In striving to build a secure information infrastructure, we’re all trying to develop patterns of local behavior.

Sandy gave me her employment history without ever asking who I was or why I wanted it. She might have assumed that anyone at the party could be trusted, but more likely she was distracted by the sudden absence of her son, Darrin. Just a moment before, he had been tugging at her hand and uttering that universal plea, “Mom, Mom, Mom, look!” and then he was gone.

The apartment was more crowded than it probably should have been, and the room held many objects tempting to an energetic young boy and his new-found compatriots. “He’s a good boy,” she said, “but he needs constant monitoring for his own safety.” I added, “And he always will,” which drew a little smile.

Sandy started explaining that she was in charge of cybersecurity for a large government agency. She had come to her position with no special training, having received a bachelor’s degree in English literature. “No one knew anything about cybersecurity when I started my job in the 1990s,” she said, “so we had to invent it all by ourselves.”

As Sandy shared stories about how she had developed policies for her agency and trained her staff, we watched her son move through the crowd. He was filled with energy that left a trail of minor disruptions in his wake—a lamp tipped off the table, a plate of food placed on a bookshelf, a rug kicked into a ball. He wasn’t particularly interested in the adult environment, just as Sandy didn’t seem especially concerned with the context of her career.

Sandy may have created the cybersecurity office within her agency but others were developing the framework in which she worked. Members of this society invented the methods of cybersecurity. Congress began to impose cybersecurity strategies in 1987, and the National Institute of Standards and Technology created two documents that set minimum security standards for government systems.

I tried to engage Sandy in a discussion of the bigger issues of cybersecurity but she was distracted by her son, who was making his way through a crowded apartment. A couple of times, she was clearly inclined to call, “Watch out!” and urge him to pay attention to his surroundings. Others, however, were closer to him and guided the little boy away from danger. Sandy clearly wished that Darrin was a little more observant and behaved in a slightly more disciplined way.

If Darrin served as the metaphor for his mother’s career, then he suggests that we’re in the position of training our clients to be aware of threats against the information infrastructure and are trying to help them develop the skills that will protect them. The task is a bit overwhelming, and we’re always grateful for extra hands that provide extra protection.

Our conversation ended when Darrin brought himself too close to danger and was saved with little room to spare. As Sandy left, she surprised me by saying that it was nice to talk with someone from the IEEE who understands cybersecurity. Before that moment, I had thought that she had not realized that I was involved with computing technology. Apparently, a good cybersecurity professional is always paying attention to context, always assessing the situation, and always taking steps to stay out of trouble.

David Alan Grier is the author of many books including the recent The Company We Keep (IEEE CS, 2012). Contact him at grier@computer.org.