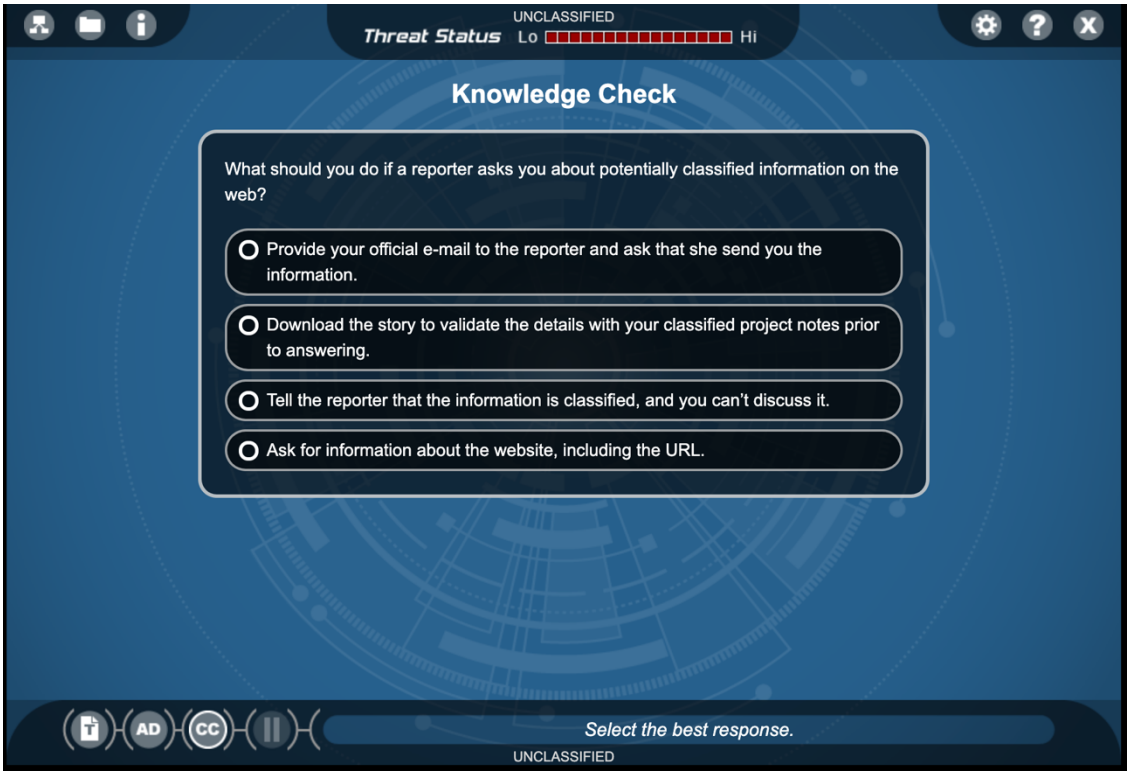

Figure C: Knowledge Check question example from the "spillage" module.

Addressing the Skill Gap among Army Personnel

There is a huge skill gap between members of the Cyber force and those who are not. Obviously, it is necessary for cyber personnel to be subject matter experts of their trade, however the main discrepancy can be found in other kinds of training. For anyone who enters into the military, they must go through Basic Training, no matter what military occupation specialty (MOS) or branch they eventually enter. This training includes rifle marksmanship, land navigation, and other necessary skills to plan and perform land operations, which are primarily carried out by infantry personnel (Military.com). These skills for most branches are not practiced often yet are still necessary to understand in order to support and integrate with infantry forces. Thus, understanding of these basic infantry skills are emphasized and often tested to ensure all personnel, not just infantry, are proficient.

On the other hand, many non-Cyber personnel, especially those who go into the infantry, are not required to have any similar, extensive cyber training. And yet, many of them will operate a computer or rely on a network-connected system. Just as civilians are constantly interacting with the Internet of Things, military vehicles and weapon systems are increasingly dependent on network connected systems/sensors (Schradin). While these systems increase efficiency in warfighting capabilities, they also provide the enemy with a new avenue of approach – through Cyberspace. This provides a new challenge of operational and mission readiness, one that is not reflected in the level of mandatory training now. And while those who frequently operate these systems may have an understanding of the specific cyber risks for these machines, it is still necessary for every individual to understand such risks, especially in combat.

Additionally, Cyber personnel have a deeper grasp on the reality of cyber threats. The Persistent Cyber Training Environment (PCTE) is used to highlight such threats and allow Cyber personnel to prepare for missions in a non-threatening environment (Pomerleau). This exercise is similar to field training exercises carried out by non-Cyber personnel, where units go out to the field to conduct a mission that is similar to one carried out on deployment. They are critical for hands-on training and active participation of soldiers. These exercises help personnel understand the reality of threats. Although a training as rigorous as the PCTE is not necessary for non-Cyber personnel, it must be as interactive. It is necessary to ensure that they understand that these cyber threats are real and persistent and must be able to recognize such threats.

