2019

Implementing Cybersecurity into the Wisconsin K-12 Classroom

Dennis Brylow
Marquette University, dennis.brylow@marquette.edu

Justin Wang
Marquette University

Debbie Perouli
Marquette University, despoina.perouli@marquette.edu

2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), (2019) : 312-317. DOI.

Implementing Cybersecurity into the Wisconsin K-12 Classroom

Justin Wang
Mathematics, Statistics and Computer Sciences Department, Marquette University, Milwaukee, WI
Dennis Brylow
Mathematics, Statistics and Computer Sciences Department, Marquette University, Milwaukee, WI
Debbie Perouli
Mathematics, Statistics and Computer Sciences Department, Marquette University, Milwaukee, WI

Abstract:

Cybersecurity is a field that has seen its workforce demands rising steadily throughout the past decade. Although the Wisconsin Department of Administration has been actively encouraging collaboration efforts between the public and private sectors and promoting cybersecurity as a promising career path, the demand for cybersecurity professionals continues to be greater than the supply, which is a trend noticed also nationwide. The state of Wisconsin is facing several challenges in attempting to promote cybersecurity including limited security curricula resources, lack of programs and other initiatives that promote security principles, and lack of awareness of cybersecurity risks. In this paper, we discuss the

major challenges Wisconsin is facing towards establishing proper cyber hygiene for the general population and growing the cybersecurity work force. In addition, we suggest ways to overcome or lessen the effect of the identified issues.

SECTION I. Introduction

Cybersecurity is a young field that has received public attention and become highly valued by organization executives in recent years. In the wake of cybersecurity breaches and attacks on Fortune 500 companies and popular websites, cybersecurity related roles have had high demand throughout the past decade. Even though the demand for cybersecurity specialists continues to rise, there appears to be a supply shortage of cybersecurity professionals across the United States. For example, the state of Wisconsin thrives in the manufacturing, food processing, health and utility industries. Based on the Verizon Data Breach Report [1], these industries suffered from 653 cyber incidents nationwide in the fiscal year of 2017 alone (utilities: 22, manufacturing: 389, healthcare: 242).

Cyberseek is a collaborative initiative between the National Initiative for Cybersecurity Education (NICE), Burning Glass Technologies and CompTIA. The interactive website provides detailed and actionable data on the cybersecurity job market across the United States. According to the website "heatmap", 72% of the states within the U.S. have more than 1300 cybersecurity related role openings as of the end of March, 2019.

The National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) are involved in the development of cybersecurity related standards [2]. NICE, a division of NIST, has published the NICE Cybersecurity Workforce Framework (NCWF). They have also taken the initiative to host educational camps on cybersecurity across many states in hopes of raising cybersecurity awareness and promote cybersecurity as a promising career path. The National Science Foundation (NSF) CyberCorps is a program offering scholarships for service to students studying in preselected university programs. In addition, the Department of Homeland Security (DHS) jointly with NSA have established designations for two-year colleges and four-year universities as National Centers of Academic Excellence (CAE). If such an institution satisfies rigorous requirements, it can earn the CAE designation with a focus on Education, Security or Cyber Operations. As of 2019, there are about 260 such designated institutions throughout the United States.

Currently only five institutions that offer cybersecurity programs are accredited by the Accreditation Board for Engineering and Technology (ABET): the U.S Naval Academy, U.S. Air Force Academy, Towson University, Southeast Missouri State University, and University of Central Missouri. The Joint Task Force on Cybersecurity Education, which is a collaboration among the Association for Computing Machinery (ACM), the IEEE Computer Society (IEEE CS), the Association for Information Systems Special Interest Group on Security (AIS SIGSEC), and the International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8), launched the 2017 Cyber-security Curricular Guideline that attempts to define the field of cybersecurity and list the requirements for a major in this field. However, currently higher education institutions often categorize cybersecurity as a concentrated discipline under computer science or information technology and offer elective topics courses to their students.

Despite the efforts undertaken at a national level, most of the initiatives have not yet affected the primary and secondary school (grades "K-12") environment. In this paper, we explore the challenges that are preventing local government agencies from raising cybersecurity awareness and we provide potential solutions to address the identified issues. In addition, we discuss current practices and efforts that are sponsored by the government to spark students' interest in cybersecurity practices and exercises in hopes of addressing the global issues of defending the cyberspace and closing out the skill gap that is ever-increasing throughout the past decade. We finally encourage and identify opportunities for all residents to get educated on privacy and security.

