Educating the Masses: Cybersecurity for Everyone

Abstract

Cybersecurity is no longer just the concern of Information Technology (IT) teams. Emerging technologies like artificial intelligence and machine learning are changing the game for cybersecurity. To remain relevant and promote pedagogical framework, K-12 and institutions of higher education should continue to have conversations about cybersecurity education. As part of the paradigm shift cybersecurity education should be a priority. It is essential to equip administration, faculty, staff, and students with the advantages and disadvantages to ensure end users are not introducing a threat. Having a "cyber aware" student means they go home and into the 21st Century workforce exercising those same best practices. As the National Cybersecurity Alliance points out: "This is Shared Responsibility. We each have to work together to keep ourselves, families, schools, communities and our nation safe." The purpose of this paper is to communicate on the subject of cybersecurity – across all sectors of government; businesses, academic institutions, and individuals.

Keywords

Cybersecurity, Higher Education, Government, Business, Awareness, Home User, Curriculum, Individual

1. Introduction

Cybersecurity education has become increasingly important, as cybersecurity integrates into all aspects of daily life. As individuals think back to their daily habits 15 years ago versus their daily habits today, a smartphone or even a social media profile was not part of those habits. The custom was the sound of dial-up and having to manually connect to the Internet. There has been a movement from the introduction of Facebook in 2004 to the launch of Apple iPhone in 2007 and currently the adoption of the cloud to store documents, photos and music. These tech innovations have changed people's lives and daily routine, as well as the course of modern history. The advancement of innovation is not slowing down, and neither is the increase growth of new technology. From connected watches to connected homes, things people never imagined have become essentials in their daily lives. These changes in human behavior that has been triggered by the adoption of tech innovation have consequences of living a connected life.

The future of cybersecurity in light of tech innovation creates an increase in stolen credentials, massive data breaches, ransomware and other malicious cyberattacks driven by increasingly sophisticated cybercriminals. The unprecedented threats for both consumers and businesses open up a new range of cybersecurity and privacy risks. Institutions of higher education are prime attractive targets for cybercriminals for two reasons [1]. First, colleges and universities are responsible for a variety of sensitive and lucrative data, including social security numbers, medical records, financial information, intellectual property, and cutting-edge research. Second, higher education's open access culture, decentralized department or unit-level control, as well as federated access to data and information makes it a particularly vulnerable target for unauthorized access, unsafe Internet usage, and malware [1]. To remain competitive, organizations should be prepared to invest in several different types of cybersecurity and privacy education, training, and awareness programs. Higher education institutions should promote improved awareness and new knowledge insight in an effort to achieve the goal of robust cybersecurity defense.

2. Elevate Cybersecurity to the Executive Agenda

Due to the demands on higher education president's time, cyber discussions are often sidelined by more familiar and seemingly significant matters. The majority of college and university presidents and chancellors have limited exposure to and fluency in cyber issues and their potential business impact on an institution. Some Board of Trustees may or may not bring relevant experience and fluency on cyber issues to their respective institutions. Many times, it takes a major breach to escalate cybersecurity matters to the executive and board level agenda. There is often an important disconnect between senior leadership an institution of higher education highest ranking IT staff. Most of the highest-ranking IT official do not have the ear of leadership. According to EDUCAUSE, only 56% of the higher education institutions surveyed have a chief information officer (CIO) or equivalent role that is part of the president's cabinet [2]. The EDUCASE higher education IT workforce study found that CIOs who served on the cabinet are significantly more likely to discuss the IT implications of institutional decisions with campus executives [4]. Often this means that important conversations about cybersecurity don't make it beyond an institution's IT department.

