Cyber Teaching Hospitals: Developing Cyber Workforce Competence

James R. Elste[1][a] and David Croasdell[2][b]

[1]*Cyberworkerz, 5 Cowboys Way, Suite 300, Frisco, Texas, U.S.A.*
[2]*Department of Information Systems, Univ. of Nevada, Reno, NV, U.S.A.*

Keywords: Cybersecurity Education, Cyber Workforce, Cyber Skills Gap, Cyber Teaching Hospitals, Cyber Clinics, Cyber Hygiene, Conscious Competency.

Abstract: The cybersecurity profession suffers from a crisis commonly referred to as the "Cyber Skills Gap." The crisis highlights the dramatic shortage of cybersecurity awareness and skills in the modern workforce. This manuscript presents an alternative approach to the current cybersecurity educational paradigm. We propose a novel solution that would establish a system of cyber teaching hospitals. We provide an overview of the history and development of medical teaching hospitals and extrapolate the model to the cyber security domain. Incorporating the Conscious Competence model into the development of practical skills in a Cyber Teaching Hospital provides a structure for experiential learning and the acquisition of cybersecurity skills.

1 INTRODUCTION

The cybersecurity profession suffers from a crisis commonly referred to as the "Cyber Skills Gap." The crisis highlights the dramatic shortage of cybersecurity awareness and skills in the modern workforce. This manuscript presents an enhancement to the cybersecurity educational paradigm. What is required is an orthogonal strategy that catalyses the adaptation of existing education programs and cybersecurity practices. Put simply, we need to try something different. We propose a novel solution by creating a network of cyber teaching hospitals – a construct that fosters the adaptation of education programs and advancement of cybersecurity practices, while complimenting existing programs. We borrow from the field of that medicine to propose a sufficiently instructive model for effectively developing both practices and practitioners in a complex problem space. Specifically, the practical education of medical professionals in teaching hospitals. A conventional approach to medicine with a long and progressive history of the effective development of competent practitioners in a complex knowledge domain.

1.1 Efforts to Quantify the Cybersecurity Skills Gap

The current consensus is that there is a worldwide gap in skills needed for a competent cybersecurity workforce. (Vogel, 2016) Implied in the multitude of references in current research publications to this cybersecurity skills gap crisis is a concern regarding the competence of cybersecurity practitioners and the relative efficacy of the education programs that strive to produce qualified cybersecurity professionals. This is not an indictment of the practitioners, who with time, effort and experience will usually achieve a level of proficiency. It does, however, bring into sharp relief the complex challenges extant in the cybersecurity domain and failure of academic programs to adequately adapt curriculum to prepare students to enter the cybersecurity profession. "An evaluation of U.S. cybersecurity workforce development initiatives must ask whether cybersecurity education and training programs are preparing students for the kinds of high-skilled technical roles that represent the most serious workforce shortage. The evidence suggests that the answer may be no." (Crumpler, 2019)

Alan Paller, in his testimony before the Nevada Technological Crimes Advisory Board ("NV-

[a] https://orcid.org/0000-0001-5565-3701
[b] https://orcid.org/0000-0002-6160-6271

Elste, J. and Croasdell, D.
Cyber Teaching Hospitals: Developing Cyber Workforce Competence.
DOI: 10.5220/0011783800003405
In *Proceedings of the 9th International Conference on Information Systems Security and Privacy (ICISSP 2023)*, pages 643-650
ISBN: 978-989-758-624-8; ISSN: 2184-4356

TCAB") was more direct – "…the colleges and community colleges are not working as a supply pipeline. They are completely failing the nation. Well, maybe not 'completely' – maybe one half of one percent is not failing the nation." (Paller, 2011)

This is not for lack of effort, as many institutions of higher education have established or expanded cybersecurity education programs and associated degrees. To the contrary, there is a significant global effort to formalize and improve cybersecurity education. So why do we still have a gap? Is this simply a matter of demand exceeding the production capacity of our educational institutions to produce a supply? Do we have a thornier problem of adequately defining the requirements for a qualified security practitioner? Why do we appear to be unable to define requirements, develop effective curriculum, share practices across institutions so that we can achieve some level of consistency matriculating qualified practitioners, and then simply increase the volume of production?

