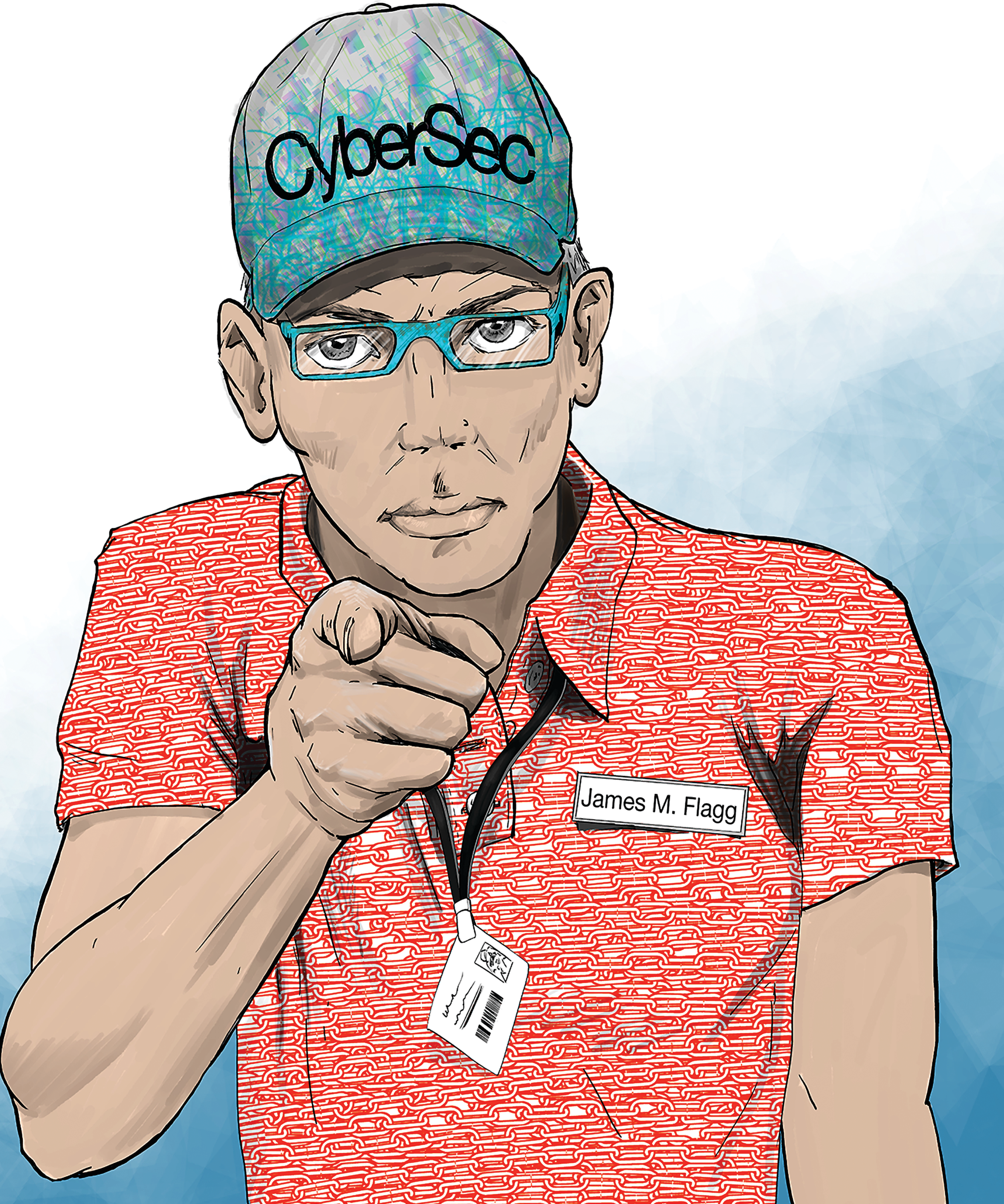
CyberSec
James M. Flagg

Jeremiah D. Still, Old Dominion University

Cybersecurity Needs You!

