Open Access License Notice

Improving Workplace and Societal Cybersecurity via Post-Secondary General Education

Maeve Dion
Security Studies Department
University of New Hampshire
Manchester, NH, USA
0000-0001-9352-6447

***Abstract*—Everyone has a role to play in cybersecurity and cyber risk management, but people without security backgrounds seldom understand—let alone accept or endorse—such roles. Public and private organizations face common challenges in facilitating more secure behaviors among employees. As part of their missions, most colleges and universities in the United States have general education programs that aim to instill certain competencies and characteristics in all graduates (for individual and greater good). This paper proposes that a cybersecurity general education course could help improve common workplace challenges in cybersecurity training and awareness, and that such a course could align with each institution's general education goals to benefit not only graduates but also communities and society writ large.**

Keywords—cybersecurity education, risk management, general education, information security, computer security

I. INTRODUCTION

A successful cybersecurity posture means that an organization (a) is confident in its understanding of its cyber risks and (b) is comfortable with its current allocation of risk decisions related to protection/mitigation and incident response activities throughout the enterprise. Maintaining that successful posture requires regular re-evaluation of both (a) and (b) conditions, especially as internal and external changes occur.

Cybersecurity was often allocated to the information technology (IT) team in the past, but the pervasiveness of technology and interconnectedness of systems means that all end users should have a fundamental understanding of cyber risks and basic skills to fulfill their roles in relation to those risks. Inherent to a successful cybersecurity posture is an organizational culture in which all participants not only understand their cybersecurity roles but also accept and even advocate for these responsibilities. Thus, as our everyday societal, civic, and business operations have increasingly become reliant on information and communication technologies, both public and private organizations have introduced cybersecurity training and awareness activities for their employees.

The crux of these activities must be *behavior change*: fostering the skills and attitude shifts needed for the organization to achieve its desired cybersecurity posture. This behavior change can provide benefits beyond a specific organization — i.e., the awareness and skills that end users learn in one organization can carry over into other realms such as their families, social/civic communities, and future employment organizations. This continuum of the shared benefits of cybersecurity training aligns with some of the rationales and purposes for general education in colleges and universities: generating improvements not only for individuals but also for a greater good.

As discussed in this paper, the commonalities within end-user cybersecurity training and awareness needs, and the benefits sympathetic to general education goals (individual, societal, and market based), combine to present a solid argument in favor of including cybersecurity in general education. Section II discusses fundamentals of cybersecurity knowledge and behaviors needed in all kinds of organizations. Section III presents a brief review of post-secondary general education concepts in the United States and a summary of prior literature on cybersecurity for general education. Section IV analyzes how a general education course for cybersecurity could help meet organizational and societal needs while also fulfilling some of the common expectations and purposes for general education. Section V is a brief conclusion.

II. CYBERSECURITY EXPECTATIONS

Cybersecurity standards typically require not only role-based training (targeted to employees with specific duties), but also general training and awareness raising activities for all users authorized to access the organization's systems [1], [2]. In some countries, these requirements have been incorporated into regulations or other legal mechanisms [3], [4]. Similar requirements are found in college-level cybersecurity curriculum guidelines such as [5], which, while targeted toward the education of cybersecurity professionals, also emphasizes that security professionals must be prepared to address cybersecurity training and awareness needs of all end users within their organizations.

For years, organizations in both the private and public sectors have endeavored to establish and maintain general cybersecurity training/awareness programs for their employees. As noted by [6], many programs are focused on policy compliance and are based on rewards/sanctions and deterrence theory, but these may not be the most effective bases for encouraging secure behaviors.

The importance of employees' cybersecurity capabilities and behavior has been amplified by the growing integration of remote work structures and the increased use of personal devices and smart devices throughout organizations. In two large surveys [7], [8], 52% to 56% of respondents identified human error by their employees as the largest cybersecurity vulnerability for their organizations. Lessening the likelihood of errors, and mitigating the impacts when problems occur, are two of the goals of cybersecurity training and awareness programs.

However, while organizations recognize the need to educate and raise cybersecurity awareness in their employees, research shows that their training/awareness programs can still struggle to effect the behavior change needed to sustain or improve the organization's cybersecurity posture [8], [9]. In a 2022 study [9], the largest challenges were: employees' lack of acceptance of the need for cybersecurity training, misunderstanding of the concepts, and a low motivation to participate.