There is a significant amount of work being undertaken to try and understand these very questions. An extensive two volume RAND Corporation study of the U.S. Air Force ("USAF") exploring the views of the enlisted and civilian workforce to support the USAF goal to "revamp and improve the training and development of its offensive and defensive cyberwarfare workforce" provides insight into the perspectives of the individuals in the workforce. (Hardison, 2022) The examination of programs, such as the National Initiative for Cybersecurity Careers and Studies Workforce Framework for Cybersecurity ("NICE Framework"), for the development of profiles of cyber security job roles, commonly encompassing inventories of knowledge skills and abilities to define the activities of cybersecurity professionals, reflect the initiative to address the problem, but lack the practical solutions to effect change in the current educational programs.

Borka Jerman Blažič provides a good review of the efforts in the European Union and observes they "…indicate that cybersecurity encompasses a very broad range of specialty areas and work roles, and that no single educational programme can be expected to cover all of the specialized skills and sector-specific knowledge desired by each employer. However, the studies pointed clearly that there are certain knowledge sets and skills that are essential for any new employee performing critical technical work where cybersecurity issues are present, regardless of the field they are in or the specialty they adopt." (Blažič, 2021) In a review of the the academic literature Ruoslahti et al indicate a bias that "primarily discusses current cybersecurity issues, such as cyber threats, cyber-related training and qualifications, and training." (Ruoslahti, 2022)

1.2 Our Approach to Address the Cybersecurity Skills Gap

"One of the challenges in writing an article reviewing the current state of cyber education and workforce development is that there is a paucity of quantitative assessment regarding the cognitive aptitudes, work roles, or team organization required by cybersecurity professionals to be successful." (Dawson, 2018)

We will not recapitulate the current efforts to analyse and quantify these job profiles and training requirements for the cyber domain, rather we highlight the gap in the practical application of skills and experiential learning, which is commonly addressed in the medical profession through residency in a teaching hospital.

We will provide a overview of the history and development of medical teaching hospitals and extrapolate the model to the cyber security domain. We incorporate the conscious competence teaching model to address questions of the development and measurement of competence in a complex field of study. Finally, we demonstrate the potential for the Cyber Teaching Hospital construct by incorporating the results of our prior research into training interventions in the form of "Cyber Clinics." "In a cyber clinic, trained "cyber-medics" provide individualized guidance on good cybersecurity practices to the participants. This provides a more engaging and effective interaction for the participants and allows the students to apply their cybersecurity knowledge in a meaningful way, generating an experiential learning opportunity." (Croasdell, 2018)

2 A BRIEF HISTORY OF TEACHING HOSPITALS

Humankind has always faced the existential threat of illness. We have evolved from a reliance on superstitious folk medicine, practices such as bloodletting and leeches, to effective, scientifically evaluated and proven practices of bloodletting and leeches. "Medicinal leeches were used by Egyptian, Indian, Greek and Arab physicians thousands of years ago. The main application was bloodletting…In the 1960s, physicians rediscovered the pharmacological potential of leech saliva." (Lemke, 2020)

2.1 A Few Thousand Years of Development

The art and science of teaching medicine has evolved significantly over the last few thousand years and in that evolution the current medical training paradigm favours the teaching hospital as the final stage of the development of practitioners to ensure their competence in the application of medical knowledge and practices.