Insights

- → Cybersecurity needs human-computer interaction designers and researchers.
- → Usable security is possible from a human-centered design perspective.

IMAGE BY AUSTIN G. STILL

Cybersecurity systems are complex. Given the diversity of stakeholders and the variety of system uses, it is unlikely that some magic bullet will eradicate our security concerns. The successful security of our cyber-physical systems depends on corporations and government agencies working together to identify threats, possible future weaknesses, and timely solutions. Some headway has been made in this regard, with cybersecurity committees meeting to create meaningful policies and a platform for confidential information sharing. However, many of these initiatives focus on systems and technology, without addressing well-known user compliance issues. This negligence is due not to a lack of interest or need, but rather to a lack of experience. As such, the multidisciplinary perspective naturally found in HCI is a great fit for designing cybersecurity systems.

Users have been identified as one of the major security weaknesses in cyber-physical systems [1]. They click on things they ought not to click on and grant systems authority without knowing they have done so. Clearly we users are unaware that our inappropriate behavior carries real consequences. Negative outcomes seem distant from our inappropriate actions. In addition, we may feel that current security policies are unreasonable, given the negative impact they have on our daily goals, personal or work-related. For example, you might share your password with a colleague to quickly share documents. Engaging in this behavior saves everyone time and conveys an implicit message of trust to your colleague. These users do not act with malicious intent. Regrettably, this does not stop cybersecurity professionals from describing their system users as "the enemy" [2].

How has the user become the enemy? I believe a confluence of factors—uncertain consequences, use history, system expertise, and shared responsibility—have contributed to this position. Traditionally, we have blindly depended on technology experts to keep us safe. They regulate what you can download and install, what systems you can access, what files you can share, and what you can access outside an individual device. But the nature of networks has changed, allowing us to bring our own devices and services. Further, we have unique usage needs and authority levels. These changes make compartmentalization a nearly impossible task for network administrators. As the environment evolved, so did expectations for the users. We now all have an active role to play in digital security.

It seems, though, that some users do not know they have this role and that those who do know may not have the tools at their disposal to be effective in this role. The technical environments we operate in do not facilitate a clear understanding of risk [3]. This ambiguity could lead users to an apathetic view of security (e.g., it won't happen to me; I'll just change my password) and difficulty knowing their personal responsibility. For example, I do not think about my company's "bring your own device" (BYOD) policy when selecting a flashlight application. I'm thinking, *its dark, and I can't see what I'm doing—oh, cool, a free flashlight app—yes, yes, to all the required permissions screens to progress toward use*. And after use I don't think, *oh geez, I ought to remove the flashlight app because it is potentially dangerous*. I don't even think about the flashlight app until I need to use it again.

Those of us who do understand the risk and our role in risk management face additional challenges. Historically, security-related features were buried deep in advanced menus. Even the training and interfaces we are presented with contain technology jargon, making us feel incapable of maintaining security within our digital world. For instance, online learning modules focusing on security often reference technical things like firewalls, with no explanation of what those things are or how they are used. If the user doesn't know what a firewall is but is able to pass the module, how have they learned to protect themselves or the systems they work with? Of course, there will always be individuals who do not understand the intricacies of computing systems and security (in fact, some still don't know what a browser is), but these training programs should provide basic instruction (e.g., how to configure a firewall) that most users can understand.

If we are to take the perspective that users are one of the greatest risks to system security, we also must accept that users are one of the greatest hopes for system security. This perspective dictates that designers explore how compromising behavior can be designed out of the system (see also: life-critical systems design). This means that interactions need to be supported by appropriate mental models and increased transparency—how else could we hope to make good decisions? It might appear that users are the enemy, but in reality we do not intend to endanger ourselves, family, friends, or employers. The design community can help communicate this message—that users are not acting maliciously but rather simply trying to fulfill their work and personal-life needs within a complex system.