Other studies [6], [10] have indicated that employees engage in insecure and noncompliant behavior due to stressors such as high workloads, perceived barriers to efficient task completion, and a mismatch of benefit/risk calculation. So, even employees who are trained in and aware of the organization's cybersecurity expectations may thus justify their noncompliance with organizational policies/rules; these attitudes and actions can negatively impact an organization's cybersecurity posture.

Echoing these problems, Gartner [11] identified the goals of "fostering new ways of thinking and embedding new behavior" as a key trend to help organizations move "beyond awareness" in their general employee training on cybersecurity. Various scholars, such as [12] and [13], have emphasized the importance of involving the breadth of human motivations in order to encourage the behavior change desired by cybersecurity training and awareness programs.

In the sections below, this paper proposes that a college-level general education course in cybersecurity could lay the foundations for more positive cybersecurity attitudes and behavior, so that more employees go into an organization with clearer expectations and firmer acceptance of their cybersecurity roles and responsibilities, and with enhanced abilities to address the everyday risk decisions related to cybersecurity.

III. BACKGROUND / LITERATURE REVIEW

A. General Education at U.S. Colleges and Universities

In the United States, many higher education institutions use general education to try to inculcate certain kinds of behavior, ways of thinking, and common capabilities in all its graduates. The history of post-secondary general education shows a varied and contentious approach, with institutions typically choosing for themselves how and what to offer as general education [14]. Depending on an institution's choices, general education can emphasize traditional liberal education or professionally targeted preparations for entering the workforce or a blend of both; and, as detailed more fully in [14], institutions may reconsider and reformulate their general education approaches as societies evolve and internal and external pressures come into play.

A full discussion of the social, political, and economic pressures in the history and current context of U.S. general education is beyond this paper, but [14] – [18] provide a solid overview. The purpose of this section is to summarize the goals and nature of post-secondary general education, laying a foundation for considering the inclusion of cybersecurity in such programs.

General education often encourages exploration into broader contexts of a situation or discipline. It helps to develop skills for extrapolating beyond one's own experience/understanding and for spotting and raising questions that can facilitate new or better knowledge. And it exposes students to the processes required to participate and collaborate in solving complex problems. General education also typically cultivates the common knowledge and capabilities necessary to communicate and engage as citizens and members of a community.

Depending on the institution, a general education program may emphasize select moral considerations and social impacts of decision making (e.g., environmentalism, inclusion/diversity, tenets of a certain religion, etc.). Some institutions may focus more on professional education goals in their general education efforts; and other institutions' general education may embrace a more liberal arts experience. Most regional accrediting agencies require that institutions incorporate both career/life preparation and citizen engagement into their curricula [19].

Research on student perceptions about general education show that students have a basic understanding and appreciation of its goals, but they place greater value on discipline-specific courses which they presume have a more direct correlation to career success [18], [20].

Although each institution may differ in approach, the common presumption of general education programs is that the institution wants to achieve some sort of minimal commonality in its graduates—e.g., basic skills for functioning as individuals and as members of a community, fundamental capabilities of certain ways of thinking, an appreciation of and advocacy for particular characteristics, etc. There is often a blend of goals and outcomes, with some focused on benefitting the individual graduate and others looking to benefit communities and the broader society within which that graduate will live and work [14].

As [14] – [19] show, establishing and revising a general education program are complicated endeavors that typically involve intense debates about priorities and resources. For those lobbying to include cybersecurity within a general education curriculum, it is vital to position the course within the undergraduate general education goals and the institution's overall culture.

B. Cybersecurity within General Education

While a good deal of literature has addressed improvements in education for cybersecurity-related disciplines and majors, e.g., [21] – [26], several scholars have provided argumentation and case studies supporting the addition of cybersecurity to post-secondary general education. Incorporating modern technology-related content into general education is not a new concept; the author previously worked for a Swedish university that was one of the first to mandate an information technology law course for all law students, and Caspersen [27] discussed the Danish and broader European movements to include informatics in general education for all education levels.

In the United States, the military service academies were early adopters of adding cybersecurity to their general education curricula. As detailed in [28] and [29], their course content is generally more technically oriented, but non-technical courses in various disciplines also address cybersecurity concerns relevant to the professional missions and educational goals of those academies.

