TOWARD APPLIED ANDRAGOGY IN CYBER SECURITY EDUCATION

CHRIS SANDERS

ABSTRACT

Most cyber security educators are practitioners first and educators second. While this model ensures learners receive tangible, firsthand insight into the multi-faceted dimensions of protecting computer networks, it comes with drawbacks. Namely, practitioner-educators often fail to acknowledge or adopt educational approaches most beneficial to adult learners in the profession. In this paper, I review literature related to andragogy – the method and practice of teaching adult learners. I'll discuss the average cyber security learner and why most are exceptionally self-directed. Next, I'll describe how practitioner-first instructors fail to harness the fundamental principles of adult education. Finally, I'll paint a picture of some ways the industry might move forward to propel traditional and transformative learning based on andragogical research.

KEYWORDS

Information Security, Cyber Security, Digital Forensics, Incident Response, Security Operation Center, Security Analyst, Andragogy, Education, Pedagogy, Instructional Design, Motivation, Adult Education

If you were to walk into a typical cyber security training event, you would see a familiar scene playing out. An instructor, a practitioner themselves, stands in front of the room providing detailed overviews of technical concepts while slides transition in the background. Every so often they demonstrate a technique; perhaps how to configure a system or use a tool.

Sometimes, they set up exercises allowing the student to practice applying the concept themselves. If you are lucky, a final challenge presents students with the opportunity to connect different lessons into a capstone exercise. At the end of the session, the student walks out feeling like they have learned something and the instructor pats themselves on the back for a job well done. But what happens next?

More often than you'd hope, the student gets back to their workplace and attempts to apply what they've learned, only to find frustration. They lack perspective beyond the instructors, they've failed to retain much of what they learned, and while they understand broad concepts, they struggle to adapt them to their tradecraft. After the frustration mounts, they revert to their prior methods before seeking out new training when more budget becomes available the next year.

The prevalence of examples like this partially explains why cyber security is going through a cognitive crisis. Among the characteristics of this crisis are the reliance on primarily tacit knowledge (Sundaramurthy et al., 2014) and the growing demand for expertise that cannot be met (Oltsik, 2019). Current predominant educational practices in cyber security underscore and contribute to these issues.

In this paper, I'll discuss how the cyber security industry fails to adopt educational approaches most beneficial to its typical learners, particularly as it relates to principles of ***andragogy*** – the method and practice of teaching adult learners. First, I'll discuss the average cyber security learner and why most are exceptionally self-directed. Next, I'll describe how practitioner-first instructors fail to harness the fundamental principles of adult education. Finally, I'll paint a picture of some ways the industry might move forward to propel traditional and transformative learning based on andragogical research.

AN INDUSTRY OF SELF-DIRECTED LEARNERS

Malcom Knowles (1975) defined self-directed learning (SDL) as a process "in which individuals take the initiative, with or without the help of others, in diagnosing their learning needs, formulating learning goals, identifying human and material resources for learning, choosing and implementing appropriate learning strategies, and evaluating those learning outcomes". Cyber security students are likely to be more self-directed than other types of learners for several reasons.

First, cyber security students are primarily adults. Cyber security is a complex field requiring prerequisite knowledge in computer systems and networking. Because many U.S. public middle and high schools are just now starting to offer computer science courses (Code.org, 2019), districts rarely cover security in their curriculum. An individual's self-concept evolves as they age, moving toward more independence. Whereas learning is something that simply happens to children, learning experiences define the self-concept of adults. Learning is not just something adults do, it's who they are. Adults have the agency to choose their educational path, speaking to their self-directedness (Knowles, 1980).

Some universities' designs of cyber security curriculum reveal an understanding of their learners' self-directedness. For instance, Kessler (2007) described building university online digital forensic courses with the assumption that adult learners are "generally more mature and self-directed than traditional-aged students" (p. 4). In corporate training environments, this idea seems to be acknowledged by marketing departments, but minimized during curriculum design and delivery.

Consider that cyber security is also still a fledgling field. In its few decades of existence, even the expert practitioners haven't developed a uniform ability to describe the mental models and best practices their work depends on (Sundaramurthy et al., 2014; Sanders & Rand, 2019). Many of the most fundamental paradigms seem to rest on shaky footing, while job providers struggle to evaluate the merit of ideas for want of authoritative resources. Information is scattered, unreliable, and lacks peer review or vetting by anyone other than the author. Even if learners aren't self-directed when they begin their security careers, they must learn it as a career survival trait. The industry's lack of centralized information sources pushes learners toward self-directedness if they have any hope of solving near-term problems, filling knowledge gaps, or advancing their careers.

PRACTITIONERS FIRST, EDUCATORS SECOND

A significant portion of cyber security education occurs on-the-job or in corporate training. A common theme amongst these courses is that the content designers and instructors are practitioners themselves. This practitioner first, educator second approach is grounded in the first-hand, tangible knowledge of the individual instructor. While typically skilled in their subject matter, practitioner-educators are afflicted with the curse of knowledge. Despite their significant expertise, they don't remember how hard it was to learn the things they already know. Thus, instructional delivery is often centered exclusively on facts or demonstrations with little thought to methods, student context, and other andragogical best practices.