2.1 More CIOs to be Members of the President Cabinet

Georgia State University's (GSU's) chief innovation officer Phil Ventimiglia explains, "If you really believe in cybersecurity and the importance of technology to the operation and future of the campus, then the CIO or whatever role is leading technology for the institution should be at the cabinet level [3]." It is not imperative that the CIO report to the president but having a seat at the senior leadership table to elevate the discussion around these risks is important. It is essential that the CIOs bring strategic IT issues that builds a more resilient institution that is capable of bouncing back from cyber events quickly, recognizing that is no longer a matter of if they will occur, but when [4]. The relationship between the president and the CIO serve as "a way to keep the lines of communication open, so when matters like denial of service attack or highly disruptive situations occur the foundation does not have to be build. It is already in place and just a matter of zeroing in on a particular direction," says Rutgers University's senior vice president and CIO Michele Norin. As GSU president Mark Becker explains, "The chief information officer (or equivalent) has to be at a high level in the organization; they cannot be buried away from the president. At Georgia State, they report directly to me and sit on my cabinet, as well as on the administrative council [which allows us]to have direct conversations. Our offices are on the same floor [5]." A security mindset is created that facilitates greater understanding of the cybersecurity issues facing the institution.

American University's (AU) president emeritus Neil Kerwin recounts, "With a seat on the cabinet the vice president of information technology educates colleagues on the senior management team and is educated by them. That works its way ultimately up to the board of trustees, which now has a fixed expectation of IT being an agenda item for every board meeting [5]." Dave Swatrz, AU's vice president and CIO observes, "At most universities, what CIOs struggle with is having the authority to be able to put in place the controls that are needed to be sure that risks are mitigated [5]." The results of AU's change in organizational structure was "better alignment between responsibility and authority and accountability [5]."

The conversation around cybersecurity should be in regards of enterprise risk management with the presidents and boards of trustees, with the business impact to the institution clearly defined. GSU has put in place a cybersecurity charter to communicate to the institution that cybersecurity is not an IT domain but rather an enterprise risk. "In today's world, where information storage and processes like monetary transactions are increasingly carried out digitally, we all see instances in the news where unauthorized data access has put large numbers of people's personal information at risk [5]." Security practices are vital to protecting students, faculty, and staff, as well as all those who conduct business and research in partnership with the university," explains Ren Flot, GSU chief information security officer and director of cybersecurity services. Presidents of institutions of higher education should want to know where the greatest vulnerabilities are and what can be done to minimize those in a cost-efficient manner. As GSU's Ventimiglia observes, "We are in a day and age that if a network goes down for an hour, we cannot teach [6]."

3. The Weakest Link: Humans

Cybersecurity is not just about protecting organizational assets, corporate networks and technological defenses. It is also about people using a variety of devices every day. Everyone needs a basic understanding of cybersecurity and how to recognize cyber threats. The weakest link is often people. McAfee's 2016 Threats Predictions report notes that "within the next five years, the volume and types of personal information gathered and stored will grow from a person's name, address, phone number, email address, and some purchasing history to include frequently visited locations, 'normal' behaviors, what we eat, watch, and listen to, our weight, blood pressure, prescriptions, sleeping habits, daily schedule, and exercise routine [7]. With homeowner's unprepared and unequipped to notice and correct most security threats, some highly successful attacks will collect personal information on a continuing basis [7]. The Internet has allowed exclusively business models that have already formed our planet. The Amazons, Facebooks, and Goggles of this world is not the most profitable organization that conduct business over the Internet today – that recognition belongs to cybercrime. The most lucrative business on the Internet today speaks volume – Fraud [8].

Cyber fraud often makes headline news, but it is thought that the number of cases of fraud detected and prosecuted is just the tip of the iceberg. Internet fraud is a form of white-collar crime whose growth may be as rapid and diverse as the growth of the internet itself [8]. All the major financial institutions throughout the world, uses computers to carry out their business and huge sums of money are transferred through computers (electronic funds transfer). Fraud on the internet constitutes about one-third of all cybercrimes [8]. Internet fraud has increased by a substantial percentage over the past years. [8] It is the most profitable business on the internet. Online fraud, today, poses a major threat to the continued popularity of e-commerce [8].

The cybersecurity and privacy threat is real for the average every day person, for the financial sector, government, military, public safety, and critical infrastructure [9]. Due to a lack of knowledge, skills, or abilities the average person engaging in online behavior at home poses a cybersecurity risk. It is essential that we educate, train, and develop cybersecurity professionals to help protect our nation and our people. There should be opportunities for professional development that assist faculty with developing effective programs [10] or developing forums in which curriculum ideas can be exchanged [11]. However, the focus has too often been exclusively on this component rather than educating the masses on what they can do to protect themselves from various cybersecurity and privacy threats they encounter every day [12].