The literature also has examples of cybersecurity courses incorporated into general education at several civilian institutions of higher education, such as Slippery Rock University [30], Towson University [31], the College of Charleston [32], and Old Dominion University [33].

Three of these courses are more technically oriented and include assignments that develop basic skills in securing devices, analyzing risks, and conducting forensics [31]; installing and securely configuring security hardware and software for personal and home use [30]; and conducting traffic analysis related to denial-of-service attacks and ransomware, and exploring the techniques involved in password cracking and device hacking [32]. Faculty developing these courses noted that one of the biggest challenges to creating a general education cybersecurity course was finding suitable course materials, since most cybersecurity textbooks and hands-on cybersecurity tools are targeted toward computing/IT majors [30] – [32].

While these three courses also touched on non-technical matters related to cybersecurity, the fourth case study from Old Dominion University showed how an interdisciplinary group of faculty developed a less-technical cybersecurity course that adds more content related to the societal, cultural, economic, philosophical, and international considerations of cybersecurity [33]. The faculty for this course committed to using only open educational resources (OER) for course materials (in part due to the lack of an appropriate textbook, and in part due to the benefits of OER such as zero textbook costs, more accessibility, and more flexibility).

Among these four cybersecurity general education courses, key goals were to:

- Increase cybersecurity knowledge in the general populace/home user and promote better cyber hygiene on personal devices [30] – [32].
- Develop basic technical skills such as analyzing risks and conducting forensics [31] and performing traffic analysis and incident response [32].
- Convey a general understanding of computer and cybersecurity history, cybercrime, common threats and vulnerabilities, and related legal and ethical matters, [31] – [33].
- Encourage awareness and behavior change regarding oversharing of personal information, social engineering, and safe web browsing [30].
- Promote good workplace behavior by introducing students to the kinds of cybersecurity expectations of employers and discussing "why they should cooperate with their employer in securing the workplace" [30, p. 187].
- Understand and explain the interrelation of cybersecurity to other disciplines/professions and the potential impacts of future change [33].

Faculty in all four courses [30] – [33] indicated that an additional goal of their general education cybersecurity experience was to engage a broader, more diverse student population in the hopes of enhancing enrollments in cybersecurity majors and boosting the cybersecurity workforce.

Some authors, e.g., [31], [32], and [34], noted the need for further innovation on how to educate non-cybersecurity majors so as to reap the personal, organizational, and societal benefits of a more cybersecurity-savvy populace. As part of a wider call for increasing cybersecurity understanding among home users and K-12 students, as well as among organizations' executive leadership, [34] advocated for inclusion of cybersecurity in post-secondary general education; that article did not expound on the alignment with general education or suggest curricula beyond a listing of eight general themes.

So, while there appears to be an increased call for, and experimentation with, general education cybersecurity courses, the examples here can be summarized as (i) military academy courses that relate cybersecurity to the professional missions of those academies and (ii) civilian courses that (for the majority) focus on personal/home user behavior, fundamental technical skills and basic cybersecurity knowledge, and recruitment into the cybersecurity disciplines/workforce.

IV. EMPOWERING CYBERSECURITY BEHAVIOR AND CULTURE WITH A GENERAL EDUCATION COURSE

This section synthesizes the discussions in Sections II and III and proposes some recommendations for a cybersecurity general education course that supports the purposes of general education as well as organizations' need to enhance fundamental cybersecurity knowledge of employees and to foster cybersecurity behavior in alignment with organizational cyber risk management.

As discussed in the above sections, general education is aimed not just toward individual improvements and professional preparation, but also toward garnering benefits for communities/groups and society writ large. All types of organizations face the common challenge of improving cybersecurity understanding and awareness among their employees. Increased cybersecurity knowledge and normalized cybersecurity behaviors are competencies that can be carried by individuals from one organization to another. "Home user" education is a good step toward better cybersecurity practices, but it does not encompass the workplace cybersecurity challenges involving non-technical end users.

Further, studies of the perception of students toward general education courses show that students most value those general education courses that they can directly relate to their future careers. A cybersecurity course that specifically targets workplace expectations—and is transparent as to this goal and the pedagogical approaches — can build on this career-related impact to help foster student motivation and engagement.

At the same time, and as seen in some of the examples discussed above, a cybersecurity general education course focused on the individual's role in an organization can also support general educational goals of promoting certain moral characteristics and liberal education values such as considering broader perspectives, questioning deeper, weighing community impacts of individual decisions, etc.

