Teaching Cybersecurity in the Digital Rhetoric Classroom

Christoffer Turpin

Department of English, The Ohio State University

March 30th, 2023

Introduction

Weiss et al (2022) wrote “it is clear the current prevention and mitigation cybersecurity strategies are not working.” One only needs to look at the never-ending parade of cybercrimes in the news to see this. Uber, Apple, Meta, major universities, the IRS, the Democratic National Convention, all of these (and more) have been victims of cybercrimes in the past five years. These institutions have massive amounts of resources they can leverage, but even with all those resources they regularly fall victim to cybercriminals. And that’s just the high-profile cybercrime, everyday tens of thousands of smaller institutions and individuals become victims (University of North Georgia, 2022). Clearly, the way we do cybersecurity today isn’t working. Given the very real risks of cybersecurity breaches, it’s time to reconsider how we do cybersecurity. In this article I argue that it can be fruitful to turn to the field of rhetoric when reconsidering how we do cybersecurity, because most cybercriminals leverage rhetoric as their principal attack vector. More specifically, I describe how one can draw from the field of digital rhetoric to design cybersecurity education programs that are more effective than the current programs.

The structure of this article goes as so; I begin by providing background on both rhetoric and cybersecurity. I then discuss social engineering, a practice where rhetoric and cybersecurity collide. Next, I discuss what security education, training, and awareness (SETA) programs are and why they tend to fail. After that, I describe how one can draw on the field of digital rhetoric to produce more effective SETA programs. I end with the early results of my research and a brief discussion of potential future research directions.

Background

I want to begin this article with some general definitions because those who have a strong understanding of what rhetoric is may not have a strong understanding of what cybersecurity is and those who have a strong understanding of cybersecurity may not really understand what rhetoric is. So, in this section I describe rhetoric and its subfield of digital rhetoric as well as cybersecurity.

Rhetoric

Rhetoric gets a bad rap in popular discourse, generally its viewed as something akin to lying. Often, you'll hear phrases like "mere rhetoric" or "troubling rhetoric" and so on. These phrases speak to the distrust of rhetoric in the popular understanding. But rhetoric is a much broader and ethically nuanced thing than that understanding accounts for. Aristotle (circa 400 B.C.E.) defines rhetoric as "an ability… to see the available means of persuasion" in any given situation (qtd. in Kennedy, 2007, p. 37). Of course, being able to see how to persuade someone to do something outside of their own interest is in most cases clearly unethical; however, there are many instances of ethical persuasion. Rhetoric can be used to persuade people to follow traffic laws, to buy into shady investments, to give to charity, to swarm a capitol building, to release a hostage, to believe (or not to believe) a scientific finding, to take up or drop a religion, and so on. The academic field of rhetoric is interested in explicating how rhetoric works in order to better understand persuasion, both so people can be stronger critical thinkers who are able to see when and how they have been persuaded and so that they can be better rhetors (those who do rhetoric) themselves.

Digital Rhetoric

Digital rhetoric is a subfield of rhetoric which focuses on rhetoric about, with, and by computer enabled systems (Eyman, 2015). Digital rhetoric is interested in asking questions *about* the discourse around computer systems, with questions like is this new computer system good or bad for society? Can this system be built better? What does "better" even look like? And so on. Along with these discourses about computer systems, digital rhetoric is also interested in exploring rhetoric produced *with* computer systems with questions like, how does the modality of a computer system or software enable new forms of rhetorical production and how can these forms used? Finally, digital rhetoric is interested in rhetoric done *by* computer systems with questions like how the user interface of a computer system persuades users to act a certain way. In a nutshell, rhetoric is the study of persuasion – which may or may not be ethical. Whereas digital rhetoric is the study of persuasion related to computer systems.