While the focus has remained mostly on cybersecurity professionals and organizational users, there is some evidence that the need for a broader cyber security education is being recognized. The development of awareness programs and some type of enforcement mechanism for home users via their Internet Service Providers (ISPs) could be implemented [13]. When the society at large is educated in cybersecurity and privacy, there is less problems for organizations as non-malicious insiders. There is no substitute for promoting awareness for all users in how to protect their network from malware, botnets, and other advanced threats. The war against cybercriminals is fought each time a user decides to click an unfamiliar link or open an attachment- just a single mistake could be the reason for massive data loss.

3.1 Home Users

A home user is defined as a citizen with varying age and technical knowledge who uses Information Communication Technologies (ITCs) for personal use anywhere outside their work environment [13]. A home user is someone who accesses the Internet from a personal computer at home, and who is self-responsible to secure that computer in terms of malware, updates, patches etc. [13]. Home users are vulnerable due to many reasons. One of the most significant ones is the fact that such home users are in many cases not even aware of the risks of using the Internet, and are increasingly exposed to security threat while using their PC systems. The home users do not have the information security knowledge to understand and protect their PC and without the awareness this causes their personal information to be exposed.

Accessing the Internet for social networking, emails, and Internet banking and shopping can be a big problem that in many cases for such home users are not cybersecurity aware, and are therefore potentially exposing themselves in a large way. The majority of home users are likely to be vulnerable targets unless safeguards are automatically provided for them [14]. If home users lack the proper information security awareness knowledge, they will also not understand and/or be aware of the cyber risks they are exposed to and that they are ultimately responsible for securing their own cyber environment [14].

One of the main reasons for this lack of cybersecurity is that there is no enforcement by a third party to ensure that home users are securely using the Internet or that their cybersecurity awareness is up to date. Although research had been done on making home users aware of the importance of securing their own information, the enforcement to do so does not usually exist [13]. Home users, therefore, in many cases venture onto the Internet without any idea of what the risks are and what they must do to protect themselves.

Home users should be information security aware as supported by the following statistics:

- Home users account for 95% of Internet attacks [15]
- Novice users are likely to face a range of Internet threats as their unfamiliarity with the technology can limit their ability to recognize the threats and understand the requisite protection [14]
- Three million computers have been infected with Koobface – a social networking site [16]
- Spam levels are expected to rise 30-40 percent in 2010 [16]
- One in every 600 PDF files download from the web contains malicious software [16]
- 23,500 infected websites are discovered every day. That is one every 3.6 seconds-four times worse than the same period in 2008 [17]
- 15 new bogus anti-virus vendor websites are discovered every day. This number has tripled, up from average of 5 during 2008 [17]
- 89.7% of all business email is spam [17]

3.2 Electronic Awareness and Enforcement Model

A methodology to consider is an E-Awareness and Enforcement model (EAAEM). I propose a strategy in which home users can be forced to become familiar with the risks involved in venturing into cyber space. The EAAEM model proposes a way to improve cybersecurity awareness for home users by presenting some cybersecurity content and enforcing the engagement of this content. The EAAEM will consist of two components: the awareness component housed in the online awareness portal and the enforcement component. The main function of the online awareness portal is to provide current content regarding cybersecurity risks within the home user environment. This component will address the cybersecurity awareness content. The goal is to introduce home users to best practices of cybersecurity issues such as what cybersecurity is, why it is important, and how to protect personal devices and network from unauthorized access or modification. It is essential to realize and understand that the home users who will utilize the portal have limited or no cybersecurity background. It is therefore important that the design and implementation of the portal is:

- easy to access
- user friendly
- interactivity
- integrated
- relevant content
- comprehensive
- adaptable to all devices