SECTION II. Current Challenges

Multiple factors have contributed to the formation of the workforce gap that we have observed during the last decade. In this Section, we list contributing factors: limited security curricula content in K-12 classrooms, lack of effective training methods for teachers, lack of programs or other initiatives that promote cybersecurity principles in the state of Wisconsin, and lack of cyber risk awareness among residents. We also discuss the consequences of each of these factors.

A. Limited Security Curricula Content and Educator Skills

The Wisconsin Standards for Computer Science were approved by the state Department of Public Instruction in June of 2017 [3]. The development committee explicitly included cybersecurity related topics throughout the K-12 grades. However, the current adoption rate of this framework is low in the state of Wisconsin. As a "local control" state, it falls to each of the 446 individual public school districts to act on academic standards approved by the state. As a new academic standards area, many school districts have struggled to understand this unfamiliar content, or to find qualified teachers that can teach computer science. Recent pushes by the PUMP-CS Project [4] have used funding from the National Science Foundation and national non-profit Code.org to drive up the number of well-prepared K-12 computer science teachers, including professional development for Computer Science Fundamentals (CSF) [5] for K-5 students, Project GUTS [6] and Computer Science Discoveries (CSD) [7] for middle grades, and Exploring Computer Science (ECS) [8] and Computer Science Principles (CSP) [9] for high school students. Despite rapid strides that have more than doubled the number of CS teachers in the state in the past five years, more than 80% of public schools still lack any identified computer science teachers or coursework.

Where computer science curriculum is present, there are frequently elements of cybersecurity also in evidence. For example, in the CSF curricula [5], one of the courses designed for first graders enables the students to learn about their digital footprints and how to stay safe when visiting websites. Students who are in third grade learn what information is appropriate to share online and what should stay confidential in the digital citizenship course. The CSP course [9], which is designed for high school students, contains lesson plans oriented around the concept of encryption to provide the students the opportunity to explore practical measures to encrypt sensitive information.

While some cybersecurity concepts such as the CIA triad (Confidentiality, Integrity, Availability) can be more easily understood, techniques such as address resolution protocol (ARP) poisoning, domain name service (DNS) spoofing, social engineering, and malware analysis are more technical and best understood through practice and demonstrations. K-12 schools do not typically have the resources and expertise required to educate students through live demonstrations.

More than 2,000 Wisconsin school teachers have participated in some level of computer science professional development with Marquette University in the past five years. However, organized efforts to raise awareness and train teachers on cybersecurity are sporadic. There are several websites and tutorials that provide security training such as Pluralsight, Cybrary or even YouTube, but those tutorials are often not well organized or are subscription-based. Teachers should be supported in order to dedicate time and effort into cybersecu-rity training. In addition, considering that Cybersecurity is a relatively new discipline, and that it consists of a wide range of topics, the shortage of professionals interested in hosting such technical summer camp for teachers is an additional challenge.

B. Lack of Awareness from Non-Technical Residents

Technological advancements are progressing with speeds that are too rapid for most consumers to be able to follow. In-ternet connectivity is increasing and many aspects of our lives now involve cyber infrastructure: from

grocery shopping to managing the brightness of light bulbs and the temperature of thermostats at home. The habitual reliance of people on online connectivity has increased our vulnerability to cybersecurity risk, since more consumers have not had the time to educate themselves on the risks of new technologies. Not many realize that a connected device can become a relay sending unwanted traffic to a specific destination or be at the receiving end of unwanted traffic that could paralyze an Internet of Things (IoT) device. This lack of awareness impacts the propagation of knowledge into the younger generations, since older adults are not able to advise and train their children.

C. Limited Collaborative Efforts

Several organizations in the private sector have allocated resources in an effort to train their employees on cyberse-curity. For instance, in response to the breaches that took place in 2014, JPMorgan Chase indicated that they intend to spend 250 million on digital security annually [10]. In the state of Wisconsin, Northwestern Mutual (NM) has openly expressed interest in promoting security and information risk management. NM has been actively cultivating local talent through the STEM outreach program. In December of 2017, they invited local high school students to participate in a risk management and security topic-based capture the flag game for students to demonstrate their capabilities to function in teams and solve security related challenges in a competitive environment under limited time [11]. Nevertheless, the overall collaboration across Wisconsin is still considerably limited.