Cybersecurity

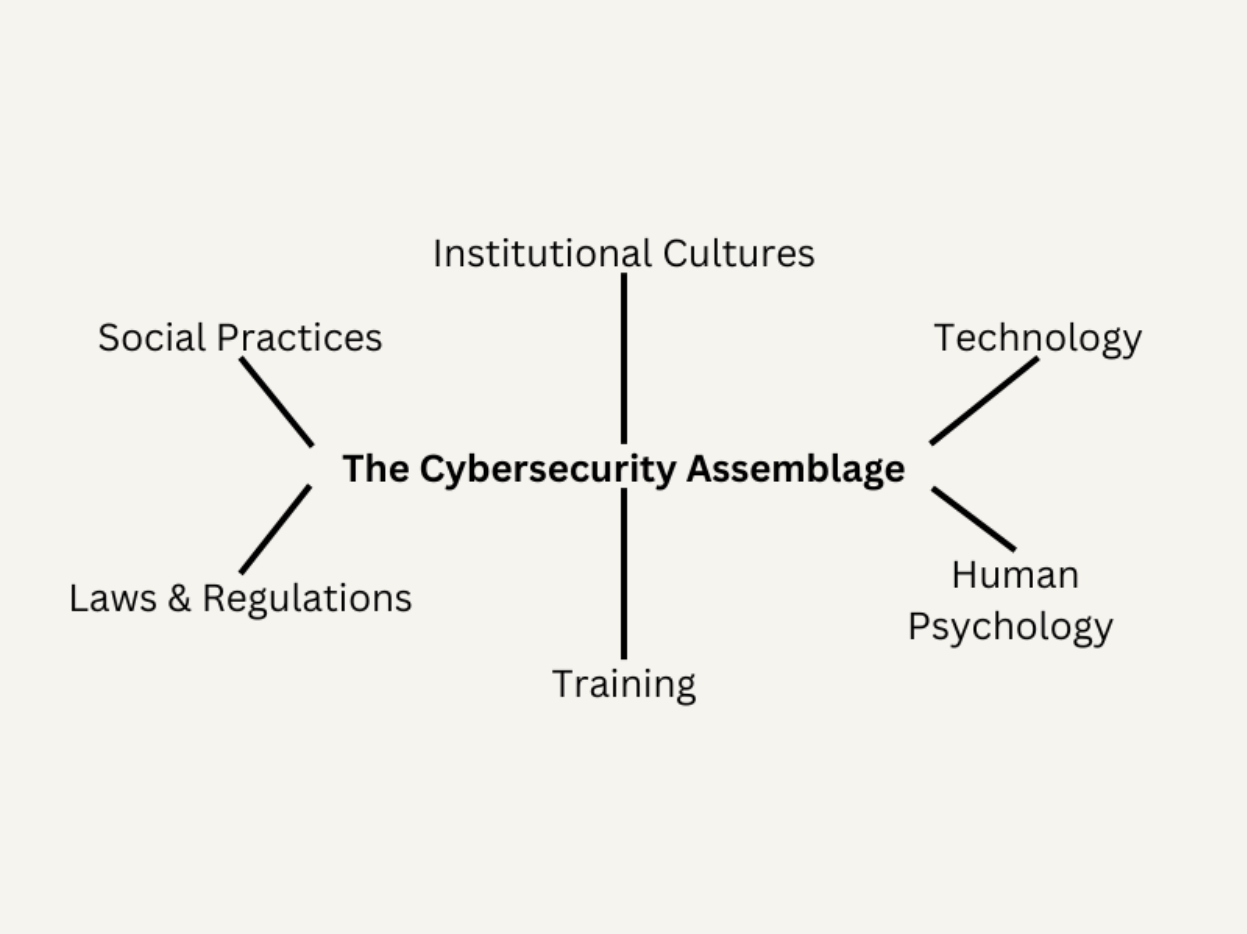
Craigen et al. (2014) defined cybersecurity as:

> the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights.