If we are to take the perspective that users are one of the greatest risks to system security, we also must accept that users are one of the greatest hopes for system security.

A HUMAN APPROACH TO SECURITY

In light of the increasing role individual users play in cybersecurity, it is time for cybersecurity professionals to reframe the problem space. Instead of focusing on what we shouldn't do (e.g., click links in suspicious emails), why not focus on what we *should* do to safely use a system? This is an opportunity to empower users! One step in this direction would be to provide meaningful security training. While digital security training has become standard in many professions, there are clear shortcomings. As mentioned earlier, some training modules do not seem particularly well suited to training, as they lack a teaching component and present content at a level that is too abstract. Another indicator of a poorly designed training module—that is, one that overlooks the individual learner—is one that has all users in a company complete the same training. In some cases, these training modules look more like credential systems whose purpose is to satisfy legal constraints (e.g., responsibility is mitigated if all employees pass a test).

A final but no less important concern is the practices encouraged in training programs. It is vital that the best practices communicated truly are best practices. For instance, in training you might be taught that you must create strong passwords. Technically speaking, password strength is determined by a bit-strength calculation that assumes the entire password space is used—the 95 characters found on a typical keyboard, 26 uppercase and 26 lowercase letters, 10 numbers, and 33 special characters. For instance, a strong password like "1cQdbxe"