While we enjoy the benefits of the current practice of medicine, it took a little while to develop these teaching modalities. According to HD Modanlou, the origins of the teaching hospital are inaccurately portrayed as emerging in Europe during the Middle Ages or early renaissance periods, however this appears to be the re-emergence of the academic medical center after the “Dark Ages”. The development of modern academic medicine includes “the contributions of Greeks, Persians, Indians, Syriacs and Jews assembled first in the city of Gondi-Shapur in the Persian empire (third to eighth century AD), then later in Baghdad and Spain (ninth to thirteen century AD). The innovative medical practice and teaching hospitals and writings of medical texts during these periods ushered in the birth of current teaching hospitals, medical schools and the rise of academic medicine.” (Modanlou, 2011)

As late as the 19th century, the practice of training competent medical professionals still suffered from challenges, not always related to the lack of scientific knowledge about medicine, but rather defects in the institutions. One example from Sir Arthur Tomson’s “History and Development of Teaching Hospitals in England” describes oversights in the process as a “nineteenth century official inquiry established the interesting fact that, though many doctorates of medicine had been conferred on members of this university…the men trained in this haphazard way [produced] a vast army of quacks who had no instruction of any kind and who certainly never endured any examination before they embarked on their careers. (Thomson, 1960)

Quackery has not been eliminated from medicine, however, as the rise of the Internet seems to have revitalized some superstitious practices, but science continues to redeem itself and demonstrates that it produces more reliable interventions.

2.2 The Practical Application of Skills

In a teaching hospital the focus is on the delivery of medical interventions to real patients. It is the practical application of knowledge and skill, in an operational setting, that provides the opportunity for the practitioner to solidify their ability to practice medicine. Becoming a qualified medical professional is not simply a matter of developing sufficient knowledge in a classroom setting, it involves integrating the education into an operational function.

A comparative analysis of a primarily didactic learning model and a teaching hospital that is “multi-faceted, employing lectures, outpatient clinic attachments, inpatient bedside teaching, clinical skill practice, small group learning, clinical reasoning and others” favoured the teaching hospital. (Fanwei, 2019)

This brief history of teaching hospitals illustrates both the time-tested efficacy of the teaching hospital model, as well as the long and arduous journey to develop effective interventions and competent practitioners. Society and individuals enjoy benefits from modern medical advances like penicillin, MRIs, and when medically necessary and prescribed by a qualified practitioner – leeches.

3 DEVELOPING COMPETENT CYBERSECURITY PRACTITIONERS

Developing competent cybersecurity practitioners presents a unique challenge that is in many ways very different than the development of qualified medical practitioners. It requires the evaluation of competence in the application of skills in an adversarial environment, not simply evaluating the acquisition of knowledge.

3.1 Incorporating the Conscious Competence Model

Developing skills in any field of endeavour is different than mastering a body of knowledge. Effectively, the development of skills comes from the application of the skill. This truth is summed up best in the old joke – “How do you get to Carnegie Hall? Practice, practice, practice.”

This simple truism applied to music is illustrative of the cyber skills development challenge. One may study music theory, attend lectures and recitals, but the primary development of a musician’s ability to play the instrument comes from extensive practice.

Cybersecurity professionals are practitioners of applied knowledge through the instrument of information technology. Some play their instrument well, others need more practice to become competent.

The heart of the cybersecurity skills gap problem is the competence of practitioners with the application of skills in the "real-world" of industry. Citing both PriceWaterhouseCoopers and European Cybersecurity Organization ("ECSO") studies, Blažič revealed that the inefficient skills-matching among the candidates was the leading cause of failed hires and in the ECSO study that "results pointed also to several gaps in the organizational capabilities and of the employee's skills required for implementing cybersecurity rules and tools in everyday business life." (Blažič, 2021)

Incorporating the Conscious Competence model into the development of practical skills in a Cyber Teaching Hospital provides both a structure for experiential learning and a basis for evaluating performance and the acquisition of cybersecurity skills.

