**How does Cyber-Security Awareness Training improve security standards in the medical and healthcare fields?**

Jesse Chin

IDS 300W: Interdisciplinary Theory and Concepts

Dr. Kathryn LaFever

April 18, 2022

**Abstract**

With the consistent evolution of technology, cyber crime continues to grow. In the medical and healthcare industries, businesses and people alike are targeted by threat actors for the potential access to private health information and unwarranted access to computer systems which can be used for a variety of purposes ranging from monetary gain, and business disruption, to damaged and stolen data. Cyber security awareness training is one of the industries most effective methods in improving cyber security standards. How it improves cyber security in the medical and healthcare fields is understood by taking an interdisciplinary approach in studying its positive effects through the political, business, and mathematic disciplines.

 *Keywords:* Cyber-security, cyber-security awareness, healthcare,

Technology is an endlessly, evolving aspect within modern society. Whether it has been acknowledged or not, computerized, and technological advancements have made their way into every aspect of human life. Everything from communication, and entertainment, to education, and professional careers incorporate the advantages of computers and digitized information. However, the benefits of technology are not without risks as cyber-crime has become a growing consequence parallel to evolving technologies. The intent behind acts of cyber-crime ranges but the most common reasonings include financial gain, stealing information or property, or social/ political terrorism. (Perakslis, 2014) One of the most targeted industries in relations to cyber-crime are the medical and healthcare industries. The potential access to personal information and private computer systems makes businesses and people ideal targets alike. While there are numerous safeguards and tools organizations and people can utilize to prevent themselves from being victimized, one of the most fundamental concepts put to practice is improving upon one’s *cyber security awareness*. Many companies have made it a common business standard to train employees in cyber security awareness. Doing so helps to reduce the potential risk of criminal gain and data loss while simultaneously increasing the general knowledge of recent technologies the company may have adopted. This paper discusses the question of how does cyber security awareness training (C.S.A.T for short) improve cyber security standards in the healthcare and medical fields. The effectiveness of said training is understood by comprehending the implications viewed from a mathematical, business, and political perspective. Although it can get convoluted to approach the subject matter from various disciplines, researching the topic from an interdisciplinary standpoint provides invaluable insight to the practical applications and benefits C.S.A.T. has brought to the healthcare and medical fields. The reason behind choosing this question is not only because it directly ties into my cyber-security major, but because the concept has been a long-running and highly debated discussion argued back and forth in the professional industry. As the paper continues, substantial reasoning is provided to support the idea that cyber security awareness training is not only effective but undeniably necessary in helping create a more secure standard in the healthcare and medical industry.

 Before being able to recognize the effectiveness of C.S.A.T, it helps to understand what cyber security awareness is, what the trainings can consists of, and common phrases and terms used in the cyber-security and the healthcare industries. Cyber security awareness is the level of understanding an individual has regarding general safety practices when utilizing a computer and its systems. (OA.MO.GOV, 2022) Cyber security awareness training can very among different industries and companies; however, the general structure of training may involve learning about the distinct types of malware¸ how it could be delivered to an employee’s computer, safety techniques on identifying possible threats, and the company’s own guidelines on how to report and handle possible cyber threats. Malware is “a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim’s data, applications, or operating system...” (NIST) Malware is a technical description for several types of computer viruses. Criminals who engage in malicious cyber activities are referred to as *threat actors.* These instigators attempt to infiltrate and disrupt computer systems by distributing malware in numerous ways. One of the most common methods as seen in the healthcare industry is via *phishing* *emails*. These types of fraudulent messages are created by threat actors to appear as legitimate correspondence in order to trick victims into providing private data or downloading malicious malware. In the healthcare industry, common types of targeted data include any form of payment information or *PHI,* personal health information. The paper includes information regarding federal legislations pertaining to the usage and storage of such data. The *Health Insurance Portability and Accountability Act of 1996 (HIPAA)* refers to the privacy regulations a business in healthcare and medicine must maintain in managing and utilizing a patient’s PHI. (Mbonihankuye et el., 2019) The *Health Information Technology for Economic and Clinical Health Act (HITECH Act),* which is a part of HIPAA, pertains to providing criminal penalties for breaking HIPAA privacy laws as well as allows for PHI audits to verify they are not being abused. (Heckler & Edwards, 2014) While the explanations are simple, knowing these terms and references assists in better understanding the improvements C.S.A.T. brings.