- knowledge based appropriate
- up to date

The online awareness portal should be scalable. A user should be able to start with an introductory module/unit regarding cybersecurity education and then move to an intermediate and then a more advanced module/unit. Goals and objectives will be clearly written in measurable outcomes. The content in the online awareness portal will be sequenced and structured in a manner that enables the user to achieve the stated goals. The content will be presented through a combination of concepts, activities, and emerging technologies. Multimedia will be used for the various users learning styles and accessibility will be considered and the transcript will be included. Microsoft translator will be used to break the language and communication barrier at home, at work, and anywhere it is needed. Microsoft Translator helps bridge communication gaps, supporting accessible learning with live captioning, and cross-language understanding. The content will be provided in chunks utilizing visual and auditory components. Each module/unit will have an assessment environment where the home user can be evaluated regarding the material of each module/unit. A glossary with various terminology will be included.

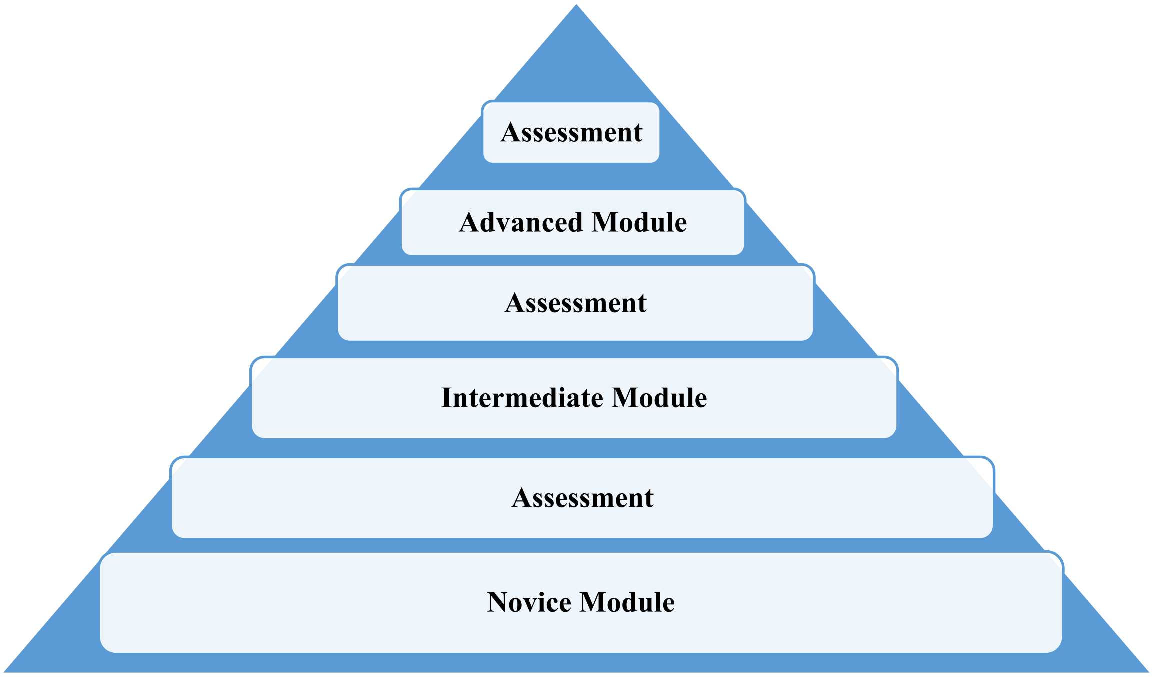


Figure 1: Layout of Online Awareness Portal

It is essential that the online awareness portal be regularly updated to keep track of new developments. It is important that the online awareness portal is designed and implemented for home users, accessible for home users, and ensures that home users are presented with all the cybersecurity knowledge to safely access the Internet. The other vital aspect is the online awareness portal is that it must be enforced.

The solution to the enforcement problem is to host the online awareness portal within regulating services, for example information service providers (ISPs) or financial institutions (FIs), since almost all users must gain access through these regulating services [13]. Such regulating services must then ensure that access to the Internet is only provided after passing via the awareness content part in the online awareness portal [13].