Howell succinctly describes the four stages as follows:

> *"Unconscious incompetence - this is the stage where you are not even aware that you do not have a particular competence. Conscious incompetence - this is when you know that you want to learn how to do something, but you are incompetent at doing it. Conscious competence - this is when you can achieve this particular task, but you are very conscious about everything you do. Unconscious competence - this is when you finally master it and you do not even think about what you have to do such as when you have learned to ride a bike very successfully."* (Howell, 1982)

Just like learning to ride a bike, we struggle and fail at first, then, as we practice, often with guidance, we develop sufficient skill to ride unaided, and as we continue to ride the bike, encountering unknown challenges (i.e. bumps in the road) we develop the unconscious mastery of bike riding. We simply no longer have to think about what we are doing; we just do it. This level of competence is the goal in cybersecurity skills development.

Applying the conscious competence model to cybersecurity skills is arguably more difficult than riding a bike, however a more precise objective is to develop sufficient competence to evaluate a situation, make a decision, and take appropriate action. As Alan Paller noted in his testimony "It's a shift in thinking about cyber security – from it being something you learn from a book, to it being something you actually have to know how to do. And, you have to do it under pressure when other people are fighting against you. It is just a whole different view of cyber security training." (Paller, 2011)

3.2 Developing Cybersecurity Skills Through Simulations and Games

As Higher Education institutions ("HEI") expand cybersecurity offerings, they predominantly focus on theory and fall short on practical "hands-on" experimentation. (Topham et al., 2016) The conventional approach to developing practical cybersecurity skills is through case studies, simulations, cyber ranges and cyber contests.

"Case studies are prevalent in cybersecurity courses that teach adversarial thinking. Students are taught about specific attacks, which often requires spending time on idiosyncratic implementation details…Some students are able to generalize from this material, and they develop an intuition for identifying assumptions that can be violated to achieve some goal—the essence of any attack. Other students, who don't make the leap from specific attacks to adversarial thinking, are not well served." (Schneider, 2013)

Simulations attempt to model case studies in an interactive environment. While this is an improvement to the "read and discuss" approach to case studies, it suffers from a lack of integration into the broader operational practices that are required in real world situations.

Simulations are "a powerful modality for training medical professionals to improve team-based communication skills, manage uncommon or high-stakes clinical situations, practice procedural techniques, and refine medical decision-making skills in a safe environment that allows for the learner to benefit from both self-reflection and constructive feedback." (Dameff et al., 2019)

Cybersecurity simulations are predefined and controlled, not something that replicates the often times chaotic reality of incident response. They may be tightly focused on a specific cybersecurity challenge or more elaborate simulations of cybersecurity and have utility early in the development of a cybersecurity practitioner.

In their extensive analysis of Cyber Ranges and Test Beds, Ukwandu et al. (2022) provide an analysis of current cyber ranges and a taxonomy to describe the elements of cyber ranges and test beds. They go on to describe the objectives of a cyber range. The spine of the training is founded on strategies informed by educational methodologies and is most often segmented into two classes. The first is centred on the relationship between coach and trainee using classical training methods characterised by the use of a number of support tools such as online courses, certification, training, and presentation. The second method relies more heavily on new elements such as gamification and video-assisted techniques. (Ukwandu, 2020)

Cybersecurity games are less contrived than simulations allowing the student to develop their skills in an adaptive manner. The generally accepted and oxymoronic term "serious games" aptly describes the objective of most cyber contests, such as Capture the Flag and Red Team/Blue Team exercises. According to Le Compte, et al the definition has been debated and redefined. They use Zyda's 2005 definition describing serious games as "a mental contest, played with a computer in accordance with specific rules, that uses entertainment to further government or corporate training, education, health, public policy, and strategic communication objectives" (Le Compte, 2015)

While simulations, cyber ranges and cyber competitions are useful tools in developing a competent cybersecurity practitioner, they share one common weakness – they are disintegrated from the actual practice of cybersecurity in the real-world.

3.3 Developing Conscious Competence Through "Combat" Experience

As the saying goes, "experience is the hardest teacher, it gives the test first and the lesson after."

