New Approaches to Cybersecurity Education (NACE) Workshop
Topic: Making Socio-Technical Cybersecurity a Part of Educational Preparation
Chris Bronk and Wm. Arthur Conklin
University of Houston

Summary

While cybersecurity was once a small niche area, primarily, but not entirely contained in computer science and engineering, it is increasingly viewed as a significant societal problem. Getting "hacked" is a relatable experience to millions of Americans in personal or professional venues. But finding remedy or protection is far harder than being compromised by cyberattack. For this reason, we propose effort on connecting to disciplines in developing fundamental learning injects for cybersecurity that align with other forms of professional responsibility and ethics.

The Problem: Cybersecurity Outside the Cybersecurity "Priesthood"

Cybersecurity has become a fundamental component of the socio-technical environment where an enormous amount of work takes place. Professional activity in all manner of endeavor and enterprise is dependent upon a technological infrastructure that remains inherently insecure. Thus far, the primary response to our societal cybersecurity problem has been cybersecurity chiefly as a technical design objective; something to be engineered into a tool, a product, or a process. This focus on "build to deploy" efforts has resolved some issues but falls short of comprehensive remedy. Effective cybersecurity over the long-term requires greater breadth and wider penetration of cybersecurity behaviors across the entire range of activities enabled by information and computing technologies.

While we work to expand the professional cybersecurity workforce, there is an enormous unresolved question regarding our current efforts: *How do we integrate cybersecurity behaviors into the education programs for business, law, social sciences, medicine, and other areas?* The understanding of technology, its promise and limitations, as well as the responsibilities in employing it, requires the inclusion of cybersecurity know-how into a wide range of disciplines.

For example, consider the field of social work, an area of specialization that employs almost 700,000 people in the United States and will add 100,000 additional professionals by 2026.[*] Social workers observe client confidentiality, maintain records protected by multiple regulatory regimes, and increasingly employ digital tools as enablers for productivity. The question we want to answer for it is: How does social work curriculum need to incorporate cybersecurity into professional preparation? This is a question in need of application *to many fields*.

Cybersecurity for Everybody?

When we start approaching how disciplines should incorporate cybersecurity into decision-making, professional responsibility, and leadership, there is obvious pushback on simply

exporting general cybersecurity knowledge from computer science and engineering. Professionals in myriad fields need to know what is relevant to them – starting with regulatory items that may be detrimental to certification or continued practice in a given field – but accepting the need for practical professional preparation on cybersecurity will require new modes of identifying, encapsulating, and delivering relevant critical knowledge. Expanding cybersecurity education and training efforts to a wider audience should include presenting relevant material in many majors and professional degree programs: business (including MBAs); law and social science; psychology; science; medicine; and engineering among others.

One answer on cybersecurity outside of traditional areas in academia has been to leave the problem to employers. This often translates to online annual training that likely has little impact on cybersecurity awareness and behavior.[†] Critical thinking on cybersecurity in preparation and lifelong learning for non-cybersecurity professionals is desperately needed, but rarely found inside most undergraduate disciplines or higher levels of education. Consider Symantec's lead healthcare technical architect's statement from just last year, who said of medicine, "[W]ith the exception of a few 'doctor-turned-geek' type of characters, I [have] never interacted with a doctor on cybersecurity – meaning those doctors whose main role is delivering care and who have not shifted gears into the IT or regulatory space."[‡]

What Needs Doing

There is an unmet need in understanding what and how much security knowledge is needed by professionals as their careers become increasingly influenced or shaped by information and computing technology. Unfortunately, most have little expertise in how to employ them responsibly with regard to cybersecurity. Even in computing disciplines, there has been considerable debate in how much cybersecurity thinking need be horned into undergraduate and graduate degree programs.

Where we need to advance cybersecurity is in engaging with other fields – business, law, medicine, and many others – to create meaningful professional preparation that can be built upon as cybersecurity evolves. This will mean engaging with disciplines across the university. The objective is not to make people in all disciplines cybersecurity experts, but rather deliver targeted awareness to issues that are within the context of their responsibilities. For instance, social engineering and phishing education is needed by all who use email. But understanding how email works is far less important than knowing how actions and behaviors are manipulated by others in the medium. The need is in incorporating cybersecurity behaviors or logics into daily work.

Expansion of cybersecurity elements into other disciplines curricula needs to be context aware, and user context behavioral based elements should address the following areas of interest:

- What skills and knowledge should people in any respective field have, and how should that be acquired?

- What are proper ways to address the mix of education methods, industry practice, and government needs over a lifetime of work?
- What elements are discipline specific and what may be generalized across many areas of professional activity?

An Education Agenda

Academia has long offered "physics for poets" courses in the sciences that explain to non-physicists' concepts of the discipline that may be helpful to know. While requiring that all students take an introductory cybersecurity course would be folly, we do know that some cybersecurity knowledge is a necessity for doctors, lawyers, program managers, civil engineers, social workers, retail managers, schoolteachers, and many, many other professionals. They need to know how to responsibly employ computing technology with regard to cybersecurity in the conduct of their professions.

What needs to occur is determining what knowledge regarding cybersecurity can be imparted within the context of the recipient's professional preparation and career path. We are not suggesting that all students become cybersecurity experts, passing the *Security+* exam or being able to speak intelligently on the Diffie-Hellman key exchange, but rather they learn what's needed through targeted curricula, preferably in courses that already exist. No doubt, skilled experts will be needed to assist the workforce in reinforcing organizational cybersecurity capacity, but more work needs to be done on security behaviors for professionals employing systems that may be attacked via cyber means.

The engagement needed is between cybersecurity programs and the other areas of education and professional preparation undertaken in colleges and universities. The task at hand is to engage with other academic programs on incorporating cybersecurity knowledge and behavior with appropriate, tailored content by discipline in the context of professional responsibility.

---

[*] "Social Workers." Occupational Outlook Handbook. Bureau of Labor Statistics, Washington, DC, available at: https://www.bls.gov/ooh/community-and-social-service/social-workers.htm.

[†] Bada, M; Sasse, A; (2014) *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?* Global Cyber Security Capacity Centre, University of Oxford: Oxford, UK.

[‡] Wirth, Axel. "The Doctor Is In." *Biomedical instrumentation & technology* 51, no. 6 (2017): 514-517.