I intend to share my ideas from an information science perspective to address the question that has perplexed cybersecurity researchers and educators: “How do we get more US citizens—and a more diverse population —into cybersecurity in meaningful ways?”

The smart innovations ranging from wearable devices to smart homes to cars to medical devices have become part of our daily life and continue to shape our behavior in the foreseeable future. According to 2018 Global Megatrends in Cybersecurity by Ponemon Institute, 82% of IT practitioners predicted a data breach from unsecured Internet of Things (IoT) devices is very likely to occur in the subsequent years. However, a recent cyber-security knowledge survey by Pew Research Center reported most Americans had limited cyber-security knowledge, which implies that those with smart devices connected to the Internet are at higher risks of cybersecurity threats. While most Americans have limited knowledge about cyber-security concepts (like strong passwords and risks of public WiFi network), most of them are unfamiliar with the key technical cyber-security concepts, such as botnet, VPN, and two-factor authentication (Olmstead and Smith, 2017). This reveals the fact that there is an urgent need to increase the cyber-security knowledge level of general public in the United States.

Extending Existing Stop-Think-Connect Model to a Complementary Education Model for the Public: Learn-Think-Change

"Leaning without thinking leads to confusion; thinking without learning ends in danger." ~ Confucius

In 2010, President Obama designated October as National Cybersecurity Awareness Month. The Department of Homeland Security (DHS) has initiated the national campaign and promoted partnerships between public and private sectors using the hashtag #cyberaware. Apart from that, a cybersecurity awareness program, entitled Stop-Think-Connect from DHS, has been adopted as a cybersecurity education model for community colleges (Fernandez et al., 2016). Inspired by this model, I suggest considering how learning and behavioral change theories/models can contribute to creating a complementary education model of cybersecurity literacy, namely Learn-Think-Change, for the general public.

(1) Learning Cyber-Security Knowledge and Public Opinion of Cyber-Security Awareness on Social Media

Many scholars have been investigating the professional knowledge trends in cyber-security research based on scientific research publications. However, few efforts have been put into mining user-generated content relevant to cybersecurity knowledge exchange on social media platforms. It would be meaningful to monitor the informal knowledge and resources shared through the hashtag networks in social media-enabled electronic networks of practice (eNoPs). eNoPs refers to geographically dispersed virtual communities with members who may never meet each other but share the same professional interests and publicly exchange information, advice or resources online. Social media enables eNoPs to informally exchange knowledge across boundaries in a timely manner (Beck, Pahlke, & Seebach, 2014). Taking the healthcare field as an example, Healthcare Hashtag Project is an open platform for connecting healthcare stakeholders (i.e., patients, caregivers, advocates, doctors and other providers) to timely information on Twitter. Hashtag networks link social media enabled eNoPs among professionals with diverse backgrounds to a variety of information resources, including questions and answers, news, hyperlinks, videos, images, and so on. I think it would be helpful to have one similar initiative, Cybersecurity Hashtag Project, for connecting cybersecurity stakeholders and communities through hashtag networks to organically create a substantial knowledge base. Such an initiative has the potential to engage and influence both cybersecurity curriculum across disciplines as well as life-long continuing education for the public.

(2) Thinking about Cybersecurity Risks and Risk Information Seeking

Cybersecurity behavior is always a choice. People can choose how they respond and react to cybersecurity challenges. What cybersecurity behaviors and choices will serve people best depends on their cybersecurity risk perceptions and how they view and cope with cybersecurity risks. Human information behavior could serve as a bridge to understand how people seek, process, and share cybersecurity risk information to bridge their information and knowledge gap. Integrating the concept of risk communication from the field of communication and information behavior from information science, the risk information seeking and processing (RISP) model (Dunwoody and Griffin, 2015) appears to be an appropriate framework to discuss the factors influencing how people seek and process risk information to bridge their knowledge gap. It is worth noting that information insufficiency and informational subjective norm are the significant predictors that drive people's risk information seeking through different information channels. Though the RISP model was originally developed to examine motivations behind information

seeking and processing behaviors on mass media, the recent studies have shifted the focus to social media. Therefore, cybersecurity professionals could use this model to rethink their role in educating the public and influencing other professionals about seeking and acquiring cybersecurity risk information. Leveraging the perceived social influence from social media could be a meaningful way to motivate the public's desire to be informed pertaining to cybersecurity risks. As a result, risk information seeking plays an essential role in motivating people to make corresponding changes when facing cybersecurity threats, thus leading to an informed understanding of cybersecurity risks.

