SEMS

Industrial engineers are needed everywhere – from unchartered

'Where are the engineers?' applies to customer experience, too

I thought I was ready for anything. Then came a call from a colleague who had just been named the inaugural chief experience officer for a technical solutions and business services company.

Researching the field of customer experience yielded an enormous quantity of information but no scientific body of knowledge. Critics say the field suffers from a high "rhetoric to results" ratio. Examining customer experience programs yields mostly anecdotal accounts about a basket of interventions, but rarely can folks explain the scientific foundation of an idea or predict its effect.

I wondered, "Where are the engineers?"

For customer experience to be a true business discipline, not a fad, it must grow up. We spent more than a year developing a suite of core principles, enabling frameworks, customer data gathering and analysis methods, and communication tools.

We founded everything on original customer research. We replaced the age-old practice of insider stakeholders "putting their customer hats on" by insisting on listening to customers, thinking about what they said and then building solutions. Customer events previously accomplished via PowerPoint became open-ended listening and observing events, often with more authentic customer insights acquired in a day than over months and years under the old ways.

With a solid conceptual foundation, we are expanding the scope and taking our methods out to the front lines. Associates are learning basic listening and analysis techniques right out of the industrial engineers' playbook and applying them to customer problems. Customer-sourced evidence is becoming a requirement in any conversation, and improvement efforts are becoming more rigorous and based on scientific, body-of-knowledge content.

Looking back, the inherent sense of the customer experience vision was clear. However, we arrived at several core conclusions: The industrial engineering perspective was absent, i.e., the design of integrated systems based on customer needs; there was a lack of data-driven engineering processes framed by science and core principles; and there was no body of knowledge to inform the design process, and, therefore, no basis to choose interventions, predict results or describe the ROI.

Takeaways: Engineers are vital to any client problem; engineers have unique perspective and tools that make them vital in unchartered waters; solving the client's problem may require a deep dive into the unknown, and engineers have the background for that and should not be shy; and engineers should actively seek new domains.

So next time you find yourself in unchartered waters with only a distant star for reference, first ask, "Where are the engineers?"

— Jerry Seufert is an independent consultant based near Atlanta. He has an M.S. in management engineering from Rensselaer Polytechnic Institute.

Says...

waters to cybersecurity

Cyber as an emerging area for industrial engineers

One of the most exciting aspects of being an industrial engineer is the ability to enact real change through continuous improvement initiatives, especially when opportunities arise in emerging areas such as cybersecurity. Although computer science and network infrastructure research have dominated this realm, IEs are ready to make their contributions.

Science of Security (SoS), sponsored by the National Security Agency, is a transdisciplinary open access research initiative that aims to provide scientific understanding and predictive principles to make the cyber world more trustworthy and secure. SoS organizes cybersecurity policy and research into "The Five Hard Problems": scalability and composability, policy-governed secure collaboration, resilience, human behavior and metrics. Each problem has risk, optimization and decision analysis components where IEs can contribute solutions.

For example, researchers at the U.S. Military Academy's Army Cyber Institute are performing a within-domain (offensive and defense cyberspace operations) and cross-domain (social sciences, privacy, behavioral sciences, engineering, medical) study of the strengths, weaknesses and gaps within the domain of big data research. Data analytics, decision analysis and optimization play a role in this research. In particular, Col. Paul Goethals is using the findings to challenge the current state of intrusion detection systems, where IE tools and techniques could enhance performance or improve their capability.

Examples from industry include the Cyber Risk Assessment Foresight Tool (CRAFT) in development by Innovative Decisions Inc. CRAFT will help banks field a network during design and acquisition with a reduced probability of being exploited. It also will provide regulators with a tool to support board-level discussions with regulated institutions on cybersecurity and the critical importance of cyber resilience to financial services. Another example is the Cyber Risk Index Model sponsored by the Carnegie Mellon University Software Engineering Institute Computer Emergency Response Team. This model can be used as an objective measure to determine cybersecurity event/data loss protection premiums, as well as an internal measure to gauge cyber risk posture.

I am part of a research team examining metrics and best practices indexed by the SoS initiative. We are developing a value model to enable organizations to identify preferred metrics and best practices based on current cyber posture, operating environment, workforce savvy, etc. Engineering managers can apply the model framework with values from their organizations to identify a ranked list of metrics and best practices for their firms. My team is looking for subject matter experts from a variety of industries; please contact me if you are interested.

This is an exciting time for IEs to get involved in cyber applications.

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