Steps to Increase Cybersecurity in the Military

There are three inherent aspects of the military that discourages personnel from engaging in cybersecurity training: lack of supervision, competing time commitments, and lack of engaging content. To improve this, there must be movement towards weaving realistic, hands-on training for the general population, just as there is infantry style training for everyone entering service. The following outlines a few plans of actions that increase prioritization of cybersecurity.

Fostering discussions on importance of cybersecurity awareness

Lack of supervision encourages people to put sub-par effort into the training. This means that there is no learning or retaining of information, especially long enough for the next training. To increase the supervision that goes into training, leaders can foster discussions on the importance of cybersecurity awareness. This is done when discussing topics such as leadership, respect for others, and importance of diversity. It is also done while revisiting basic infantry skills as well. Whenever there is a lull in training or ample free time, these topics are discussed to fill up the free time. Thus, adding cybersecurity awareness to the list will increase supervision on how well it is learned and retained.

The costs of this option seem minimal, but for well-prepared discussion there must be a leader willing to sacrifice time. Discussions may occur on a whim, but they require someone knowledgeable to lead the discussion. This leader must be trust-worthy and inspiring to create a discussion with active participation, otherwise the time is still wasted. Overall, this is a cost-effective option that is time-consuming but provides better supervision in learning.

Setting priority in training

The amount of time spent on infantry training places a level of importance on knowing the skills. This importance is exemplified through field exercise trainings and mandatory retrains of basic infantry skills. In order to increase priority of cybersecurity training, more time must be dedicated. This also involves a lot of planning, ensuring the unit training calendar has time. Additionally, there must be someone to lead and plan the trainings. It is essential to provide a subject matter expert to teach a crowd with varying levels of understanding. This expert may come directly from the Cyber force or may be a volunteer from the cybersecurity community,

although the latter option may be costly. This option will help increase the awareness of how probable cyberattacks are by increasing the amount of time dedicated towards learning about cybersecurity.