Practitioner-educators usually lack formal training in andragogy, often assuming that there are no appreciable differences in how children and adults learn. This assumption ignores the unique facets of adult learners, such as their need to understand the reason for learning something (Knowles, 1984). Practitioner-educators are often limited in this area by their metacognitive awareness deficiencies. Sundaramurthy et al. (2014) found that "SOC [Security Operation Center] analysts often perform sophisticated investigations, and the process required to connect the dots is unclear even to analysts" (p. 55). Sanders and Rand (2019) found that "While most analysts were able to respond to specific investigative scenarios reasonably, they could not extrapolate on a structured or deliberate investigation process without referencing real-world scenarios" (p. 17).

Even if practitioner-educators are effective at demonstrating procedural knowledge, they may not be equipped to explain why or how they decided to invoke such a procedure, or how it fits into broader investigative concepts. At the same time, they may not strive to enhance their own understanding of these topics because they are unaware of its importance to their learner. This oversight might limit the instructor's ability to provide learners with reasons why they should pursue important concepts or theories -- something adult learners thrive and depend on (Knowles, 1984).

Practitioner-educators may also fail to recognize the value of the adult learner's prior experience and what can happen if that experience isn't adequately assessed and acknowledged. As people get older, they acquire more diverse experience and also place more value on it. Because adults derive much of their identity and self-concept from their experiences, ignoring or devaluing that experience in a classroom environment may have negative consequences (Knowles et al., 2014). In investigation-centric fields like cyber security, analysts acquire diverse experiences to encourage investigative success. The more examples of normal and abnormal system behavior they acquire, the better equipped they'll be differentiating the two moving forward. If instructors fail to acknowledge experience in this

field where practitioners so actively seek it, they may find themselves at odds with their students and hinder the learning process.

A WAY FORWARD WITH SELF DIRECTED AND TRANSFORMATIVE LEARNING

Given the security workforce landscape, it's unreasonable that we should expect all educators in the field to acquire a degree in education. At the same time, the practitioner-educator model is unlikely to go anywhere soon. Therefore, practitioners seeking to maximize learning gains for their students should pursue knowledge about unique facets of the adult learner and apply those andragogical principles to their instructional design and delivery.

Practitioner-educators can start by leveraging how environmental context plays a role in adult education. For example, cyber security practitioners are likely to be more amenable to online learning due to their comfort using technology supporting online course delivery. Online learning shares a strong link with SDL, as students need a higher degree of self-direction to succeed in distance education environments (Shapley, 2000). This idea fits well within the notion that cyber security learners may already be highly self-directed for the reasons discussed earlier in this article. While Knowles primarily discusses SDL as a process, Brockett and Hiemstra (2018) describe it as a goal for learners to assume responsibility for their learning. Vonderwell and Turner (2005) found that online learner context impacts learner's perceptions of their self-direction, making them feel as though they're taking more control over their education. Therefore, effective use of online instruction in cyber security education leverages propensity toward SDL that already exists, while also helping to instill those qualities in learners.

Instructors would also be thoughtful to leverage prior experience to spur self-directedness. Candy (1991) found that learners have higher levels of self-directedness when topic areas are familiar or where they have similar previous experiences. Instructors who find mechanisms that allow cyber security learners to express their diverse experiences may create opportunities to connect new knowledge to those experiences. This tactic may also enable learners to stumble upon sources of intrinsic motivation, which is a powerful tool for increased learning.

Cyber security instructors who acknowledge the self-directed nature of their learners may also adapt their course delivery to characteristics inherent to their students' context. For example, Taylor et al., (2017) highlighted tactical issues faced when developing online cyber security courses, such as with the length of course sessions:

> *The developers discovered the level of concentration in self directed learning dipped quickly after 30 minutes. This was usually because the build-up of emails or the desk phone lights blinking became an increasing distraction to the learner. As time went on, the learners felt the need to manage these intrusions and this required that they Save & Return the programme, thereby losing important focus at a critical time. (p. 6)*

Considering the context of the adult learner in educational content delivery provides an opportunity for instructors to incorporate findings such as this one.

When instructors thoughtfully consider the context of the learner, they can kindle transformative learning. Mezirow (2000) described transformative learning as a process where learners transform mindsets to "make them more inclusive, discriminating, open, emotionally capable of change, and reflective so that they may generate beliefs and opinions that will prove more true or justified to guide actions" (p. 8). **Since so much cyber security knowledge is tacit, practitioners are likely to become a victim of their own experience**. An analyst may reach a conclusion the first time because it's the best they could do without some explicit knowledge that they can't find or doesn't exist. Even though the conclusion is weakly supported, they rely on it for so long that it becomes a foundation for other knowledge to which even more outcomes depend. The opinion they now rely on as fact provides shaky scaffolding for future investigations, creating a potential for cascading failures. This type of knowledge and the mindsets it creates are ripe for transformation by skilled instructors.