One of the realities uncovered via surveys of USAF cybersecurity practitioners reflects the schism between training and actual practice. Describing the training system as broken and lacking relevance. One study participant sums it up:

> *"That's why I say just get people to mission…the Air Force way of training is they send you to school and you learn everything you can there, but only that. Then, at the next school, they tell you to forget everything from the last school and learn only what we're teaching you. Then, you get to your unit, and they tell you to forget everything that you learned in training because it's all bull and out of date—this is the stuff you need to learn here. Then, you get to your actual shop, and they say to forget what your unit told you. Then, you go to another base, and it happens again. It takes 3.5 years to get through training, and, at every stage of the pipeline, this happens. That's how Air Force training goes."* (Hardison, 2021)

Just get the people to mission is perhaps the most succinct description of the objective of a Cyber Teaching Hospital. We learn much in the preparation of modern Cyber Warfighters. Regrettably, we learn more from actual warfare.

The U.S. Civil War was fought "in over 10,000 places and was the bloodiest war in the history of the United States. More Americans died in the Civil War than in all other wars combined…During the Civil War, there were many medical advances and discoveries…How medical care was delivered on and off the battlefield changed during the war. (Reilly, 2016).

A surplus of patients in need of medical attention, from both battlefield wound and disease, provided the opportunity to advance the practice of medicine born out of necessity. Innovation occurs when demand for improvements intersects with the opportunity to apply and evaluate novel interventions. Both practitioner competence, as well as the practices and protocols improve.

Do we not also have a surplus of organizations that struggle in the face of constant cyber-attacks? Are we not involved in a conflict with a motivated adversary? If so, why are we not taking full advantage of the real-world opportunities to develop both cybersecurity practices and competent cybersecurity practitioners?

In researching the issues with small to mid-size businesses ("SMB"), we reinforced the need for direct intervention and propose to enlist the resources of the National Guard Defensive Cyber Operations Elements ("DCO-E") to aid struggling businesses with their cyber-defense. "Extending the cyber capabilities of the National Guard Defensive Cyber Operations Elements (NG DCO-E) to assist SMBs requires a delivery model that addresses the gap of cybersecurity practices between public and private sector organizations and the scalability challenge. While public sector organizations are few and large, as we have addressed, SMBs are many, smaller, and with limited resources…with government-funded Cyber Squads of student interns to help SMBs and to fill a desperately needed talent pipeline. By doing so, we will also be educating the next generation of cyber leaders." (Lathrop et al., 2023)

While calling out the National Guard to assist SMBs approaches the hyperbolic, the principles espoused in the proposal are relevant to developing a model of practical interventions with public and private sector organizations – legitimate casualties of the cyber-battlefield.

Approached as part of a network of Cyber Teaching Hospitals, designed to support the patient, train the practitioner, and advance research into cybersecurity practices capitalizes on the crisis, benefits the practitioner, and provides meaningful support to organizations struggling to cope with cyber-attacks.

In other words, we do not need war games, we need to enter combat and fight the war.

4 DEVELOPING COMPETENT CYBERSECURITY PRACTITIONERS

There is clearly a significant focus on the cyber skills gap problem, developing a cyber workforce and on enhancing cybersecurity education. As stated, we do not propose to recapitulate those evaluations or argue with their conclusions, they serve as a rational basis for developing Cyber Teaching Hospitals is a novel model that addresses some of the challenges and an augmentation to existing educational programs.

4.1 Cyber Clinics Demonstrate the Potential of the Cyber Teaching Hospital

In 2016, we developed a program to engage students in a direct cybersecurity intervention with students delivering cybersecurity expertise to individuals. We used the medical metaphors of "Cyber Clinics" and "Cyber-Medics" to focus expectations and orient the development of the student practitioners.