 Because cyber security awareness policies and training differ among industries, there is no standard guideline companies follow. Instead, having the flexibility to create a customized regime, allows companies to cater to their specific needs so long as they comply with federal legislations. Per political science, HIPAA is a common link between cyber security and the healthcare industry. With HIPAA, a person’s PHI is allowed to be digitized for ease of accessibility but requires that the business that manages the PHI to take precautions in securing the information from a cyber-security perspective. Since HIPAA is a federal mandate, employees in the medical industry are required to be professionally trained in handling PHI. “Security awareness training must be implemented. So, employees are trained and reminded of policies and procedures..., and other key security measures.” (Mbonihankuye et el., 2019) Should improper or a lack of training take place, a risk of broken privacy regulations is presented. The HITECH Act will catch these issues due to its ability to audit the situation. (Hecker & Edwards, 2014) While there may be numerous laws pertaining to cybersecurity, the fact that the U.S. government saw fit to pass these regulations pertaining to PHI used by healthcare professionals and medicals businesses, a correlation is seen that the federal government is favoring toward behaviors that revolves around proper C.S.A.T.

 According to (Garner & Thomas, 2014), the concept of how effectiveness is measured in a numerical aspect can be taken from various points of data, or *measurements*. In the instance of measuring effectiveness in C.S.A.T, since there can be multiple factors of measurements, (for example: how many phishing emails were opened by untrained employees, how many computers were infected with malware, etc.) all these points of data are culminated into what is known as a *metric*. “Metrics are generated by the analysis of measurements. A metric is a comparison of two or more measurements taken over a certain amount of time and compared to a predetermined baseline.” (Gardner & Thomas, 2014) An example of how mathematics verifies the improvement brought on by cyber-security awareness training is represented through a recent study completed back in 2019 by the National Technical University of Athens. (Georgiadou et al., 2021) Over the course of a three-month period, a number of Greek healthcare facilities participated in a cyber-security awareness webinar customized for the healthcare system. The measurements were collected in two parts: participants completed questionnaires pertaining to the training concepts/ opinions of the webinar’s effectiveness and at some point, they were unknowingly subject to a fake phishing scheme to evaluate to their knowledge post training. A variety of metrics were calculated based on categories of cyber-security awareness training, accuracy, demographics, profession, and percentage of correct answers over individual and groups: 77% of participants were accurate in identifying how businesses should allocate their resources to training, 67% were accurate in generating a security plan guideline for the employer to follow, 90% understood efficient cyber security awareness habits, etc. While there were positive statistics, the study also concluded there was room for improvement in the structure of the training given and that changing it could provide additional results, but it was also stated that “regular training could certainly shield an organization…” (Georgiadou et el., 2021)

 When imagining the phenomena of a business discipline, a variety of visualizations are given. The hierarchical structure of a work environment, an employee’s relation to the company and vice-versa all form the concept we as humans understand as business. A systematic review completed back in 2021 by (Nifakos et el., 2021) took an in-depth review into the business environment of healthcare organizations and how it affected employee relations to their understanding of cyber-security awareness. The paper references additional resources in relation to its findings by notating “…the literature considers how the lack of sufficient training and awareness impacts healthcare organizations facing ever-increasing cyber threats.” (Nifakos et., 2021). It further continues to state that per healthcare organizations, there are some that promote cyber-security awareness greatly and emphasizes the importance of further development and training to improve safe practices regarding attacks, like phishing. While this is a much more direct approach in understanding the benefits, a cost-benefit analysis framework, developed by (Zhang et el., 2021) provides a more conceptual idea of how businesses, including those in healthcare, have benefited from proper C.S.A.T. Summarizing the analysis framework, Zhang et el., (2021) highlights the importance of proper allocation of resources regarding cyber-security and training. By being able to understand how a company can optimize their resource allocation in an effective manner, C.S.A.T becomes more effective for employees. However, the most significant piece of knowledge coming from the analysis revolves around understanding cost versus potential loss: that the cost of a well-developed C.S.A.T. will benefit the business more than not funding C.S.A.T and the potential loss resulting from a cyber-attack.

