Lessons Learned by Our Editorial Board

Shari Lawrence Pfleeger | Editor in Chief

Collectively, *IEEE Security & Privacy*'s editorial board has deep and broad expertise and experience in all aspects of security and privacy matters. From government service to research to application development, our editorial board members work year after year to suggest topics, solicit articles, and oversee the rigorous review process that leads to high-quality articles written in interesting, accessible language. In addition, some members oversee *S&P*'s various departments, provide quality control for invited articles, and ensure that the content appeals to our three types of readers: practitioners, researchers, and policymakers. They do all this and also work at their day jobs and spend time with friends and family. We couldn't produce this magazine without them!

At our 2014 editorial board meeting, we invited editorial board members to share what they had learned during their fruitful careers. As a result, this special issue on lessons learned includes two articles from authors with experience as educators, authors, practitioners, and researchers. In "Quantitative Risk Analysis in Information Security Management: A Modern Fairy Tale," Rolf Oppliger shares his observations about measuring and managing risk in information security. His suggestions reflect his long career as professor at the University of Zurich and as founder and owner of eSECURITY Technologies. Oppliger shows us the significant gap between what textbooks tell us about risk and the realities of capturing meaningful information to inform our security decisions and designs.

Similarly, Charles P. Pfleeger's discussion of our difficulty in anticipating how our software will be used is based on his professorship at the University of Tennessee as well as activities at security consulting firms, telecommunications giants, and ultimately his own security practice. In "Lesson Learned: Security Is Inevitable," Pfleeger emphasizes the need to document not only

 Copublished by the IEEE Computer and Reliability Societies

what our products can do but also what they can't and shouldn't do, so that we implement security and privacy controls responsibly and well.

We supplement these articles with three examples that illustrate Oppliger and Pfleeger's reflections. The first, "Toward Economic-Aware Risk Assessment in the Cloud," by Valerio Bellandi and his colleagues, discusses the difficulties of monitoring risk in the cloud. The authors show how to use microeconomic analysis to inform and improve risk-based comparisons of security strategies.

The second article, "Mitigating Risk with Cyberinsurance," by Per Håkon Meland, Inger Anne Tøndel, and Bjørnar Solhaug, emphasizes our inability to predict the future. The authors suggest that cyberinsurance can address some aspects of the chasm between what we think will happen and what actually does.

Finally, in "Privacy Awareness Diffusion in Social Networks," Artemis D. Avgerou and Yannis C. Stamatiou show us how to use close-knit social network graphs to influence users' privacy awareness. This approach draws on techniques from other disciplines, especially economics, and is a good example of how broadening our thinking also broadens our effectiveness.

It's fitting that this last issue of my tenure as editor in chief of *S&P* is both forward thinking and multidisciplinary. Over the past three years, I've expanded the magazine's pool of authors, countries, professions, and disciplines to stretch and grow our readership. My successor, Professor Ahmad Reza-Sadeghi (ahmad.sadeghi@trust.cased.de) oversees a multidisciplinary research group at the Technical University of Darmstadt. He'll continue to solicit thought-provoking, accessible articles from around the world. I encourage you to contact him to discuss what you like about *S&P* and what you think is missing. ■

cn *Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.*