3.3 Regulating Services

The regulating services will represent the body through which the user can connect to the web [13]. The regulating services will provide the enforcement aspects [13]. The ISPs may reject this responsibility, there seems to be a growing international movement towards getting ISPs more involved. In 2008, The Controller of the Communications Authority in Zambia, urged ISPs to 'protect their customers from fraud and thefts that may arise as a result of sharing personal information online' [18]. Also, in 2008, the Council of Europe at its Strasbourg Conference in France, asked ISPs to help battle cybercrime [19].

In a BCS paper, it is stated that there has been '… increased calls for ISPs to play a more central role in detecting, monitoring and preventing illegal file sharing, in addition to their ongoing contribution to fight against other, perhaps more serious, criminal activities like online fraud, identity theft, phishing, terrorism and pedophilia' [20]. The Australian Government proposed measures to improve safety of the Internet for families. The proposal included 'mandatory ISP-level filtering' to be implemented by ISPs. 'These additional filtering services will help parents to choose what they want filtered without having to download and install software to their home computers' [21]. Therefore, the idea that ISPs can in the future get much more involved in providing cybersecurity and other types of services is definitely possible. The proposed E-Awareness and Enforcement Model could empower home users in regards to providing a better understanding of basic cybersecurity education, privacy, threats, and ways to avoid them. The proposed model can assist in home users being educated and learning cybersecurity tips.

4. Cybersecurity Curriculum Across all Disciplines

Most institutions of higher education emphasis on cybersecurity education only as part of the institution's computing or information security curricula. Cybersecurity focused degrees have become more popular in the past several years; however, there remains a lack of courses in cybersecurity for the non-major. While the focus has traditionally been on curriculum development for cybersecurity professionals, there has been increasing recognition that also need to educate everyone else [22]. If humans really are the weakest link within cybersecurity, then this gap within our education system must be addressed immediately [23].

Another approach that could be taken is to require all students to take an introductory cyber security course or a general information technology course as a general education course with a moderate focus on cybersecurity. This approach works well for some institutions, such as West Point, that have a structure and curriculum conducive to such an approach [22]. The considerable focus on technical majors and courses of study is likely to foster rather than hinder such courses, especially if they are required.

An all-inclusive cybersecurity course is multi-disciplinary by its very nature, and there are opportunities that can be attractive to other disciplines. For example, a course at one university introduces a multi-disciplinary approach to intelligence analysis [24]. Leveraging the social and behavioral sciences into our cyber security and privacy curriculum also makes a lot of sense since a large part of the problem is the human factor [25]. The needs for other approaches have also been acknowledged by the Department of Homeland Security and other entities [26].

The development and implementation of a course could serve as an elective for undergraduate students that fulfills a general education requirement. In most institutions of higher education across the country, general education is regarded as the foundation for preparing students for lifelong learning, for success in their chosen field, and for their eventual role as self-educated and knowledgeable citizens in society [27]. To function as digital citizen in modern society, students should have an understanding of the cyber infrastructure in which they live. They should be aware of security and privacy issues involving personal devices, online behaviors, social networking, gaming sites, and downloading information. A panel [28] commented, all users need to have some security knowledge, and addressing these concepts holistically, rather than focusing on stand-alone classes, is most effective.

