Understanding the needs of cybersecurity;

In cybersecurity, different professionals value different attributes

My previous column in the November/December 2017 issue of *Industrial Management* suggested that how your subject matter expert (SME) thinks should be considered when choosing a decision analysis methodology.

For example, SMEs who have a decision analysis or quantitative background may be able to provide reliable value functions to support a utility model. Those without these backgrounds may respond better to a pairwise comparison or analytic hierarchy process analysis. The engineering manager's goal is to build a model that can aid in decision-making; reliably elicited SME data is a key to success.

In the March/April 2016 issue of this column, I wrote about the need for industrial and systems engineers to contribute to open research questions in cybersecurity. Strong cybersecurity practices include physical, human and digital components, which is a systems approach. Furthermore, human components may require SME input as well as tailoring models and policies to support the network or device being secured. Of course, implementing security practices involves project management.

Both of these concepts – tailoring models to your SME and systems approaches to cyber – come together when we consider value. What do your SMEs consider to be important when securing their cyber systems? Research from my team (Towson University undergraduate student Lorraine Black; Col. Paul Goethals, an academy professor at the United States Military Academy; and James Howard, a research scientist at Johns Hopkins Applied Physics Lab) has identified that values are not consistent and depend on many factors, such as industry, SME background and size of the organization.

We specifically examine two populations: information technology (IT) professionals and attorneys who work at small legal firms or are solo practitioners.

The IT professionals worked in a variety of industries, but many were part of IT services at colleges and universities in the United States. They obviously have experience working in cyber operations and had formal training in cybersecurity. The legal professionals owned their businesses or worked in small firms; for the most part, these professionals had no formal cybersecurity training or operations experience.

Our analysis identified that different attributes were valued when securing cyber systems. For example, IT professionals valued automation, awareness and training in a secure system, while legal professionals valued fraud protection. Both populations valued prevention, threat detection and human behavior, among other attributes. We will be presenting this research at the 2018 IISE Annual Conference and Expo, scheduled for May 19-22 at the Loews Royal Pacific Resort in Orlando, Florida.

Says...

a quick look at the Annual Conference EM track

Our paper is titled "Values and Trends in Cybersecurity."

Cybersecurity works in practice when employees understand risk and their work productivity is not hindered by policy. If processes to secure systems are too cumbersome, employees tend to find ways to circumvent the process and therefore expose more risk to the system. Approaches to take for securing systems vary. Large scale solutions are appropriate for established or high-profile organizations, but less complex solutions may be appropriate for small businesses.

Our goals, as engineering managers, are to understand the needs and values of an organization and tailor solutions to address those needs. Solutions become projects that need to be managed. Employees buy in when they understand the security goal and subsequent processes. Engineering managers need to work together, identify risks and tailor solutions, which will lead to stronger, more secure cyber systems.

— Natalie Scala is an assistant professor in the Department of e-Business and Technology Management in the College of Business and Economics at Towson University. You can reach her at nscala@towson.edu.

Engineering management track updates

We are less than two months away from the IISE Annual Conference and Expo.

The Engineering Management track, which includes innovative research and practice-based solutions focusing on the convergence of the fields of engineering, technology and business, received 89 abstracts. Seventy-six abstracts were accepted. The accepted abstracts cover a wide range of interdisciplinary topics such as decision analysis, operations and supply chain management, manufacturing and service process improvements, performance measurement, change and risk management, organizational behavior and design, team-based work systems, and project management, among others.

The authors of accepted abstracts were invited to submit full papers or extended abstracts. A total of 28 full papers were submitted. Thank you to all the authors and co-authors for submitting full papers.

To maintain quality of submission, we are ensuring these papers are peer reviewed (double blind). Over the next few weeks, EM track chairs will be working very hard to create quality educational sessions.

In addition, SEMS will hold its annual SEMS Town Hall meeting, where officials will update members on the state of the society and plans for the future. Attendees will have the chance to meet and ask questions of the current SEMS board of directors, network with other members and provide suggestions for future activities.

Visit *www.iise.org/annual* for details and to register. We are very excited to see things take shape.

— Niranjan S. Kulkarni is the director of operations improvement for CRB.