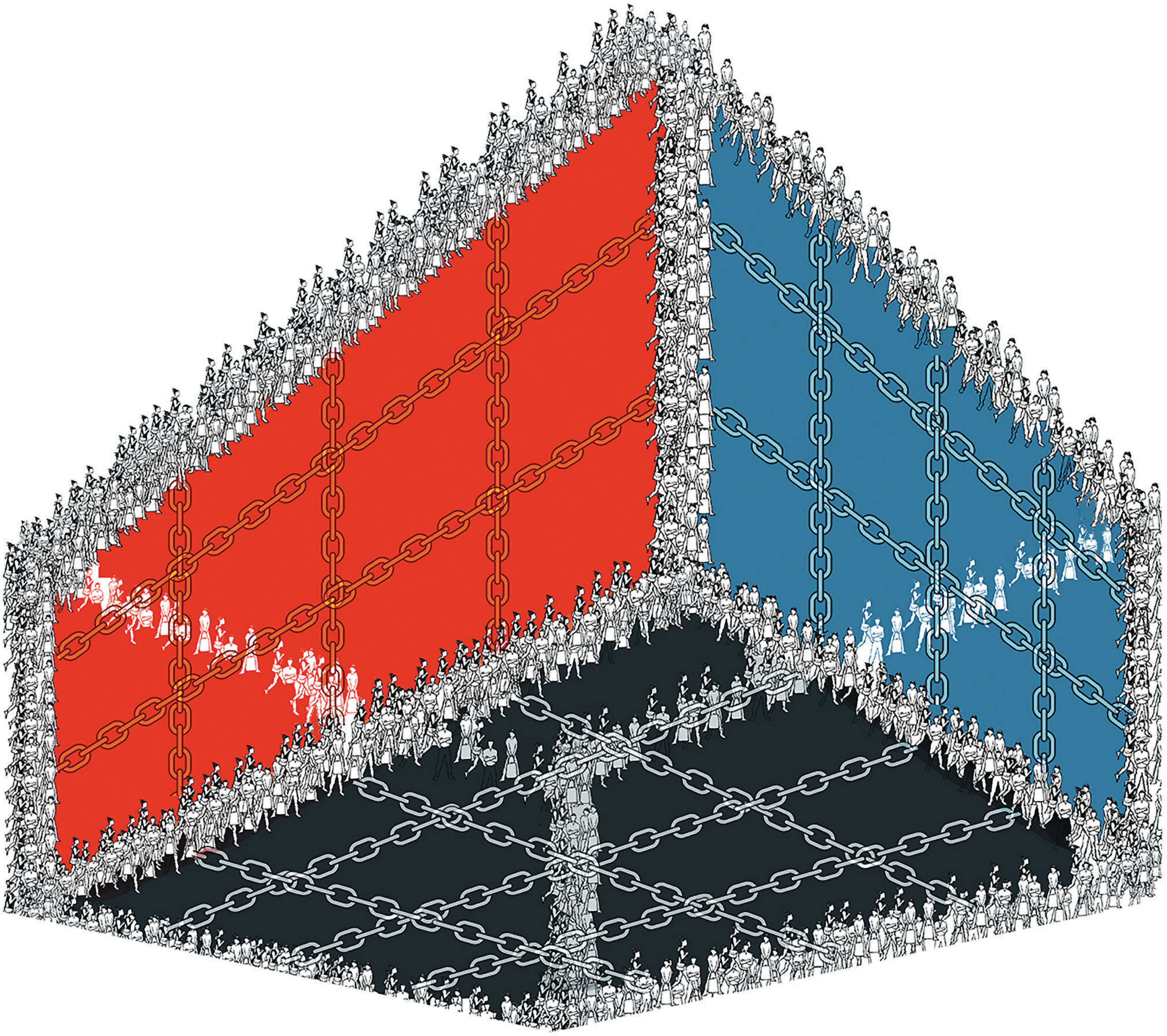

IMAGE BY AUSTIN G. STILL

employs seven characters, upper and lowercase letters, and a number. This password is approximately 41.7 bits. Of course, we do not use the entire space; we select passwords that are familiar, memorable. Which password would you remember, "1cQdbxe" or "1Monkey"? The latter password is potentially meaningful; therefore, it is easier to store and retrieve from long-term memory. The former could be assigned meaning, but that takes additional effort to store and it is retrievable only with sufficient memory cues. Unfortunately, the possible password space may be further reduced when users are required to use strong passwords that must also be frequently replaced. In short, while there is clear instruction on how to develop a stronger password, those instructions stack the deck against successful user implementation. And unfortunately, learning to make a strong password will get you only so far. Bit strength measures how long it would take an attacker to crack a password by brute force, trying every possible combination. But hackers rarely use this approach anymore. It is much quicker to use a method such as social engineering (e.g., gather personal information through social media to make educated guesses) or hybrid dictionary (e.g., using achieved databases of common passwords). By considering the user—what they know, how they use the system, what their needs are—designers will be better positioned to empower them in their digital security role. Clearly, there is a direct relationship between security and usability.

To this point, I have limited discussion to the end user. But, there is also a large need for improving system experiences for professionals [4]. For instance, many intrusion detection systems (IDS) have professionals compare strings of text all day long to find potential threats. I wish I were kidding. In the cybersecurity domain, the majority of researchers are focused on technical development. We need designers and researchers to discover human-centered solutions if we hope to advance overall system performance.

Researchers have been discussing and exploring the domain of usable security for over three decades [5], but recently there has been rapid development. One example is the advent of the Symposium on Usable Privacy and Security (SOUPS) annual meeting in 2005. The ideas emerging from SOUPS have increasing influence in the field. A major topic has been authentication interface design. Essentially, the authentication process is intended to verify who you really are. It does so by asking for an identity (i.e., something that represents you like an email address, phone number, or fingerprint) and validates that identity with a known secret (i.e., something only you know, like a password, "OpenSesame"). There are challenges in both aspects of the authentication process; in fact, researchers have been working to develop a replacement for alphanumeric passwords for over 15 years [6]. Clearly, strong traditional passwords are marked by a lack of memorability. By acknowledging this challenge from a user perspective, researchers are finding ways to create secure but useable authentication systems. For instance, a variety of graphical password systems have been presented to solve this memorability issue because pictures are more easily remember than words. In addition, these systems can utilize recognition processes (e.g., select items from those presented) as opposed to the more laborious task of recalling and generating an exact response. Of course, these new authentication approaches introduce their own unique difficulties. For example, logging in with a graphic passcode typically takes more time (efficiency issue) and is more vulnerable to over-the-shoulder attacks (security issue). These challenges are to be expected in any new area of development.