SECTION III. Current Efforts and Resources

While there exist several challenges that are preventing the cybersecurity workforce from growing systematically and consistently in Wisconsin, government agencies and other organizations do offer some resources that enable the students to get exposed to cybersecurity concepts and principles at a young age. We discuss those resources that are available to school districts across the state of Wisconsin.

A. AFA CyberPatriot

CyberPatriot is the National Youth Cyber Education (NYCE) program created by the Air Force Association (AFA) to inspire K-12 students towards careers in cybersecurity or other science, technology, engineering, mathematics majors that are critical to the nation’s future. The CyberPatriot program primarily targets middle and high school students and presents them a ten-unit curriculum aimed to educate the students on concepts such as cyber ethics, online safety, computer security and file protection. The students are also eligible to participate in team competitions that test the students’ ability to identify Windows and Linux system vulnerabilities and fix them. In addition, they are also presented with tasks related to virtual networking. The difficulty of the challenges presented in the competitions increases as the participants advance further into the competition [12] In the 2019 school year, Wisconsin is represented by 52 teams of various skill levels.

B. GenCyber Summer Camps

GenCyber is a summer camp program sponsored by both the National Science Foundation (NSF) and the National Security Agency (NSA). The acronym stands for "Inspiring the Next Generation of Cyber Stars" and the program provides a summer cybersecurity camp experience for students and teachers at the K-12 level. The goal of the program is to increase interest in cybersecurity careers and diversity in the cybersecurity workforce of the nation. This is one of the government’s proposed solutions in addressing the shortage in skilled cybersecurity professionals. This summer camp is open to all students and teachers at no cost. Wisconsin was one of the last handful of states to participate in GenCyber. The first camp was hosted in the summer of 2017 by the University of Wisconsin Green Bay. In the summer of 2018, two additional GenCyber camps were hosted at Marquette University and the Waukesha Country Technical College (WCTC). At the time of writing, the 2019 camps had not yet been publicly announced [13].

C. Private Sector Training

The Infosec Institute, which is headquartered in Madison, Wisconsin, was founded in 1998 by information security instructors that built a business offering top tier quality training experience to their students [14]. Although the service is not free, this resource provides the means to individuals wishing to receive professional security training from instructor led courses and assistance on the preparation of their professional certification examinations through online test banks and exercises. There are also other Wisconsin based companies offering cybersecurity training to another organization's employees (e.g. Barracuda PhishLine).

D. Nationwide Resources

The OWASP Foundation is a non-for-profit organization dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted. The foundation provides tools, documents and chapters that are free to anyone interested in improving application security. OWASP also maintains an open-source web application challenge-based learning (CBL) tool named OWASP Juice-Shop [15] that was built intentionally vulnerable to the top ten most common vulnerabilities within web applications as identified by OWASP.

CyberStart is a suite of challenges, tools and games designed by the Sans Institute to introduce young people to the field of cyber security. The Department of Administration in Wisconsin is currently collaborating with Sans on identifying students who may be interested in cybersecurity through the invitation of students to participate in the shortened version of the CyberStart challenges and solve problems in the topics of open source intelligence, cryptography, web application exploits, forensics, binary attacks, and Linux related challenges [16] [17].

The Open Cyber Challenge Platform (OCCP) is a free, configurable open source virtualization platform for cyberse-curity educators. It is designed to provide a controlled scenario in cybersecurity areas including network defense, penetration testing, incident response, malware analysis, digital forensics, and secure programming [18].

TeachCyber [19] is a website that provides free lesson plans and hands on practice materials on foundational computer science and cybersecurity skill curricula organized by grade levels based off the national K-12 Computer Science Framework in response to the rising of the need for security. Similarly, C5 Colleges (Catalyzing Computing and Cyberse-curity in Community Colleges) focuses on raising awareness for students that attend community colleges. This NSF funded project provides free modules that are in alignment with the ACM Computer Science Curricular guidelines. Topics include applied cryptography, secure scripting, cyber threats and countermeasures, cybersecurity principles and responsible software development. Clark Center is a more recent open source library funded by the NSA to advance the state of cybersecurity. The contents on this library feature cybersecurity and data science curricular modules that are freely available. Instructors can also upload content and course manuals for other teachers to use. Contents on this library are typically reviewed by either the C5 or by the National Cybersecurity Curriculum Program [20].