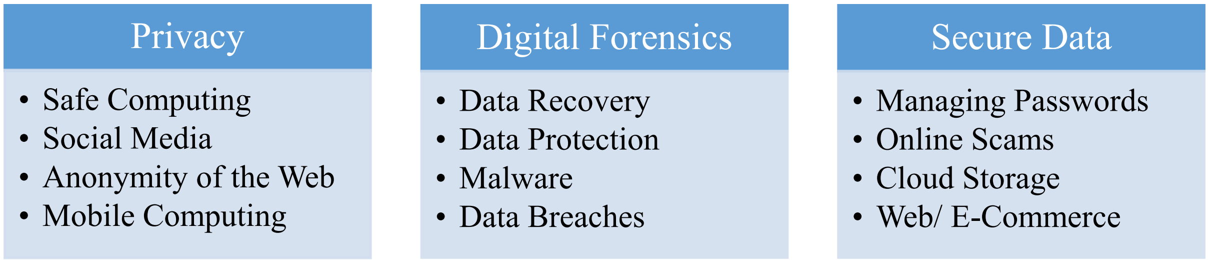
The new innovative approach to general education provides an ideal opportunity to educate all students not just computing majors. It is critical that all students receive education that deeps their conceptual and practical understanding of issues and awareness in cybersecurity. By offering a course of this type, students can learn how to better protect their information and improve their behavior from a cybersecurity and privacy standpoint. This approach can be particularly effective in bringing more women into the STEM majors since stereotype threat remains a very large impediment [29]. Divisions, departments, and schools could benefit by providing an important class that serves as a public good while helping fulfill a general education requirement. Society at large benefits by having more people educated in cybersecurity and privacy. These cyber aware learners are less likely to pose problems for organizations as non-malicious insiders, which present a security challenge due to curiosity, ignorance, and/or a lack of training and education [30]. In like manner, they are also less likely to have their computers serve as botnets that can be used to target any number of corporate, financial, governmental, or military targets [31]. Thus, having a course such as this is but one step that can be taken to make us all more secure. The goal is to increase cybersecurity awareness for everyone.

The USA recognizes education as a crucial component of its national cybersecurity readiness and has established legislation and strategies to develop cybersecurity education and a workforce. In some developing countries a cybersecurity curriculum for children based on videos are proposed in order to educate and help them protect their privacy on the Internet (e.g., social networks) [32]. In the UK, enhancing cybersecurity education and skills is one of the four main components of the national program [33]. There is a cybersecurity educational gaps in the South African national cybersecurity strategy based on a high-level comparison with USA and UK initiatives [34]. It is essential that students are cyber aware of how they engage with technology in their daily lives. The conversation needs to be part of the curriculum and how to stay secure online is as necessary as learning the days of the week, how to identify letters in the alphabet and their sounds, and recognizing numbers. Cybersecurity should be viewed as one of those essential skills that one needs to through today’s life.

Generation Z are those colloquially born after 1995 and are considered ‘digital natives,” having never known a time when they could not connect to the Internet. Most of the Generation Z have a high comfort level with technology, but there are areas where they are still naïve. Their skills might be strong in gaming and social media, but that does not mean they understand the risk that populate the online world. They are savvy about some things but naïve about other things. Few institutions of higher learning are focused on cyber at the undergraduate level, and even fewer schools in the K-12 sector are developing curriculum to initiative cyber awareness about the security risks of online behavior. We must start earlier, with five to 12 years old. There needs to be more discussion about how to education everyone around this area.

To provide the needed broad and deep understanding of cybersecurity for all undergraduate majors, the author proposes a strategy for developing cybersecurity knowledge and skills to prepare all students outside of computer science programs to enhance security across all disciples:

1. Develop course modules that can be embedded into existing general education courses. Modules are a common pedagogical tool for computing and cybersecurity topics, but are typically used in a single course or set of courses within computing disciplines [35-38]. Modules have also been used to embed security topic rapidly into an existing information assurance curriculum [39].



Privacy	Digital Forensics	Secure Data
• Safe Computing	• Data Recovery	• Managing Passwords
• Social Media	• Data Protection	• Online Scams
• Anonymity of the Web	• Malware	• Cloud Storage
• Mobile Computing	• Data Breaches	• Web/ E-Commerce

Figure 2: Suggested Topics

The topics in Figure 2 are suggested topics that can fulfil the goal of embedding cybersecurity awareness across the curriculum. These topics not only assist the student in learning about cybersecurity but they can take proactive measures on their own computers to become more secure. Students can understand operating systems, security software, file backup, home network configuration, Wi-Fi networks, password management, and social networking. Innovative lab assignments can consist of installing anti-malware, running a comprehensive scan on their own computer, installing software that automatically backs up their computer and allows them to recover previously deleted files. The lab experience and knowledge gain can be invaluable to the student in their daily lives when they pursue graduate school or join the workforce.

