It’s evident that we’ve accomplished many things during the magazine’s first four years. S&P has assumed a key role in the computer security and privacy arena, filling the sizeable gap between non-peer-reviewed trade publications and highly reviewed transaction-style research journals. Even the mass market media, such as The New York Times and National Public Radio, have highlighted our articles, underscoring our impact on the broader consumer community.

We knew up front when starting this magazine that a silver bullet wouldn’t solve the security and privacy challenges we face. What we needed was a larger community of talented people who could accelerate the development and deployment of solutions through the rapid and open exchange of ideas. History has proven us right: five years ago, the acknowledgment of security problems by vendors and the recognition of privacy issues by industry, government, and consumers were spotty at best. Today, security and privacy are mainstream and high on everyone’s agenda.

Naturally, several factors have contributed to this change in attitude (such as 9/11), but S&P has played an important part too, by delivering understandable messages to an increasingly larger audience. We’ve cut through the layers of hype, hysteria, and indifference to expose many real issues and disseminate promising solutions that could address those issues.

So what’s ahead of us for the next four years? Obviously, as we harden some components, others will become the weak links in the system and therefore the new targets for attackers. It’s notoriously difficult to harden people, and I suspect we’re going to see more varieties of increasingly sophisticated attacks on the cognitive channels between people and their computing systems. By this, I mean social engineering, phishing, spyware, configuration mismanagement, and the deliberate distribution of content meant to manipulate user behavior.

Moreover, as we deploy networked information systems to broader domains and communities, the user and system administration bases continue to grow to include essentially everyone. Although we can isolate the effects of some attacks to a certain extent (such as a phishing attack on an individual), we all feel the damage eventually through liability insurance and institutional losses.

Such challenges go beyond purely technical solutions. Maybe we’re growing up as a discipline—usability and human factors have long been major concerns in other areas of engineering but we’re only just getting there ourselves.

Whatever the future holds, I envy my successor, Carl E. Landwehr, for being in the thick of things as he moves ahead into this uncharted territory. Best wishes to Carl and my sincerest gratitude to a remarkable crew of lively, talented, and dedicated editors, staff, and contributors who have made these past five years so rewarding for me. Thanks! ☺