To put it another way, cybersecurity is the practice of making sure you stay in control of computer systems which are rightfully yours. Admittedly the word "rightfully" does a lot of lifting here, but for the purpose of this article I want to leave that stoned unturned since it leads to complex questions about concepts like ownership, public spaces, and so on which are to broad to really cover here.

Two inaccurate views of cybersecurity dominate cybersecurity discourse, they are that cybersecurity is a status quo which can be achieved, and that cybersecurity is a principally technical thing. Klimburg-Witjes & Wentland (2021) noted that cybersecurity is often viewed as a status quo which can be achieved. In this inaccurate view one does certain things – like installing a fancy new firewall – and thus achieves cybersecurity. This view hides the fact that cybersecurity is a "heterogenous, constantly renegotiated process" (Klimburg-Witjes & Wentland, 2021, p. 1333). For Klimburg-Witjes & Wentland cybersecurity is more a "matter of concern rather than a matter of fact with its ontological status being both political and open to contestation" (p. 1337). In other words, cybersecurity is more of a constant dance or ongoing debate, rather than a stable checklist one can tick off.

Along with this misunderstanding of cybersecurity as a status quo, cybersecurity is viewed as a principally technical endeavor. Collier (2018) writes that cybersecurity is best understood not as a chiefly technical endeavor but as an "assemblage" composed of human and non-human actors. Here one can see an example of the cybersecurity assemblage.



(Figure 1: The Cybersecurity Assemblage)

Yes, technical elements like firewalls are part of the assemblage. But so too are things like institutional cultures, regulations, social norms, human psychology, and so on. To be cybersecure is to be aware of the elements in the assemblage and how those elements interact and produce desirable and undesirable possibilities.

Rhetoric & Cybersecurity

Rhetoric and cybersecurity come together and overlap in a lot of ways. When an IT department sits down to determine how to approach cybersecurity in their network they are enmeshed in an extremely rhetorical process, being persuaded and persuading each other that

certain systems are better in certain contexts, that certain threats need more attention than others, that the budget is being spent in the most effective way, and so on. While I focus on something called social engineering in this article, I mention this sort of rhetoric *about* cybersecurity just to demonstrate how deeply rhetorical cybersecurity is at numerous levels. But, as I said, the intersection of rhetoric and cybersecurity which I focus on in this article is social engineering.

Social Engineering

What is social engineering? Social engineering is an array of rhetorical strategies designed to manipulate users into doing an attacker's bidding (Wu, 2020 / Gehl & Lawson, 2022). Readers may be familiar with the phishing email, a common social engineering attack. In the phishing email attackers attempt to persuade users to take certain actions (like clicking on a malicious link) which compromise their cybersecurity. The phishing email is a simple form of social engineering, but there are numerous types of varying complexity. Case in point, in 2019 a British energy company was attacked by social engineers who trained an AI speech synthesizer to mimic a top executive's voice, allowing them to trick employees into transferring money by impersonating that executive on the phone (Stupp, 2019). Social engineering comes in many flavors of varying complexity and is often extremely effective. Social engineering is so effective it is the principal attack vector in 75% to 90% of cybersecurity breaches (Nobels, 2016 / Mitnick, 2022). In other words, cybercriminals rarely attack computers with code, they attack people with rhetoric.

Security Education, Training, and Awareness Programs

Security education, training, and awareness (SETA) programs are programs designed to harden the human attack surface against social engineering. Most large institutions use some

form of SETA program, for example the SETA program here at OSU is called Cybersecurity 4 U. Unfortunately, empirical research shows SETA programs are at best not very effective at fostering cybersecurity and at worse actively harm cybersecurity outcomes (He et al, 2019 / Wu, 2020 / Klimburg-Witjes & Wentland, 2021 / Zhang et al, 2021). This is a major problem since, as I described above, the vast majority of cybercriminals leverage social engineering as their principal attack vector. Until we develop an effective SETA program that hardens users against social engineering, we will continue to see the same never-ending parade of cybersecurity incidents caused by social engineering.