 The common ground, found among the three disciplines, is evaluated not by the direct correlation they have with one another but instead how the benefits and consequences seen in each discipline can coincide at times. For instance, the paper’s overall argument defines how C.S.A.T improves cyber security in the healthcare field. Mathematically, proper C.S.A.T provides positive results in dealing with potential malware and threat actors as referred to in Georgiadou et el., (2021). Positive results can lead to reduced risks for potential attacks. In the medical industry, reduced attacks mean less chance for PHI to be stolen, meaning HIPAA laws are less likely to be broken. Since no laws are broken, less legal consequences for healthcare businesses. And since there are no lawsuits, legal fees, or fines pertaining to broken legislations, from a business perspective a company has more freedom to allocate additional resources and potentially grow. However, one key factor that is consistently mentioned throughout the research literature is acknowledging that while C.S.A.T. is effective, it only is so for as long as proper planning and knowledge are used to create an effective C.S.A.T. One discipline that will be necessary to study in the future regarding this topic would be psychology or sociology. At its core, how C.S.A.T. is utilize falls onto how employees (people) react and perceive from the training. Insight from a discipline that deals with the actions and thought processes of people will provide interesting results.

 Cyber-security awareness is the level of understanding a person has regarding safe computer habits and the potential dangers. In the healthcare industry, cyber-security awareness training is utilized to help protect businesses and people from potential threat actors seeking to steal PHI or gain unauthorized access to the business’s systems. By taking an interdisciplinary approach, I was able to understand how cyber security awareness training improves cyber security in the medical and healthcare fields. The insight provided from researching the concept through a mathematical, business, and political discipline gives way to understanding that doesn’t exist in a traditional disciplinary mindset. And taking that perspective, and further applying it to cyber security and its place in the healthcare or industry will undoubtedly provide new insights that may never have been viewed before simply because it has always been seen through one point of view.

**References**

* *Compliance Component*. (n.d.). Retrieved April 19, 2022, from https://oa.mo.gov/sites/default/files/Carpool%20Newsletter%2001%20-%20June%202018.pdf
* Editor. (n.d.). *Home*. CSRC. Retrieved April 18, 2022, from https://csrc.nist.gov/
* Gardner, B., Thomas, V., & Thomas, Valerie. (2014). *Building an Information Security Awareness Program Defending against Social Engineering and Technical Threats*.
* Georgiadou, A., Michalitsi-Psarrou, A., Gioulekas, F., Stamatiadis, E., Tzikas, A., Gounaris, K., Doukas, G., et al. (2021). Hospitals’ Cybersecurity Culture during the COVID-19 Crisis. *Healthcare*, *9*(10), 1335. MDPI AG. Retrieved from <http://dx.doi.org/10.3390/healthcare9101335>
* Hecker, L., & Edwards, A. (2014). The Impact of HIPAA and HITECH: New Standards for Confidentiality, Security, and Documentation for Marriage and Family Therapists. *The American Journal of Family Therapy,* *42*(2), 95-113.
* Mbonihankuye, S., Nkunzimana, A., & Ndagijimana, A. (2019). Healthcare Data Security Technology: HIPAA Compliance. *Wireless Communications and Mobile Computing,* *2019*, 1-7.
* Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina,
	+ S. (2021). Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review.*Sensors (Basel, Switzerland), 21*(15)<http://dx.doi.org/10.3390/s21155119>
* Perakslis, E. (2014). Cybersecurity in Health Care. *The New England Journal of Medicine,* *371*(5), 395-397.
* Zhang, Z., He, W., Li, W., & Abdous, M. (2021). Cybersecurity awareness training programs: A cost–benefit analysis framework. *Industrial Management Data Systems,* *121*(3), 613-636.