Slightly more advanced are the following three hands-on resources. The SEED Labs [21], designed and developed by Dr. Wenliang Du at Syracuse University under an NSF grant, contain a variety of guided exercises on numerous cyberse-curity topics. The Naval Postgraduate School has developed Labtainers, more than 40 exercises and tools to build more. It has also developed CyberCIEGE, which is an educational video game. [22].

Lastly, the National Initiative of Cybersecurity Education (NICE), led by the National Institute of Standards and Technology (NIST), is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development. NICE has been hosting the NICE National K-12 Cybersecurity Education Conferences, an effort initiated in 2015.

SECTION IV. Potential Solutions

Based on resources that are currently freely available, we have identified components, which are crucial to the success of establishing a sustainable and consistent pipeline that will enable students to get exposed to the field of cybersecurity. With the idea that both the citizens and the government each have their due diligence to ensure the success of the proposed solution, we propose solutions that correspond to the cybersecurity challenges faced in Wisconsin in particular.

A. Incorporate CS Standards into the Existing K-12 Curricula

K-12 schools in Wisconsin need to more rapidly adopt the already established computer science standards. For example, in the framework under the NI.1 standard, ("Students will understand the importance of security when using technology") [3], learning priority NI.1.A states that students in the K-2 grade band are instructed on how to use secure practices, such as passwords, to protect private information. Students between the grades 3-8 are supposed to be instructed on the development of strong passwords and analyze the risks associated with the usage of weak passwords. Further, under learning priority NI.2.A, students begin their exploration of how packets are sent and travel through the network, which is one of the key points that will help them understand how malicious users implement network-based attacks. Additional cybersecurity concepts such as the CIA triad, exploration of security policies, encryption practices and brief discussions on ethics associated with hacking are all included within the computer science standards for students throughout the K-12 grade bands to explore and learn.

It is critical for the state to further promote the benefits of the computer science standards as well as to encourage and equip school districts to adopt specific curricula that meet the standards. The information could help students to understand risks within cyberspace, and to learn more about security related knowledge progressively over the entire K-12 sequence. Apart from making children aware of the cyber-security risks and helping them to understand procedures to protect themselves and their personal identifiable data, this exposure will also enable them to pursue a career in that field. In addition to the contents covered within the computer science standard, motivated teachers can incorporate additional concepts such as counter measures against trojan viruses, phishing and ransomware to help the students understand how to properly prevent themselves from becoming the victims of such threats.

B. Focused Professional Development

State-promulgated academic standards are a foundational piece required to promote broad acceptance of computer science content in general, and cybersecurity concepts in particular. Wisconsin is only the ninth state to adopt model computer science academic standards for K-12, and the final version includes enhanced cybersecurity content above and beyond what was recommended by the computer science teachers association (CSTA) K-12 standards. However, in the absence of effective professional development for teachers, standards documents alone are unlikely to directly impact students in the K-12 classroom. Teachers in practice function as the first line of defense if information security contents are to be integrated into the curriculum. Adequate access to content training and support tools will help prepare them to respond to any potential issues or questions that the students may be having. While in many content areas it is supposed that a little exposure is better than none at all, cybersecurity is one domain in which poorly developed training or poorly executed curriculum could actually cause more harm than good.

We understand that most teachers have ample issues to deal with already; therefore we propose that an educational curricula be created to provide the teachers access to carefully vetted training materials. Marquette plans to host quarterly workshops to inform, update and educate participants on new security knowledge and concepts. More importantly, our workshops will allocate time for teachers to incorporate the newly adopted content into their existing curricula for conveying this complex information to their students. Prior experience in

a similar context has shown that this shared lesson planning and content assimilation time is an essential factor in effective classroom transfer [23]. Furthermore, our team has deep experience launching other computer science curricula in scores of school districts across the state.

C. Cybersecurity Exercise Testbed

In response to the ideas mentioned in the previous subsection, we further propose the development and construction of a cybersecurity exercise testbed that can be utilized by the teachers to better carry out live demonstrations for the students without having to worry about the configuration and set up of both the hardware and software components. The tasks and exercises within the cybersecurity exercises testbed will adhere to the performance indicators as described in the computer science standards and the terms and instructions will also be designed around their grade band to ensure they are age appropriate and won't pose challenges for the students to understand the task at hand. Each exercise topic will include instruction for teachers and a step-by-step user operation manual for the students as they operate and obtain hands-on experiences with these topics.