Researchers often see transformational learning as unique to adults. One reason for this may be that the breadth of experiences adults have provides a broader base for disorienting dilemmas. A disorienting dilemma is a significant life event that may lead to intense self-examination and critical assessments of assumptions. These dilemmas are the first step of what Mezirow (2000) identified as a typical ten-step process that students undergo when transformational learning occurs. Disorienting dilemmas lead to self-examination, critical assessment of assumptions, exploration of new ideas, acquisition of diverse knowledge, and eventual reintegration of new perspectives into a world view. These ideas align with many favorable traits most associate with critical thinking.

Cyber security does not exist in a vacuum. Analysts conduct investigations and draw conclusions that frequently consider social, historical, and political contexts. But, many analysts don't formally study these additional subjects. Instructors can help analysts view the world through these lenses from time to time by facilitating individual paradigm challenging transformational learning.

CONCLUSION

Any field in its infancy must formalize what is known, how it's known, and how educators relay that information. Cyber security is no different. Practitioner-educators that understand what makes adult learners unique and apply those andragogical principles position themselves to achieve the most effective learning outcomes with their students. This result could mean engaging more students within a given classroom, ensuring concepts are better applied when analysts take what they've learned back to their network, or sparking transformational learning that helps analysts tackle familiar problems in new ways. All three outcomes can result in a more secure society.

REFERENCES

Brockett, R. G., & Hiemstra, R. (2018). *Self-direction in adult learning: Perspectives on theory, research and practice*. Routledge.

Candy, P. C. (1991). *Self-Direction for Lifelong Learning. A Comprehensive Guide to Theory and Practice*.

Code.org. (2019). *State of computer science education*. (2019). https://advocacy.code.org/

Heuer, R. J. (1999). *Psychology of intelligence analysis*. Center for the Study of Intelligence, Office of the Director of Central Intelligence

Kessler, G. C. (2007). Online education in computer and digital forensics: A case study. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)* (pp. 264a-264a). IEEE.

Knowles, M. S. (1975). *Self-directed learning: A guide for learners and teachers*.

Knowles, M. S. (1980). *The modern practice of adult education*.

Knowles, M. (1984). *The adult learner: a neglected species*.

Knowles, M. S., Holton III, E. F., & Swanson, R. A. (2014). *The adult learner: The definitive classic in adult education and human resource development*. Routledge.

Merriam, S. B., & Bierema, L. L. (2013). *Adult learning: Linking theory and practice*. John Wiley & Sons.

Mezirow, J., & Associates. (2000). *Learning as transformation: Critical perspectives on a theory in progress*. Jossey-Bass.

Oltsik, J. (2019, January 10). *The cybersecurity skills shortage is getting worse*. https://www.csoonline.com/article/3331983/the-cybersecurity-skills-shortage-is-getting-worse.html

Sanders, C. & Rand, S. (2019). Creative Choices: Developing a theory of divergence, convergence, and intuition in security analysts. Retrieved October 11, 2019, from https://chrissanders.org/2019/10/creative-choices-paper/.

Shapley, P. (2000). On-line education to develop complex reasoning skills in organic chemistry. *Journal of Asynchronous Learning Networks*, *4*(2), 43-52.

Sundaramurthy, S. C., McHugh, J., Ou, X. S., Rajagopalan, S. R., & Wesch, M. (2014). An anthropological approach to studying CSIRTs. *IEEE Security & Privacy*, *12*(5), 52-60.

Taylor, J., McAlaney, J., Hodge, S., Thackray, H., Richardson, C., James, S., & Dale, J. (2017, April). Teaching psychological principles to cybersecurity students. In *2017 IEEE Global Engineering Education Conference (EDUCON)* (pp. 1782-1789). IEEE.

Vonderwell, S., & Turner, S. (2005). Active learning and preservice teachers' experiences in an online course: A case study. *Journal of technology and teacher education*, *13*(1), 65-84.

AUTHOR BIOGRAPHY

Chris Sanders is the founder of Applied Network Defense, an information security training company. He is also the Director of the Rural Technology Fund, a non-profit organization that donates scholarships and technology education equipment to public schools to further computer science education in rural and high poverty areas. He is the author of Intrusion Detection Honeypots, Applied Network Security Monitoring, and Practical Packet Analysis.

Chris is an EdD candidate at Baylor University. He holds the GSE, GCIA, GCIH, GREM, GPEN, GSEC, CISSP, and Security+ designations. His current research focus is on the intersection of cyber security, cognitive psychology, and education to enhance the field of information security investigative disciplines through a better understanding of the human thought and learning processes.

Chris blogs at https://chrissanders.org and is on Twitter @chrissanders88.