This alignment with general education goals is especially evident in the teaching of cyber risk management, where individual risk is also a component of group/organizational risk. The interrelationship of risk decisions and consequences can be explored with examples and extrapolation to broader contexts, e.g., for understanding and assessing both individual risk and community risk in situations such as public health (skills that were challenging for many during the COVID-19 pandemic). Helping individuals to consider the wider effects of their decisions may add additional motivation when graduates participate in workplace cybersecurity training/awareness activities.

Currently, innumerable public and private entities—across a swath of professions—are attempting to teach similar fundamental concepts and to promote similar behavior change as part of their organizational cybersecurity training and awareness activities. Most organizations are not experts in education or training, and many are stymied by the challenges inherent in these efforts and by employees' neutralizing behaviors (justifications for not following security protocol).

A cybersecurity general education course for all students could provide a more solid foundation for organizational efforts to build upon. The course could start addressing those neutralizing approaches and could help fulfill a general education mission of enabling a more engaged, responsible, and capable citizenry.

Such a cybersecurity course could be designed in alignment with each educational institution's own priorities for general education (e.g., emphasizing professional or liberal education competencies or both, encouraging appreciation for certain characteristics, etc.) while also fulfilling common, unmet needs in our workplaces.

A recommended approach is to not start with content (firewalls, spam, etc.) but rather to design a curriculum based on general education goals that incorporate common needs for cybersecurity knowledge and behavior change in all workplaces. For example, learning objectives could include the ability to:

- Construct real-world examples of the interconnected systems that we all work and live within and describe how threats, vulnerabilities, and opportunities may evolve.
- Explain how individual, daily activities can impact the security posture of an organization or community.
- Identify real-world factors (social, economic, political) that may alter everyday decisions and consequentially affect organizational cybersecurity postures.
- Develop practices to deliberatively consider risk during daily activities, looking at individual, organizational, and societal consequences (near term and future).
- Access applicable cybersecurity policies (be aware of them and locate them) and discuss their impact on everyday activities.
- Research and maintain current knowledge of processes related to cybersecurity problem-spotting, reporting, and incident response.
- Extrapolate common cybersecurity problems to a particular situation (e.g., hospital, factory, law firm, etc.) and recommend approaches for sustaining cybersecurity awareness among employees there.

The OER approach is also recommended. Although this involves considerably more effort on the teacher's part, the flexibility of OER allows for better customization to a post-secondary institution's general education approach and for more timely adaptation of curriculum to current events (to help further engage students).

It should be acknowledged that the recommendations here would primarily impact those employees who have attended colleges with general education programs. While the number of college graduates is growing and over two million bachelor's degrees were conferred in 2020 alone [35], many other employees move into the workplace directly from secondary education or from a vocational technical program. Various scholars and organizations, such as [36] – [39], are working to improve cybersecurity education and training for youth and young adults outside of the college environment, and these efforts should be considered in

parallel with this paper's call for a post-secondary general education course for improving workplace and societal cybersecurity.

V. CONCLUSION

Organizations in the public and private sectors face common challenges in their cybersecurity training and awareness activities for non-technical end users of their systems. The deeper goal is behavior change: fostering the skills and attitude shifts needed for the organization to achieve its desired cybersecurity posture and to maintain a cybersecure culture in which employees understand their roles and regularly monitor their everyday decisions and activities with due regard to their consequential impacts on organizational cybersecurity and cyber risk management.

In the United States, post-secondary general education aims to instill certain characteristics in graduates across all majors; these competencies are based in both liberal education and professional preparations and typically have outcomes that blend benefits to the individual graduate with benefits to various communities and the democratic society.

A cybersecurity general education course can help to fulfill not only the professional preparation needs of graduates facing cybersecurity expectations in the workplace, it also can help to promote the general education goals of a post-secondary institution. Such a course should focus on interconnected and communal/organizational risks, processes of decision making and problem solving in collaborative and complex situations, and an understanding of and advocacy for individual responsibility to a collective cybersecurity good.

REFERENCES

[1] C. van der Wens, *ISO 27001 Handbook*. North Haven, CT, USA: Deseo, 2019.

[2] *Security and Privacy Controls for Information Systems and Organizations*, NIST Special Publication 800-53 Rev. 5, Sept. 2020, doi: 10.6028/NIST.SP.800-53r5.