The ideas discussed in this paper are proposed to increase cybersecurity awareness for everyone and to develop material that is supportable and effective for everyone throughout the United States and beyond. The collaborations across disciplines with faculty could possible result in continuous improvement that lead to dividends in regards to faculty scholarship, including papers and grants, as well as multi-disciplinary students’ projects. When universities cover cybersecurity education across multiple domains, they are exploring how to address security issues at every level. Universities that develop and implement cyber classes into the curriculum whether it is psychology, education, or marketing are preparing students with a fundamental understanding of how security impacts business risk. The early stages of learning will create a comprehensive scope of individuals who are more empowered with knowledge of the ways cybersecurity impacts every aspect of government, business, academic institution and individual around the world.

5. Conclusion

Media have been observed in promotional photo for Instagram, Facebook CEO, Mark Zuckerberg with his laptop in the background sporting tape covering both the camera and the microphone – the implication being he does not trust his own machine is secure from cyberespionage [40]. If the CEO of one of the world's technology innovators can not necessarily trust his own computer, what does that mean? Helping ensure a secure and successful environment ultimately comes down to every government, business, academic institution and individual around the world. All three are the targets of cybercrime and any government department, corporate network, or the smartphone could be used as a vector for attack. It takes effort to identify and take action on a critical resolution in today's technologically savvy world. This effort is true in education and academia, the government, and private sector. The technology adoption rate exceeds the ability to predict the implications of the results of cybercrime. To create a growing cybersecurity ecosystem, there is a need to increase the skill shortage and promote STEM-based skillsets throughout the educational pathway. To assist in accomplishing this goal, institutions of higher learning should consider collaboration and partnership with enterprises to understand the learning curves around cybersecurity; consequently, the information can be shared about the threat landscape within all settings.

REFERENCES

[1] T.D. Fishman, C. Clark, and J.L. Grama. Elevating cybersecurity on the higher education leadership agenda, *Deloitte Insights*, (Feb 22, 2018).

[2] EDUCASE. The EDUCASE almanac for faculty and technology survey, (2017).

[3] J. Pomerantz and D.C. Brooks. The higher education IT workforce landscape, EDUCASE Center for Analysis and Research, (April 2016).

[4] EDUCASE. 2017 EDUCASE Core Data Service. (2017).

[5] EDUCASE Annual Conference 2017, The importance of cybersecurity governance: Perspectives from presidents, trustees, and IT leaders, (November 3, 2017).

[6] EDUCASE Annual Conference 2017, The important of cybersecurity governance, (November 3, 2017).

[7] 2016 Threats Predictions, McAfee Labs, 2016 www.mcafee.com/au/resources/reports/rp-threats-predictions-2016.pdf.

[8] S.K. Bajaj and A. Verma, "Cyber fraud: A digital crime," IADIS International Conference Information, (December 2008). Available: www.academia.edu/8353884/cyber_fraud_a_digital_crime.

[9] K. K. R. Choo, The cyber threat landscape: Challenges and future research directions. *Computers & Security*, vol. 30 no. 8, pp. 719–731, (August 2011).

[10] A. S. Namin, R. Hewett, and F. Inan, Faculty development programs on cybersecurity for community colleges: An experience and lessons learned report from a two-year education project. In *International Conference on Computer Science Education Innovation & Technology (CSEIT). Proceedings* pp. 19, Global Science and Technology Forum, (2015).

[11] D. Frincke, and M. Bishop, Joining the security education community. *IEEE Security & Privacy*, vol 5, pp. 61–63, (2004).

[12] F.B. Schneider, Cybersecurity education in universities. *IEEE Security & Privacy*, vol 4, pp.3- 4, (2013).

[13] E. Kritzinger, and S. H. von Solms, Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*, vol 29 no 8, pp. 840–847, (2010).

[14] S. Furnell, V. Tsaganidi, and A. Phippen, Security beliefs and barriers for novice Internet users. *Computer & Security*, vol 27, pp. 235-240, (2008).

[15] Symante, *Symantec internet security threat report*. Trends for January-June 07. Vol. XII. (2007).