"Using the concept of a cyber teaching hospital as the organizing principle, the initial intervention focused on the problem of individual cyber-hygiene…To deliver the cyber-hygiene guidance in the most effective manner the model of a mobile medical clinic was adapted to take public health approach to "treat" individual participants. Cyber Clinics follow a triage, treat, and train approach where trained "Cyber-Medics" (students with sufficient knowledge to teach basic cybersecurity practices) provide personalized cybersecurity guidance. The main objective of a Cyber Clinic is to evaluate an individual's level of knowledge and current cybersecurity practices and then, in a one-on-one sessions with Cyber-Medics, to teach participants effective techniques in cyber self-defense. Cyber Clinics provide a mutually beneficial value proposition; the "patients" learn how to improve their cyber self-defense, and cyber-medics apply their cybersecurity knowledge and develop practical experience." (Croasdell et al., 2018)

Although the sample size was small, the results were notable:

- All participants said their knowledge of data, device and identity security issues and their awareness of issues increased after the clinic
- All participants said the Cyber Medics were "very helpful" and they would attend another Cyber Clinic
- Multiple participants implemented advice from the Cyber Clinic, specifically changing their passwords more often and backing up their device

Not captured in the 2018 paper, was the response from decision makers who authorized Cyber Clinics within their respective organizations. First, Nevada State CIO Shanna Rahming, after attending a Cyber Clinic held at University of Nevada, Reno offered to host a Cyber Clinic for state employees and their families. Governor Brian Sandoval allowed the Cyber Clinic to be hosted at the Governor's Mansion. In a single day, the Cyber-Medics trained over 100 individuals. When CIO Rahming reported the success of the Governor's Mansion Cyber Clinic to the NV-TCAB, the Nevada Attorney General Adam Laxalt requested Cyber Clinics for the employees in his Northern Nevada offices.

Seeing students train Deputy Attorney Generals, Law Enforcement Officers, and state employees in a professional and competent manner demonstrated the efficacy of the Cyber Teaching Hospital model for individual practitioners.

The success with students in the Cyber Clinic is supported by Ben Shneiderman's Relate-Create-Donate philosophy. He begins his 1998 paper with the following observation:

> *"Memorable educational experiences are enriching, joyful, and transformational. They enrich students with increased knowledge and skills, provide them with a satisfying sense of accomplishment, and reshape their expectations. Students are driven by intense motivation that propels them to solve challenging problems and fills them with the thrill of accomplishment. They are proud of what they have done, have a clearer sense of who they are, and are ready to take greater responsibility for their education."* (Shneiderman, 1998)

His three-component philosophy called Relate-Create-Donate stresses:

1. Relate: work in collaborative teams
2. Create: develop ambitious projects
3. Donate: produce results that are meaningful to someone outside the classroom.

He goes on to describe the central challenge to the model, one that we will elaborate upon. "A central problem is how to deal with the resistance to change, especially among teachers, but also among administrators and occasionally among students.

He describes it quite effectively as "the rewards of doing good by helping others are especially sweet when you are also helping yourself. This can be the case when students work on service-oriented authentic projects for clients outside the classroom." (Shneiderman, 1998)

All analogies to medicine and warfare aside, this is the philosophy/principle at the heart of the Cyber Teaching Hospital – education with a legitimate purpose and tangible benefits.

5 FUTURE RESEARCH

While we have developed the concept of the Cyber Teaching Hospital in terms of the fundamental value propositions of providing and adaptive model to address the cyber skills gap, enhance cybersecurity education, and create a collective intelligence facility to accelerate the development of effective cybersecurity practices, there are several aspects of the concept that require further elaboration and work. Specific areas include:

Contracting – patients in the Cyber Teaching Hospital model are in fact legal entities that establish relationships through contracts. A contracting model similar to a Managed Security Services Provider ("MSSP") looks like the best model but must integrate the legal requirements of the academic institutions and patient organizations.

Liability – Cybersecurity is a hazardous undertaking and the good guys. do not always win. Legal liability considerations must be accounted for and potentially ameliorated through statutory provisions for the benefit of society.