[3] J. R. Westby, *D&O Guide to Cyber Governance*. Chicago, IL, USA: ABA Publishing, American Bar Association, 2021.

[4] *Managing Cyber Risk: A Handbook for UK Boards of Directors*. Internet Security Alliance, Arlington, VA, USA, 2018. [Online]. Available: https://www.aig.co.uk/business-insurance/insight-page/article-cyber-handbook-board-directors

[5] CSEC2017 Joint Task Force on Cybersecurity Education, "Cybersecurity curricula 2017: Curriculum guidelines for post-secondary degree programs in cybersecurity," ACM, IEEE-CS, AIS SIGSEC, IFIP WG 11.8, Version 1.0, Dec. 31, 2017. [Online]. Available: https://dl.acm.org/doi/book/10.1145/3184594

[6] M. Siponen and A. Vance, "Neutralization: New insights into the problem of employee information system security policy violations," *MIS Quarterly*, vol. 34, no. 3, pp. 487-502, Sept. 2010, doi: 10.2307/25750688.

[7] Proofpoint, "2022 Voice of the CISO," May 2022. [Online]. Available: https://www.proofpoint.com/uk/resources/white-papers/voice-of-the-ciso-report

[8] R. Bhaskar, "Better cybersecurity awareness through research," *ISACA J*., vol. 3, May 2022, pp. 1-10. [Online]. Available: https://www.isaca.org/resources/isaca-journal/issues/2022/volume-3/better-cybersecurity-awareness-through-research

[9] ThriveDX, "2022 Global cybersecurity awareness training study," Aug. 2022. [Online]. Available: https://thrivedx-2714581.hs-sites.com/cyber-security-awareness-study-download-0

[10] C. Posey and M. Shoss, "Research: Why employees violate cybersecurity policies," *Harvard Bus. Rev*., Jan. 20, 2022. [Online]. Available: https://hbr.org/2022/01/research-why-employees-violate-cybersecurity-policies

[11] Gartner, "Gartner Identifies Top Security and Risk Management Trends for 2022." https://www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-security-and-risk-management-trends-for-2022 (accessed July 25, 2022).

[12] A. McIlwraith, *Information Security and Employee Behaviour: How to Reduce Risk Through Employee Education, Training and Awareness*. Aldershot, UK: Gower Publishing Limited, 2006.

[13] L. Zinatullin, *The Psychology of Information Security: Resolving Conflicts Between Security Compliance and Human Behaviour*. Ely, UK: IT Governance Publishing, 2016.

[14] I. Westbury and A. C. Purves, Eds. *Cultural Literacy and the Idea of General Education: Eighty-seventh Yearbook of the National Society for the Study of Education*. Chicago, IL, USA: Univ. of Chicago Press, 1988.

[15] S. Brint, K. Proctor, S. P. Murphy, L. Turk-Bicakci, and R. A. Hanneman, "General education models: Continuity and change in the U.S. undergraduate curriculum, 1975–2000," *J. of Higher Educ*., vol. 80, no. 6, pp. 605-642, Nov./Dec. 2009, doi: 10.1353/jhe.0.0071.

[16] M. J. Smith and K. L. Tarantino, Eds. *Generally Speaking: The Impact of General Education on Student Learning in the 21st Century*. Gorham, ME, USA: Myers Education Press, 2019.

[17] E. R. White, "General education: An academic adviser's perspective," *J. of General Educ*., vol. 62, nos. 2-3, 2013, pp. 137-143.

[18] C. A. Thompson, M. Eodice, and P. Tran, "Student perceptions of general education requirements at a large public university," *J. of General Educ*., vol. 64, no. 4, 2015, pp. 278-293.

[19] R. Stone, "Promoting the public impact of general education," *J. of General Educ*., vol. 69, nos. 3-4, 2020, pp. 142-153.

[20] M. R. Cope *et al*., "Experiences with general education: How sense of community shapes students' perceptions," *SAGE Open*, vol. 11, no. 4, Oct.-Dec. 2021, doi: 10.1177/21582440211050399.

[21] W. V. Maconachy and D. Kinsey, "Cybersecurity education: A mandate to update," *J. of the Colloq. for Inf. Syst. Secur. Educ*., vol. 9, no. 1, Winter 2022, doi: 10.53735/cisse.v9i1.138.