[16] CISCO, *A comprehensive proactive approach to web-based threats.* CISCO IronPort Web Reputation White Paper, (2009).

[17] Sophos, The Sophos security threat report, (2009).

[18] Lusaka Times, Zambia: Internet service providers urged to fight cybercrime, (2000).

[19] R. Lemos, Europe asks ISPs to help battle cybercrime, (2008).

[20] BCS, What future for internet service provider? (2009).

[21] Australia, Measure to improve safety of the internet for families, (2009).

[22] E. Sobiesk, J. Blair, G. Conti, M. Lanham, and H. Taylor, Cyber Education: A multi-level, multi-discipline approach. In *Proceedings of the 16th Annual Conference on Information Technology Education,* pp. 43–47, ACM, (2015).

[23] M. J. Dupris, Cyber security for everyone: An introductory course for non-technical major, *Journal of Cybersecurity Education, Research and Practice*: vol 2017 no 1, (2017).

[24] H. J. Kam, and P. Katerattanakul, Diversifying cybersecurity education: A non-technical approach to technical studies. In Frontiers in Education Conference (FIE), 2014 IEEE, pp. 1-4, IEEE, (2014).

[25] S. L. Pfleeger, M. A. Sasse, and A. Furnham, From weakest link to security hero: Transforming staff security behavior. *Journal of Homeland Security and Emergency Management*, vol 11, no. 4, pp. 489–510, (2014).

[26] G. C. Kessler and J. Ramsay, Paradigms for cybersecurity education in a homeland security program. *Journal of Homeland Security Education*, vol 2, no 35, (2013).

[27] RIT General Education Committee, “General Education Framework”, Rochester Institution of Technology, (November 2010).

[28] P. Mullins, J. Wolfe, M. Fry, E. Wynters, W. Calhoun, and R. Montante, *Panel on Integrating Security Concepts and Existing Computer Courses*, SIGCSE’ 02, Covington, KY, pp. 356-366, (2002) .

[29] J.R. Shapiro, and A.M. Williams, The role of stereotype threats in undermining girls’ and women’s performance and interest in STEM fields. *Sex Roles*, vol 66, pp. 3-4, pp. 175-183, (2012).

[30] P. Ifinedo, Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, vol 31 no 1, pp. 82-95, (2012), https://doi.org/10.1016/j.cose.2011.10.007.

[31] R. Wash, Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* pp. 11, ACM, (2012).

[32] R. Von Solms, and S. Von Solms, Cyber safety education in developing countries, *Journal of Systemic, Cybernetics and Informatics,* vol 13, pp. 14-19, (2015).

[33] The first national contest in cybersecurity (capture the flag) occurred in December 2015, http://detri.epn.edu.ec.

[34] N. Kortjan, and R. Von Solms, Cyber security education in developing countries: a South African perspective, *South Africa Computer Journal*, vol 52, pp.29-41, (2012).

[35] P. Denning and A. McGettrick, Recentering computer science, *Communication of the ACM*, vol. 48, no. 11, (2005).

[36] N. Herrmann, J. Popyack, B. Char, P. Zoski, C. Cera, R. Lass, and A. Nanjappa, *Redesigning Introductory Computer Programming Using Multi-Level Online Modules for a Mixed Audience*, SIGCSE 03, Reno, Nevada, pp.196-200, (2003).

[37] S.Sharma and J. Sefchek, Teaching information security courses: A hands-on approach, *Computers & Security*, vol.26, pp. 290-299, (2007).

[38] J. Walden and C. Frank, Secure Software Engineering Teaching Modules, *InfoSecDC 06,* Kennesaw, Georgia, pp. 19-23.

[39] B. Endicott-Popovsky and D. Frincke, A case study in rapid introduction of an information assurance track into a software engineering curriculum, Conference on Software Engineering Education and Training, pp. 118-123, (2004).

[40] Mark Zuckerberg covers his laptop camera and you should too, Australian Financial Review, (June 2016), www.afr.com/technology/web/security/mark-zuckerbergcovers-his-laptop-camera-and-you-should-too-20160623-gppvwy.