HCI AND CYBERSECURITY

We need more researchers at the intersection of HCI and cybersecurity. It is important to recognize that advances in cybersecurity require consideration of both technology and human behavior. Information needs to be both secure and usable. Although it is accepted that gains in usability come at a cost in security, this assumption should be tested. HCI researchers are poised to take on the challenge, providing case studies of usable security. Armed with this evidence, HCI researchers will have a more influential voice in cybersecurity. And beyond these case studies, the field needs more theory work to provide guidelines and principles to follow. If not, technology-focused professionals will try to find practical solutions that may not consider what is practical for the user. Consider a recent solution for spear-phishing attacks. In this situation, a user might receive an email that appears to be from a trusted source (i.e., one's bank or school) asking for personal information (i.e., credit card number, password). In reality, the message is from a criminal hacker who is attempting to steal personal information. The attack is successful if the user offers personal information, often after clicking a link and navigating to a page that requests said information. Recently, I heard that a government agency solved this problem by removing clickable URLs from email messages. If a user can't click any links, surely that will protect her from spear-phishing attacks. Undoubtedly, however, such a user will find workarounds to access the URL. In the meantime they will be prevented from clicking all URLs embedded in email, even legitimate ones. It is easy to see how this security measure is viewed as just another awkward software interaction. What other technical solutions are there to increase security? Perhaps USB flash-drive ports are the next to be disabled.

Cybersecurity is evolving quickly and has a limited human-centered foundation. I've identified only a handful of areas that are ripe for HCI contributions. In addition, more researchers with diverse backgrounds are needed. It does not appear that technological advances alone can solve the challenges faced in cybersecurity. Both professionals and users need better situational awareness of the current security environment. For instance, we need interfaces that help professionals detect possible attacks in real time. And we need to provide them with the tools to make them aware of the current situation with informative and persuasive design. While we might not stop well-resourced experts, at least casual attackers using conventional approaches ought to be reportable.

In the past, cybersecurity has been treated as a trade secret, effectively limiting collaborative advances. The understanding of prevalent cybersecurity threats that can have profound negative effects is starting to change this culture. While this secrecy can create challenges for advocating, researching, and designing within the domain, they also make this research extremely rewarding and ripe for discovery. By following a human-centered design approach, we will see discoveries that improve system effectiveness and satisfy stakeholder requirements. Labeling users as the problem is not a solution—this displacement of responsibility takes a costly toll on our economy and on our safety. There are many cybersecurity research opportunities available today (e.g., visualization of attacks, authentication, interactions with automation, persuasive training, understanding mental models of permissions/authority/policies, situational awareness) and into the future (e.g., cyber teamwork). Please consider contributing your expertise to the next generation of cybersecurity systems.

Endnotes

1. 2013 Data Breach Investigations Report; http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf
2. Vidyaraman, S., Chandrasekaran, M., and Upadhyaya, S. Position: The user is the enemy. *Proc. of NSFPW*. 2007, 75–80.
3. West, R. The psychology of security. *Communications of the ACM 51*, 4 (2008), 34–40.
4. Gutzwiller, R.S., Fugate, S., Sawyer, B.D., and Hancock, P.A. (2015). The human factors of cyber network defense. *Proc. of HFES*. 2015, 322–326.
5. Theofanos, M.F. and Pfleeger, S.L. Shouldn't all security be usable? *IEEE Security & Privacy* 9 (March + April, 2011), 12–17.
6. Biddle, R., Chiasson, S., and van Oorschot, P.C. Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys 44*, 4 (2012), Article 19.

Jeremiah D. Still contributes to the Center for Cybersecurity Education and Research at ODU by providing a human-centered perspective. His research is driven by a desire to help designers make products better. He achieves this by focusing on how users cognitively perceive, process, and respond to interfaces.
→ jstill@odu.edu

DOI: 10.1145/2899383 © 2016 ACM 1072-5520/16/05 $15.00