The benefits of this proposed solution include: all operations are conducted in a sandbox contained environment where students will not be able to extract files from the test bed environment (their handcrafted trojan files for instance); the software packages needed for exercises will be pre-installed, which helps to prevent them from installing powerful tools onto their own computer and utilizing those tools to cause harm to their peers that may not be aware of their newly obtained skills. Further, it will not only provide the teachers the instructions they need to guide the students through the exercises, but it will also provide teachers and students with both offensive security and defensive security experiences to ensure both the students and the teachers are aware of countermeasures that can be utilized when they suspect that they are under attack.

D. Cyber Sessions for Older Adults

Cybersecurity and cyber risks may be unfamiliar terms for many older adults. Although their Internet presence may be limited to basic email exchanges and web browsing, older adults are prone to cyberattacks due to the lack of relevant knowledge. To help raise cybersecurity awareness around all population groups, we propose the development of information sessions or bootcamps that target various age groups to spread cybersecurity knowledge. It is important for educators to rec-ognize that information sessions need to vary both in content and in pedagogy based on the audience age and cybersecurity knowledge. The development of organized training efforts specifically targeting the older adults are of high significance as it helps prevent cyber criminals from abusing the personal identifiable data that they may have obtained from these individuals through email phishing attacks and click-baits.

E. Workshops for Students

Efforts such as classes, bootcamps, summer camps and competitions are fairly limited in Wisconsin, but efforts such as GenCyber are gradually providing the students who may be interested in security to have the opportunity to learn. We propose that the number of summer camps that focus on security topics should gradually increase. One way to accomplish that is by having teachers host summer camps based on the concepts included in the computer science standards. The additional hours teachers spend will not only enable the teachers to become more familiar with the contents but also help to broaden the coverage on cybersecurity awareness across the state. As a result, such effort will certainly lead to great improvements in terms of the increase in cybersecurity awareness for the youth and their households.

F. Professionally Certified Training Bootcamps

Another solution that could help address the security expert shortage that we currently face is to collaborate with local corporations. Corporations need security experts to help secure their commercialized products. This

collaborative effort between the organizations and the community would enable the local corporations and organizations to identify talent through the offering of professional instructor led training in the form of a bootcamp. At the conclusion of the boot-camp, the organization may provide the fitting participants with attractive initiatives such as part-time or full-time career opportunities, training plan vouchers or reimbursement of the participant's first attempt on a professional certification exam. The establishment of this collaborative effort will help encourage the local students and security hobbyists within the community to consider turning cybersecurity into a career and thus indirectly address the security expert shortage issue for both the sponsoring corporation and the state of Wisconsin.

G. Build Your Own Lab Environment for Experiments

In the current digitally dominant world, much information and demonstration videos can be found online, although the information may not be well structured. We propose providing workshop consultations to help individuals interested in learning more about security to build their own isolated virtualized environment for experimentation of various toolkits. While creating a virtualized environment is not too challenging, knowing what to install and learning how to use some of the security toolkits that are available may not necessarily be easy. As a result, we propose the establishment of a security workshop that focuses on helping interested individuals not only build their own experimental security laboratory with various operating systems installed, but also provide them with lists of resources that would enable them to learn more about the proper toolkits they need, such as nmap for port scanning, Armitage or Metasploit for system exploitation and John The Ripper or Hydra for password brute-force cracking. By having a laboratory of their own and a recommended list of tools to use, the individual would now be able to experiment with security tools and perhaps launch an attack against other systems that are located on the isolated virtual network within the laboratory to gain more exposure and experience through these hands-on exercises at home.

H. Expand Challenge Based Learning Environments

Challenge-based learning is a learning methodology that is specifically applicable to learning security principles. In this competitive learning method, participants attempt to solve as many challenges of various topics as they can within a time frame. Those challenges include cryptography, reverse engineering, web exploitations, forensics, binary exploitations and general computing skills. Research studies [24] have shown that the CBL environment encourages students to collaborate and operate cohesively together as a team, understand security concepts through hands on practice, and help students identify their knowledge gaps through the participation of timed capture the flag competitions. In addition, research work also demonstrates that most participants generally feel more confident handling security issues and or instructing others on security topics after they have gone through a cycle of challenge-based learning [24]. Therefore, for individuals who may be interested in becoming security experts, challenge-based learning is an appropriate starting point. There are many "capture the flag" (challenged-based learning) events that takes place year-round for participants of all age groups nationwide. If the development of a challenge-based learning platform is too difficult, engaging in the CTFs that are freely available online is also a good alternative for individuals who wish to learn more about cybersecurity. For the above reasons, we recommended the department of administration in the state of the Wisconsin to develop a systematic challenge-based learning platform that enables students of all age groups interested in learning more about cybersecurity to participate in the program. This will ensure satisfactory coverage in the effort to raise cyber-security awareness across the state and help students who may be interested in a career in cybersecurity receive proper training and experience before they graduate from high school or college.