Cost – While we believe that the Cyber Teaching Hospital is a self-sufficient financial model at scale, potentially a profit center, if medical hospitals are any indication, however the catalysing funds are required to establish the initial Cyber Teaching Hospitals.

Faculty – academic institutions are also subject to the cyber skills gap. Some individuals in faculty positions would not be well qualified for a hands-on role, and we need to develop recruitment and development strategies to address the most noble role in cybersecurity – the competent educator.

Finally, the coordination and information-sharing potential of a system of Cyber Teaching Hospitals becomes the principal consideration once an implementation creates the first prototype and as the network emerges. The administration of the network of Cyber Teaching Hospitals.

6 CONCLUSIONS

In this paper we introduce the Cyber Teaching Hospital. An adaptive solution to address the cybersecurity skills gap, improve the education of cybersecurity practitioners, conduct research into novel cybersecurity interventions. support the continued formalization of the cybersecurity profession and, most importantly, to assist public and private sector organizations with their cybersecurity capabilities.

We provided an overview of the history and development of medical teaching hospitals and extrapolated the model to the cyber security domain. Incorporating the Conscious Competence model into the development of practical skills in a Cyber Teaching Hospital will provides a structure for experiential learning and the acquisition of cybersecurity skills.

Sir Thomson provides two examples of letters promoting Teaching Hospitals in England which led to the "foundation of the Royal Infirmary in Sheffield in 1789 is characteristic of many at the time. 'Of all the virtues which form our national character,' it runs, 'that of mercy and compassion may be justly esteemed the highest ornament.' Candour compels me to add, regretfully, that Dr. John Ash, in 1765 in Birmingham, did not take as high a line as your Dr. William Younge, for all he said in his original advertisement was, 'A general hospital for the relief of the sick and lame situated near the town of Birmingham is presumed would be greatly beneficial to the populous country about it as well as that place.'" (Thomson, 1960)

We conclude that the establishment of a network of Cyber Teaching Hospitals would likewise be greatly beneficial to any populous country and that mercy and compassion surely remain justly esteemed as the highest ornament.

REFERENCES

AB42 (2012) https://www.leg.state.nv.us/App/NELIS/REL/77th2013/Bill/872/Text

Bergström, A., Stringer, C., Hajdinjak, M. et al. (2021) Origins of modern human ancestry. Nature 590, 229–237 https://doi.org/10.1038/s41586-021-03244-5

Blažič, B. J. (2021). The cybersecurity labour shortage in Europe: Moving to a new concept for education and training. Technology in Society, 67, 101769.

Bowden, Mark. (*2011)* Worm: the first digital world war. New York : Atlantic Monthly Press

CDC (2017) https://www.cdc.gov/injectionsafety/ip07_standardprecaution.html

Chng, S., Lu, H. Y., Kumar, A., & Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. Computers in Human Behavior Reports, 5, 100167.

Croasdell. D., Elste, J. and Hill, A. (2018) Cyber Clinics: Re-imagining Cyber Security Awareness Proceedings of the 51st Annual Hawaii International Conference on Information Systems, Waikoloa, HI

Crumpler, W., & Lewis, J. A. (2019). The cybersecurity workforce gap (p. 10). Washington, DC, USA: Center for Strategic and International Studies (CSIS).

Dawson J and Thomson R (2018) The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. Front. Psychol. 9:744. doi: 10.3389/fpsyg.2018.00744

Dameff, C. J., Selzer, J. A., Fisher, J., Killeen, J. P., & Tully, J. L. (2019). Clinical cybersecurity training through novel high-fidelity simulations. The Journal of emergency medicine, 56(2), 233-238.

Fanwei, Q. U., Jin, H. E., Hua, M. A., Yanling, J., Wenlan, Z., Chongsuvivatwong, V., & Runsheng, J. (2019). A comparative analysis of medical education models and curriculums of a Medical University and a medical education center. JNMA: Journal of the Nepal Medical Association, 57(215), 45.

Gürer, D. (2002). Women in computing history. ACM SIGCSE Bulletin, 34(2), 116-120.