Why SETA Programs Fail

SETA programs fail for a few reasons. All these reasons speak to the same flaw at the heart of SETA programs, a lack of pedagogical understanding and skill on behalf of program designers. What I mean by this is that SETA programs tend to be designed and administered by cybersecurity technicians and business managers. These people – traditionally viewed as responsible for cybersecurity – lack the humanist background needed to understand social engineering and the pedagogical skill needed to design and teach SETA programs that harden students against social engineering (Nobels, 2016).

More specifically, SETA programs fail for four reasons. First is a lack of student buy-in. Students view SETA programs as boring and unhelpful (Reeves et al, 2021). Second, these programs create a false sense of security (Caldwell, 2016). Many cybersecurity professionals and business managers – and to some degree students – assume that doing these ineffective programs will make them more cybersecure, which they don't actually do. Third, these programs promote antagonism and dysfunction between user populations and cybersecurity administrators

(Klimburg-Witjes & Wentland, 2021). Within cybersecurity there is a narrative that positions users as hapless idiots come to ruin cybersecurity administrators' perfect systems. SETA programs often propagate that narrative and users tend to pick up on this positioning and resent it. Fourth – and most importantly – these programs produce reactive as opposed to proactive users (Kranch, 2019). In other words, SETA programs only train users to respond to predefined threats with predefined strategies, as opposed to teaching students to be proactive in locating emerging or potential threats and developing agile in situ responses to them. An effective SETA program needs to be engaging, teach students to be proactive, and treat them with respect – as valuable assets within a cybersecurity assemblage – not just as idiots and problems to be solved.

Building a Better SETA Program

The digital rhetoric classroom traditionally teaches the competencies that SETA programs try – but fail – to teach. These are things like analyzing digital texts, understanding how things like persona, genre, and audience function in digital environments, and just generally knowing how rhetoric and persuasion work. If rhetoric is the cause of most cybercrime, it only makes sense to turn to rhetoric for the solution. This is what I've attempted to do in my digital rhetoric class.

As part of an IRB approved study I've converted my digital rhetoric class into a place of cybersecurity education to develop and test a novel approach to SETA. I've drawn on a few pedagogical strategies from the field of digital rhetoric and high-level technical cybersecurity education to do this redesign. These pedagogical strategies are critical making, rhetorical carpentry, and what Kranch calls an "offense first" approach to cybersecurity education. I describe these strategies below.

Critical making and rhetorical carpentry are pedagogical strategies which ask students to think about how they are enmeshed within assemblages by actually making with the things of those assemblages as opposed to simply learning about a topic at an intellectual arm's length (Ratto, 2011 / Brown & Rivers, 2013). Critical making and rhetorical carpentry – referred to just as making from here on out – differ from active learning in their focus on product and process. In active learning the focus is on making things so that students produce ever more perfect (according to some metric) products. For example, in a portrait drawing class students may use active learning by drawing portraits over and over again until they become competent artists according to some metric. In contrast to active learning, making focuses on the act of making itself, not so much the product. Making asks students to think about how the various elements of an assemblage can come together, what the many possibilities of that assemblage are, and how these possibilities can come to be by using the process of making itself as sort of focus or nexus that brings these things into relief.

Making complements what Kranch (2019) called an offense first approach to cybersecurity education. Kranch was talking about high-tech education for cybersecurity professionals, but his approach can be made to work at the more social and discursive level of social engineering and SETA. What Kranch argued is that it is always better to teach the offense in cybersecurity, even if the goal is to train defenders. The reason for this is two-fold. First, learning the offense is more fun and engaging. Cybersecurity scenarios are not symmetrical; generally speaking, attackers always have an advantage. The reason for this is that defenders only need to make one mistake to open themselves up to attackers, while attackers are free to make as many mistakes as needed until they eventually succeed. Because of this those training in defensive modes tend to fail much more often than they succeed, and failure – Kranch reasoned