SECTION V. Conclusion

This paper has described some of the challenges that Wisconsin has been facing that prevent the cybersecurity workforce from successfully expanding. By identifying the challenges and potential resources that are available, we identify the need to create a cyber security curriculum that is all age appropriate for students and teachers in Wisconsin. We propose the creation of a tool that enables the students to learn more about cybersecurity through the challenge-based learning methodology. Further, since the teachers within the K-12 school systems are critical in the success of a more cyber aware population here in Wisconsin, they need to be enabled to provide students with enough knowledge and skills so that students can establish proper cybersecurity practices. We finally outline ways though which older adults can be encouraged to get educated on matters of privacy and security.

ACKNOWLEDGMENT:

This research was motivated by the speech given by David Cagigal, during the Cyberstart event that took place at Marquette University. We appreciate all that he has done to promote Cybersecurity awareness across Wisconsin.

References

1. Verizon, "2017 Data Breach Investigations Report", [online] Available: https://enterprise.verizon.com/resources/reports/dbir/.
2. E. A. Fischer, "Cybersecurity issues and challenges: in brief", *Congressional Research Service Report prepared for Members and Committees of Congress*, 2014.
3. "Wisconsin standards for computer science", [online] Available: https://dpi.wi.gov/sites/default/files/imce/computer-science/ComputerScienceStandardsFINALADOPTED.pdf.
4. "Preparing the upper midwest for principles of computer science", [online] Available: http://pumpcs.mu.edu/.
5. "Computer science fundamentals", [online] Available: https://code.org/educate/curriculum/elementary-school.
6. S. F. Institute, "Project GUTS: Growing up thinking scientifically", [online] Available: http://www.projectguts.org/.
7. "Computer science discoveries", [online] Available: https://code.org/educate/curriculum/middle-school.
8. J. Goode and G. Chapman, "Exploring computer science", [online] Available: http://www.exploringcs.org/.
9. "Computer science principles", [online] Available: https://code.org/educate/csp.
10. J. Silver-Greenberg, M. Goldstein and N. Perlroth, "JP Morgan Chase hack affects 76 million households", [online] Available: https://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/.
11. K. Kuhn, "Northwestern Mutual Encourages Students to Explore Careers in IT", [online] Available: www.unitedwaygmwc.org/Speak-United-Blog/Northwestern-Mutual-Encourages-Students-to-Explore-Careers-in-IT.
12. "Cyber patriot", [online] Available: http://www.uscyberpatriot.org.
13. "Gencyber", [online] Available: https://www.gen-cyber.com/about/.
14. "Infosec institute", [online] Available: www.infosecinstitute.com/company.
15. "Open web application security project", [online] Available: http://www.owasp.org.
16. "SANs CyberStart", [online] Available: https://www.sans.org/CyberStartUS.
17. "Cyber education wisconsin", [online] Available: https://cyberedu.wi.gov/Home/ CyberResources.

18. "Open cyber challenge platform", [online] Available: https://opencyberchallenge.net.
19. "Teach cyber", [online] Available: http://teachcyber.org/about.
20. "Cybersecuriy library: Clark", [online] Available: https://www.clark.center/home.
21. W. Du, "Hands-on labs for security education", [online] Available: http://www.cis.syr.edu/~wedu/seed/.
22. M. Thompson and D. C. Irvine, "Active learning with the cyberciege video game", *Proceedings of the 4th conference on Cyber security experimentation and test*, 2011.
23. H. Bort and D. Brylow, "Cs4impact: Measuring computational thinking concepts present in cs4hs participant lesson plans", *Proceeding of the 44th ACM Technical Symposium on Computer Science Education ser. SIGCSE '13*, pp. 427-432, 2013, [online] Available: http://doi.acm.org/10.1145/2445196.2445323.
24. R. S. Cheung, J. P. Cohen, H. Z. Lo and F. Elia, "Challenge based learning in cybersecurity education", *Proceedings of the International Conference on Security and Management (SAM). The Steering Committee of The World Congress in Computer Science*, pp. 1, 2011.