[22] B. Scott and R. Mason, "Cyber as a second language? A challenge to cybersecurity education," *J. of the Colloq. for Inf. Syst. Secur. Educ*., vol. 9, no. 1, Winter 2022, doi: 10.53735/cisse.v9i1.137.

[23] E. A. Enright *et al*., "Building capacity for systems thinking in higher education cybersecurity programs," *J. of the Colloq. for Inf. Syst. Secur. Educ*., vol. 8, no. 1, Fall 2020.

[24] M. E. Whitman and R. L. Chaput, "Experiential activities for risk management education," *J. of the Colloq. for Inf. Syst. Secur. Educ*., vol. 8, no. 1, Fall 2020.

[25] E. Fulton, C. Lawrence, and S. Clouse, "White hats chasing black hats: Careers in IT and the skills required to get there," *J. of Inf. Syst. Educ*., vol. 24, no. 1, Spring 2013, pp. 75-80.

[26] M. Bishop and D. Frincke, "A human endeavor: Lessons from Shakespeare and beyond," *IEEE Secur. & Privacy*, vol. 3, no. 4, July/Aug. 2005, pp. 49-51.

[27] M. E. Caspersen, "Informatics as a fundamental discipline in general education: The Danish perspective," in *Perspectives on Digital Humanism*, H. Werthner, E. Prem, E. A. Lee, and C. Ghezzi, Eds., Cham, Switzerland: Springer, 2022, pp. 191-200, doi: 10.1007/978-3-030-86144-5.

[28] E. Sobiesk, J. Blair, G. Conti, M. Lanham, and H. Taylor, "Cyber education: A multi-level, multi-discipline approach," in *Proc. 16th Annu. Conf. on Inf. Technol. Educ*., Chicago, IL, USA, Sept.-Oct. 2015, pp. 43-47, doi: 10.1145/2808006.2808038.

[29] C. Brown et al., "Anatomy, dissection, and mechanics of an introductory cyber-security course's curriculum at the United States Naval Academy," in *Proc. 17th ACM Annu. Conf. on Innov. and Technol. in Comput. Sci. Educ*., Haifa Israel, July 2012, pp. 303-208, doi: 10.1145/2325296.2325367.

[30] D. W. Valentine, "Practical computer security: A new service course based upon the national strategy to secure cyberspace," in *Proc. 6th Conf. on Inf. Tech. Educ*., Oct. 2005, pp. 185-189.

[31] G. Meiselwitz, "Information security across disciplines," in *Proc. 9th ACM SIGITE Conf. on Inf. Tech. Educ*., Cincinnati, OH, USA, Oct. 2008, pp. 99-104.

[32] X. Mountrouidou, X. Li, and Q. Burke, "Cybersecurity in liberal arts general education curriculum," in *Proc. 23rd Annu. ACM Conf. on Innov. and Technol. in Comput. Sci. Educ*., Larnaca, Cyprus, July 2018, pp. 182-187, doi: 10.1145/3197091.3197110.

[33] B. K. Payne, W. He, C. Wang, D. E. Wittkower, and H. Wu, "Cybersecurity, technology, and society: Developing an interdisciplinary, open, general education cybersecurity course," *J. of Inf. Syst. Educ*., vol. 32, no. 2, Spring 2021, pp. 134-149.

[34] D. Andrews Graham and D. Andrews Graham, "Educating the masses: Cybersecurity for everyone," *J. of the Colloq. for Inf. Syst. Secur. Educ*., vol. 7, no. 1, Summer 2020.

[35] M. Hanson. "College graduation statistics." Education Data Initiative. https://educationdata.org/number-of-college-graduates (accessed Dec. 11, 2022).

[36] K. Pye, "Teaching cybersecurity in K-12 schools," M.S. thesis, Utica College, 2016.

[37] S. Edwards, A. Nolan, M. Henderson, A. Mantilla, L. Plowman, and H. Skouteris, "Young children's everyday concepts of the internet: A platform for cyber-safety education in the early years," *British J. of Educational Technol*., vol. 49, no. 1, pp. 45–55, 2018, doi: 10.1111/bjet.12529.

[38] "Girl scouts to offer cybersecurity badges," *J. of AHIMA*, vol. 88, no. 9, p. 8, Sept. 17, 2017.

[39] Air & Space Forces Association. AFA CyberPatriot Website. https://www.uscyberpatriot.org/ (accessed Dec. 11, 2022).