– is less engaging and fun than winning. If students aren't engaged and having fun, they likely won't want to learn about critical cybersecurity concepts and strategies. Learning the offense also provides students with firsthand experience using the tools and techniques of attackers. This gives them a much more intimate knowledge of the ways cybercriminals attempt to attack them than a defense first approach. Students are given a more intimate knowledge of the tools being used against them, because they learn how those tools work. This turns students into proactive assets within a cybersecurity assemblage by giving them the ability to find new weaknesses and come up with proactive responses to these weaknesses before they are exploited by malicious actors.

What making and Kranch's offense first approach to cybersecurity education suggest is this; if we want to train students to be able to resist cybercriminals, we need to teach students the actual tools and techniques of cybercriminals. The goal here isn't to produce more cybercriminals, but instead get students thinking about how cybercriminals actually do what they do so that they can resist them. Given that most cybercriminals leverage social engineering – a form of digital rhetoric – these tools and techniques can be effectively taught and explored in the digital rhetoric classroom.

In figure 2 you can see my students practicing this makery/offense-first approach. They are building a mock internet out of string and paper routers and computers to understand how information flows through the internet and how cybercriminals can take advantage of that process.

(Figure 2: Students practicing critical making.)

Along with exercises like the one seen above, I've experimented with lessons and activities where students do things like develop mock phishing campaigns, produce and attempt to disseminate misinformation, learn digital forgery, learn how strong cryptography works, and so on. Again, the goal here isn't necessarily to teach students how to produce great forgeries, for example. Instead the goal is just to show students how actual cybercriminals do what they do so they can resist these techniques.

Early Results

While I won't know the full results of my approach until my class is completed and I can really dig in and analyze the data I've collected, the early results are promising. All the classroom data I provide below is taken from anonymous surveys and in class quizzes.

It's hard to tell exactly how effective current approaches to SETA are at raising awareness about cybersecurity concerns like social engineering. The main reason for this is that the analysis of SETA programs is a relatively new academic endeavor (Amara et al, 2021). However, the general consensus is that current SETA programs do little to actually raise awareness of social engineering (Aldawood & Skinner, 2018 / Aldawood & Skinner, 2019 / Grassegger & Nedbal, 2021). In my approach 95% of students can describe social engineering and 75% can do so at a high level, describing specific social engineering strategies and their application. As described above students of traditional SETA programs find them boring and unengaging (Reeves et al, 2021). In my approach 94% of students anonymously report being at least "somewhat engaged" with the class content, and 75% reporting they are "very" engaged. As Kranch describes, traditional defense first approaches to cybersecurity education do not tend to foster an ongoing interest in cybersecurity. In my approach 64% of students anonymously report wanting to learn more about cybersecurity. In traditional SETA programs only 2% of students can articulate their role in improving the overall cybersecurity of their assemblages (Hadlington, 2017). In my approach 95% of students can articulate ways to improve their overall cybersecurity assemblage based on questions drawn from the Global Cybersecurity Index, a questionnaire designed to test cybersecurity skills (Bruggemann et al, 2022). It seems my approach to SETA is more effective than traditional approaches.

Conclusion

In this article I described why SETA programs don't work, and a way of doing the sort of education SETA programs fail to do in the digital rhetoric classroom. What this research suggests is this; SETA programs may be improved by adopting a makery and offense first approach. In a nutshell, if one wants to teach students how to resist cybercriminals one must teach students how cybercriminals actually do what they do. Doing this creates proactive, engaged, user-assets who can contribute to their cybersecurity assemblages. Future directions of this research include refining the method and seeing if this approach can be used in other contexts like in corporate training programs.

If the reader takes anything from this article, it should be this; rhetoric is the cause of most cybercrime and potentially the solution. Our students will face potentially very serious cybersecurity challenges in the future. But the academy is doing very little to equip them with the tools needed to face those challenges. The approach to SETA piloted in my research suggests that the digital rhetoric classroom is an excellent place to provide students with these critically needed tools. But to do that we need to rethink how SETA is done. This article offers one way of doing that rethinking by leveraging making and offense first pedagogy.