Hardison, C. M., Whitaker, J., Bean, D., Pavisic, I., Kramer, J. W., Crosby, B., ... & Haberman, R. (2021). Building the Best Offensive and Defensiv e Cyber Workforce.

Howell, W.S. (1982). The empathic communicator. University of Minnesota: Wadsworth Publishing Company

Hubbell 2008 DOI: 10.3138/jvme.35.1.062

Lathrop, L, Croasdell, D & Elste, J (2023) Extending the Cyber Capabilities of Small to Midsize Businesses Proceedings of the 56tht Annual Hawaii International Conference on Information Systems, Ka'anapali, HI

Lemke, S., & Vilcinskas, A. (2020). European medicinal leeches—new roles in modern medicine. Biomedicines, 8(5), 99.

Le Compte, A., Elizondo, D., & Watson, T. (2015, May). A renewed approach to serious games for cyber security. In 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace (pp. 203-216). IEEE.

Modanlou, H. D. (2011). Historical evidence for the origin of teaching hospital, medical school and the rise of academic medicine. Journal of Perinatology, 31(4), 236-239. 44(1): 3-13, at p. 4.

Paller, Alan (2011). Testimony to the Nevada Technological Crime Advisory Board, December 16, 2011.

Parker, Donn B. (1998). Fighting Computer Crime. New York, NY: John Wiley & Sons. ISBN 0-471-16378-3.

Pender-Bey, George. "The Parkerian Hexad, the CIA Triad Model Expanded -- MSc thesis"

Pender-Bey, G. (2019). The parkerian hexad. Information Security Program at Lewis University.

Reid, R. C., & Gilbert, A. H. (2010, October). Using the Parkerian Hexad to introduce security in an information literacy class. In 2010 Information Security Curriculum Development Conference (pp. 45-47).

Reilly, R. F. (2016, April). Medical and surgical care during the American Civil War, 1861-1865. In Baylor University Medical Center Proceedings (Vol. 29, No. 2, pp. 138-142). Taylor & Francis.

Ruoslahti, H., Coburn, J., Trent, A., & Tikanmäki, I. (2022). Cyber Skills Gaps–A Systematic Review of the Academic Literature.

Schelling, Thomas C. (1960). The strategy of conflict (First ed.). Cambridge: Harvard University Press. ISBN 978-0-674-84031-7

Schneider, F. B. (2013). Cybersecurity education in universities. IEEE Security & Privacy, 11(4), 3-4. .

Shaw, J. (2022). Revisiting the Basic/Applied Science Distinction: The Significance of Urgent Science for Science Funding Policy. Journal for General Philosophy of Science, 1-23.

Shneiderman, B. (1998). Relate–Create–Donate: a teaching/learning philosophy for the cyber-generation. Computers & education, 31(1), 25-39.

Thomson, A. (1960). History and development of teaching hospitals in England. British Medical Journal, 2(5201), 749.

Topham, L., Kifayat, K., Younis, Y. A., Shi, Q., & Askwith, B. (2016). Cyber security teaching and learning laboratories: A survey. Information & Security, 35(1), 51.

TX-DIR Texas Dept. of Information Resources https://www.youtube.com/watch?v=YFRK_sImKkQ

Vogel, R. (2016). Closing the cybersecurity skills gap. Salus Journal, 4(2), 32-46.

Ukwandu, E., Farah, M. A. B., Hindy, H., Brosset, D., Kavallieros, D., Atkinson, R., ... & Bellekens, X. (2020). A review of cyber-ranges and test-beds: Current and future trends. Sensors, 20(24), 7148.

UWM - Univ. of Wisconsin, Madison (1965) https://research.cs.wisc.edu/includes/textfiles/phds.65-70.txt

Zeckhauser, R. (1989). Distinguished Fellow: Reflections of Thomas Schelling. Journal of Economic Perspectives, 3(2), 153-164.