Open Access License Notice

Educating the Masses: Cybersecurity for Everyone

D'Kyra Andrews Graham
Department of Computer Science
Norfolk State University
Norfolk, VA, USA
d.andrewsgraham@spartans.nsu.edu

D'Nita Andrews Graham
Department of Computer Science
Norfolk State University
Norfolk, VA, USA
dagraham@nsu.edu

***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 dos and don'ts to ensure end users are not introducing a threat. Having a "cyber aware" student means they go home and to 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 object of this paper is to communicate on the subject of cybersecurity – across all sectors of government, business, academic institution and individual.**

Keywords—cybersecurity, higher education, government, business, awareness, home user, curriculum, individual

I. Introduction

Cybersecurity education has become increasingly important, as cybersecurity integrates into all aspects of daily life. As we think back to our daily habits 15 years ago versus our 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. From the introduction of Facebook in 2004 to the launch of Apple iPhone in 2007 and 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 we never imagined have become essentials in our 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 cyber-attacks driven by increasingly sophisticated cybercriminals. These are unprecedented threats for both consumers and businesses and 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].

II. 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's 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 institutions IT department.

A. 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's 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

979-8-6425-4896-7/20/$26.00 ©2020 CISSE

foundation does not have to be build. "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]." This create a security mindset that facilitates greater understanding of the cybersecurity issues facing the institution. 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]."

III. 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 most lucrative business on the Internet today speaks volume – Fraud [8]. Internet fraud has increased by a substantial percentage over the past years. [8] It is the most profitable business on the internet.

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]. It is essential that we educate, train, and develop cybersecurity professionals to help protect our nation and our people. This includes assisting 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 each and 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. This includes developing awareness programs and some type of enforcement mechanism for home users via their Internet Service Providers (ISPs) [13]. When the society at large is educated in cybersecurity and privacy there is less problems for organizations as non-malicious insiders.

A. Home Users

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]. 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, are 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]

B. Electronic Awareness and Enforcement Model

A methodology to consider is an E-Awareness and Enforcement model (EAAEM). 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 main function of the online awareness portal is to provide current content regarding cybersecurity risks within the home user environment. The goal is to introduce home users to best practices of cybersecurity issues. It is therefore important that the design and implementation of the portal is:

- easy to access
- user friendly

979-8-6425-4896-7/20/$26.00 ©2020 CISSE

- interactivity
- integrated
- relevant content
- comprehensive
- adaptable to all devices
- knowledge based appropriate
- up to date

The online awareness portal should be scalable and 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. The goals and objectives of the online portal should utilize best practices for effective online user success.

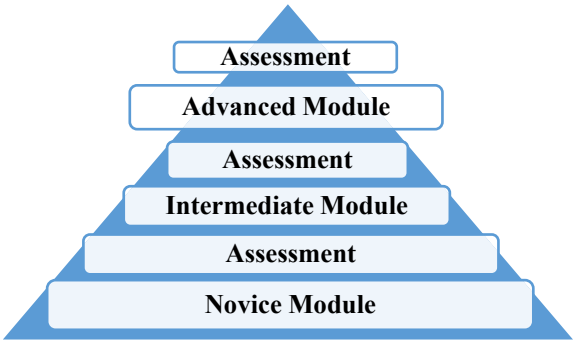

Fig. 1. Layout of Online Awareness Portal

It is essential that the online awareness portal be regularly updated to keep track of new developments and it should 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].

C. *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 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 paedophillia' [20]. '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]. The proposed model can assist in home users being educated and learning cybersecurity tips.

IV. 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 we 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].

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 [24]. 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, improve digital citizen and bring more women into the STEM majors since stereotype threat remains a very large impediment [25].

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 [26]. Likewise, 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 [27]. 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.

Those born after 1995, are colloquially referred to a Generation Z and are considered 'digital natives," having never known a time when they couldn't 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 doesn't 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 educate 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:

Fig. 2. Cybersecurity Concepts Suggested Topics

The topics in Figure 2 are suggested topics that can fulfil the goal of embedding cybersecurity awareness across the curriculum. 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. Universities that develop and implement cyber classes into the curriculum whether it's phycology, 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.

V. Conclusion

The world we live in, has been observed in a 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 doesn't trust his own machine is secure from cyberespionage [28]. If the CEO of one of the world's technology innovators can't necessarily trust his own computer, what does that mean for the rest of us? Helping ensure a secure and successful environment ultimately comes down to every government, business, academic institution and individual around the world. Today we are already in a skill shortage, and if were are to create a growing cybersecurity ecosystem we will need to continue to promote STEM-based skillsets throughout the educational pathway.

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] RIT General Education Committee, "General Education Framework", Rochester Institution of Technology, (November 2010).

[25] 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).

[26] 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.

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

[28] 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.