(3) Changing Cybersecurity Information Behavior by Choice Architecture Design (Digital Nudge of Secure Online Behavior)

Cybersecurity incidents will change the ways in which the public responds to and communicates about cybersecurity risks. Raising the awareness and knowledge level of cyber-security is the first step to trigger the cybersecurity behavioral change. Various approaches can contribute to intervention design of cybersecurity awareness and literacy. The successful experience of motivating health behavior change using choice architecture may be replicated in the field of cybersecurity. From the perspective of behavioral economics, Thaler and Sunstein (2008) proposed the notion of choice architecture and defined it as the presentation of choices that nudge user decisions. Since choice architecture aims to affect behavior change without forcing people to accept but informing them of potential choices, it considers impact evaluations of informative presentations. In the digital world, the concept of digital nudge has been proposed to provide "a sort of compass to help individuals navigate a world of choices" (Schüll, 2016, p. 303). Similar to the IRS tax map built on semantic integration and topic maps, a cybersecurity map combining different knowledge mapping tools (e.g., mind maps, concept maps, and topic maps) could be developed. Such a map can assist users in searching and navigating cyber-security and privacy concepts by providing decision aids for their tasks relevant to changing the security and privacy settings of their smart devices.

Summary

Social influence through social media is one of the characteristics that we could leverage to change public perception and human information behavior about cybersecurity risks. Information

professionals can help design interventions using choice architecture to address users' information needs. This could mean designing effective information architecture for websites and mobile applications or providing an integrated knowledge mapping tool to facilitate learning and conveying cybersecurity concepts. In this way, users can learn where to find more cybersecurity information and locate their needed resources in a timely manner.

Author's Bio Sketch

Hsia-Ching Chang is an assistant professor in the Department of Information Science, College of Information at the University of North Texas. She is affiliated with the Center for Information and Cyber Security (CICS) at University of North Texas. She received her PhD and MS in information science from the University at Albany, State University of New York as well as her MA in public policy from the National Taipei University in Taiwan. Her research interests concentrate on cybersecurity, data analytics, social media, knowledge mapping, scientometrics, information architecture, and information interaction. She got the Cloud Security Alliance's CCSK (Certificate of Cloud Security Knowledge) certified, the first IT certification for secure cloud computing. She has been teaching the graduate-level course, Information and Cybersecurity, since 2015. She is the co-editor of the new book "Analytics and Knowledge Management" in Data Analytics Applications Series published by CRC Press, Taylor & Francis Group. She is currently co-editing a book entitled "Cybersecurity for Information Professionals" to be published by Libraries Unlimited, ABC-CLIO in 2019.

References

Beck, R., Pahlke, I., & Seebach, C. (2014). Knowledge exchange and symbolic action in social media-enabled electronic networks of practice: a multilevel perspective on knowledge seekers and contributors. *MIS Quarterly*, 38(4), pp. 1245-1270.

Dunwoody, S., and Griffin, R. J. (2015). Risk information seeking and processing model. In H. Cho, T. Reimer & K. A. McComas (Eds.), *SAGE Handbook of Risk Communication* (pp. 102-118). Thousand Oaks, CA: SAGE Publications.

Fernandez, B. R., Garcia, C. A., Capriles, J. R., Ford, W. & Mooney, C. (2016). Building Bridges: From NSF I-Corps to Community Colleges – Cybersecurity for All. *National Cybersecurity Institute Journal*, 3(2), 11-23.

Olmstead, K., & Smith, A. (2017). Americans and cybersecurity, *Pew Research Center*. Schüll, N. D. (2016). Data for life: Wearable technology and the design of self-care. *BioSocieties*, 11(3), 317-333.

Thaler, R. H., & Sunstein, C. R. (1999). *Nudge: Improving decisions about health, wealth, and happiness*. New Haven, CT: Yales University Press.