References

Aldawood, H., & Skinner, G. (2018, December). Educating and raising awareness on cyber security social engineering: A literature review. In *2018 IEEE international conference on teaching, assessment, and learning for engineering (TALE)* (pp. 62-68). IEEE.

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet*, *11*(3), 73.

Aristotle. *On Rhetoric: A Theory of Civil Discourse*. Translated by George A. Kennedy, Oxford UP, 2007.

Brown, J. J., & Rivers, N. (2013). Composing the carpenter's workshop. *O-Zone: A Journal of Object-Oriented Studies*, *1*(1), 27-36.

Bruggemann, R., Koppatz, P., Scholl, M., & Schuktomow, R. (2022). Global cybersecurity index (GCI) and the role of its 5 pillars. *Social Indicators Research*, 1-19.

Collier, J. (2018). Cyber security assemblages: A framework for understanding the dynamic and contested nature of security provision. *Politics and Governance*, *6*(2), 13-21.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10).

Eyman, D. (2015). *Digital rhetoric: Theory, method, practice* (p. 177). University of Michigan Press.

Gehl, R. W., & Lawson, S. T. (2022). *Social Engineering: How Crowdmasters, Phreaks, Hackers, and Trolls Created a New Form of Manipulativ e Communication*. MIT Press.

Grassegger, T., & Nedbal, D. (2021). The role of employees' information security awareness on the intention to resist social engineering. *Procedia Computer Science*, *181*, 59-66.

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*(7), e00346.

Harman, G. (2011). *Guerrilla metaphysics: Phenomenology and the carpentry of things*. Open Court.

He, W., & Zhang, Z. (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of Organizational Computing and Electronic Commerce*, 29(4), 249-257.

Klimburg-Witjes, N., & Wentland, A. (2021). Hacking humans? Social Engineering and the construction of the "deficient user" in cybersecurity discourses. *Science, Technology, & Human Values*, *46*(6), 1316-1339.

Kranch, M. (2019, June). Why You Should Start with the Offense: How to Best Teach Cybersecurity's Core Concepts. In *Colloquium for Information Systems Security Education* (Vol. 23, No. 1, pp. 1-12).

Mitnick, K. (2022). Are social engineering attacks on the rise? *Mitnick Security.*

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. *HOLISTICA–Journal of Business and Public Administration*, *9*(3), 71-88.

Pinto, L., & Blue, L. (2021). Critical making takes a holiday. *Encounters in Theory and History of Education*, *22*, 187-204.

Ratto, M. (2011). Critical making: Conceptual and material studies in technology and social life. *The information society*, *27*(4), 252-260.

Reeves, A., Calic, D., & Delfabbro, P. (2021). "Get a red-hot poker and open up my eyes, it's so boring" 1: Employee perceptions of cybersecurity training. *Computers & Security*, *106*, 102281.

Skibell, R. (2002). The myth of the computer hacker. *Information, Communication & Society*, *5*(3), 336-356

Stupp, S. (2019). Fraudsters used AI to mimic CEO's voice in unusual cybercrime case. *The Wallstreet Journal.*

University of North Georgia (2022). Cybersecurity: a global priority and career opportunity. *The University of North Georgia.* https://ung.edu/continuing-education/news-and-media/cybersecurity.php

Wu, D., Zhang, J., Brown, N., Lowry, P. B., & Moody, G. D. (2020). Patching The "Human" in Information Security: Using the Inoculation Defense to Confer Resistance Against Phishing Attacks

Zhang, Z. J., He, W., Li, W., & Abdous, M. H. (2021). Cybersecurity awareness training programs: a cost–benefit analysis framework. *Industrial Management & Data Systems*.