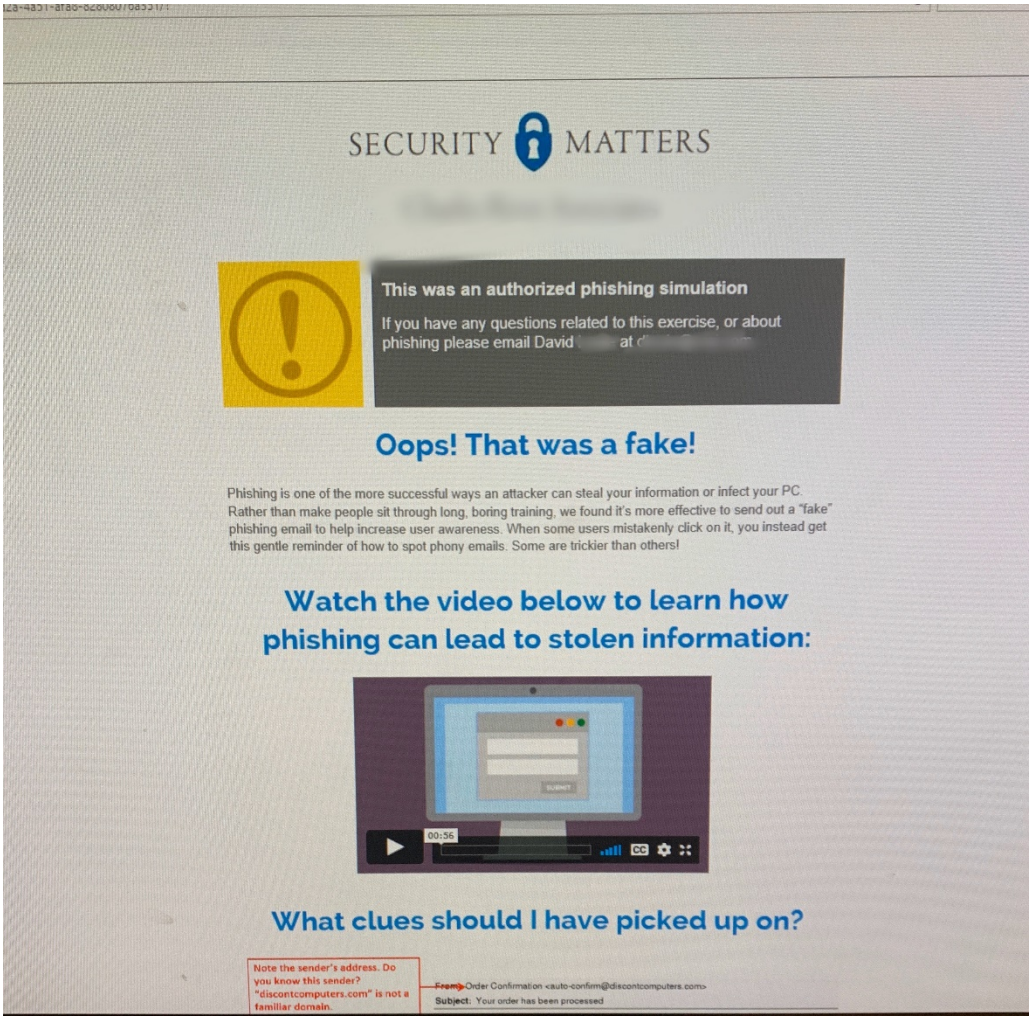

Figure D: Example training for phishing email in non-threatening environment

Allowing non-Cyber personnel to participate in skill refining/expanding opportunities

This by far is the costliest option but could be the most rewarding. By sending non-Cyber personnel to these opportunities, they are constantly interacting with training that is hands-on and lets them actively use skills in a non-threatening environment. Such opportunities could include the PCTE that occurs for Cyber personnel or conferences such as the National Cyber Summit, which occurs annually and has an impressive array of topics such as social engineering, forensics, and the cloud (2019 National Cyber Summit). These opportunities may vary in cost,

depending on the level of planning, travel costs, etc. necessary to participate in these opportunities. Additionally, the number of opportunities, especially civilian-held, is great and thus units have a lot of choices of where to send necessary personnel.

Even after implementing any of these options, noticeable change will take time. Proficiency in necessary cybersecurity skills must be flexible to ever-evolving technology. The training must be dynamic to match these changes, and overall this is difficult for the military. The nature of bureaucracy within the military inhibits rapid change, something that impacts the security of network-connected securities as well (Freedberg). However, as the military looks deeper into agile development and DevSecOps, perhaps this resistance towards change will lighten.

Conclusion

While the amount of money dedicated to the Cyber force is increasing from year to year, none of that budget increase is dedicated to cybersecurity training and will probably not be used to train non-Cyber personnel (Under Secretary of Defense, 1-5,1-10). The current annual training required is intensifying the skill gap between Cyber and non-Cyber personnel. With the increase access to DoD IT systems and development of network-connected weapons and vehicles, there should be more demand for general cybersecurity proficiency. It is risky to continue to rely on a small group of experts to continuously monitor and keep track of cyber threats and attacks. The military must begin to emphasize the importance of cybersecurity understanding and awareness. This can be done through one or more of the aforementioned suggestions but must start with leadership. The leaders of the military must start emphasizing cybersecurity's importance and the necessity for individual proficiency. If individual proficiency was emphasized on the tactical level, then society can trust the military's ability to defend the nation on the newest warfare domain, cyberspace.

References

"2019 National Cyber Summit: June 4-6, 2019." *2020 National Cyber Summit*.

Alley, Squawk. "Reuters: US Opens National Security Investigation into TikTok." *CNBC*, CNBC, 1 Nov. 2019.

"Cyber Awareness Challenge." *DoD Cyber Exchange*, Defense Information Systems Agency (DISA).

Freedberg, J. "Can DoD Get Speed & Security With The Cloud?" *Breaking Defense*, Above the Law, 13 Nov. 2019.

Military.com. "What To Expect In Army Boot Camp." *Military.com*.

"Officials Detail Scope, Units of AFCYBER Command." *U.S. Air Force*, 14 Mar. 2008.

Pomerleau, Mark. "What Happened at the Military's Biggest Cyber Training Exercise to Date." *Fifth Domain*, Fifth Domain, 24 July 2019.

Schradin, Ryan. "Today's Incredible, Hackable Weapons Systems." *Government Technology Insider*, 1 Feb. 2019.

Snider, Mike. "Using FaceApp to Age Your Photos May Be Fun, but You Could Be Giving up Your Privacy." *USA Today*, Gannett Satellite Information Network, 18 July 2019.

Strickland, Aaron, and Naval Network Warfare Command Public Affairs. "Navy Cyber Forces Established." *Navy Cyber Forces Established*, 26 Jan. 2010.

"Timeline of Army Cyber." *Goarmy.com*.

"U.S. Defense Spending Compared to Other Countries." *Peter G. Peterson Foundation*, 3 May 2019.

United States, Department of Defense. "DoD 8570.01-M: Information Assurance Workforce Improvement Program." *DoD 8570.01-M: Information Assurance Workforce Improvement Program*, 2005, pp. 1–98.

United States, Office of the Under Secretary of Defense. "Defense Budget Overview." *Defense Budget Overview*, 2019.