The following is an excerpt from an interview with Bruce Schneier. Matt Pasiewicz, EDUCAUSE content program manager, conducted the interview at the EDUCAUSE 2007 Annual Conference. The full podcast is available at http://connect.educause.edu/blog/mpasiewicz/e07podcastaninterviewwith/45439.

MP: Bruce, perhaps you can get us started by sharing some of your thoughts about the psychology and economics of security.

Schneier: Security is a lot more about people than technology. One thing I’ve learned from studying economics, the psychology of risk, security, and people is that those problems are actually way harder than the tech problems. We have as much technology as we need, but securing the people end is hard. I’m doing a lot of research in psychology right now. People are very complex: they’re not linear and rational, and they’re not computers at all. We try to think of them as logical and rational, and that’s just not true. People have internal contradictions. . . . No matter how good the tech is, if we don’t solve the human end, it’s just not going to work.

MP: What can we do to educate ourselves and our users when the experiences often aren’t as contiguous as those events that we seem to learn from most quickly?

Schneier: The answer is, really, nothing. There’s nothing we can do to educate users, and anyone who has met an actual user knows that. Users are going to pick up their knowledge from their experiences. You can try to teach them stuff explicitly, but it’s not going to stick in the same way that experiences do, and unfortunately, the experiences often don’t match our reality, whether it’s an experience of fear, an experience of an attack, or an experience of no attacks. Rather than focus on what can we do to educate users, we need to focus on building security that doesn’t require educated users. That will be much more resilient, because while there are some educated users, there are a lot of noneducated users. . . . For example, my mother is never going to be a security maven—not because she’s stupid but because it’s not her area of expertise. And we can’t expect it to be. If I say, “Look, Mom, you didn’t know enough to do this and that, and you deserve to get hacked,” I think that’s blaming the victim. . . .

MP: In 2006, you wrote a Wired article titled “The Eternal Value of Privacy.” To what extent do you project that the problem of privacy will get worse over the coming years? In an era of mash-ups, widgets, and service-oriented architectures, should we pause before embracing the new forms of innovation, or should we believe Scott McNeely, who reportedly said in 1999: “Privacy is dead; get over it”?

Schneier: The death of privacy has been predicted forever. . . . Simson Garfinkel wrote a book. Robert O’Harrow wrote a book. David Brin wrote The Transparent Society. You can go back to 1969 and a book by Jerry Rosenberg: The Death of Privacy. We’ve been saying this for generations, but it turns out it’s not necessarily true. Technology might limit privacy, but just because cameras have been invented, that doesn’t mean naked pictures of you appear everywhere. We are a nation of laws, and laws protect us in places that technology doesn’t.

Certainly technology is moving away from privacy. Your cell phone knows where you are at all times. That’s how it delivers phone calls. It also knows who you call, and it knows your text messages. More data is collected every day: your credit card, all of the cameras that are out there, automatic fare collections, anything you do on the Internet. So there is this inherent lack of privacy. But what happens to that data? Who is allowed access to it, how it is stored, how it is deleted—this is all a matter of laws. So where technology doesn’t protect us, laws have to.

MP: Do you foresee a pendulum swing over the coming decades, or are we going to continuously encroach on privacy as we know it today?

Schneier: I think it is going back and forth. We’re living in an era right now in which, in some misguided attempt to make us safe from terrorism, we are putting ourselves at risk to all sorts of other things. There is this massive loss of privacy that’s happening everywhere. That’s going to change. That’s not going to make us safer from terrorism, and it’s going to cause lots of other risks. Eventually, maybe in ten or twenty years, we’re going to have comprehensive data-privacy laws in this country and in most other countries.

I take solace in a quote by Martin Luther King Jr.: “The arc of history is long, but it bends toward justice.” Things happen slowly, but they are getting better. One hundred years ago, half of us couldn’t vote. Two hundred years ago, some of us were slaves. Things do get better. They get better slowly.

MP: At DEFCON 15 in August 2007, you noted that data is the pollution of the information age. Can you elaborate on that?
Schnieer: That's a good metaphor. Data is the pollution problem in the information age in the same way that pollution was the pollution problem in the industrial age. All processes today produce data. Every computer process produces data. Data stays around.

Data festers, and how we deal with it—how we recycle it, reuse it, dispose of it, what the regulations are concerning it—is central to the information age. Just as in the industrial age, we're largely ignoring the problem in a rush to get new technology, and twenty, thirty, fifty years from now we're going to be cleaning up massive data problems—just like we're cleaning up massive pollution problems today.

There is a notion of data decay, and some people have written about the fact that computers should be programmed to forget things, that remembering stuff forever is not necessarily good. That's a very complex, really philosophical issue, and there is no time to go into it now, but it is well worth thinking about... There are some really good thinkers thinking about what it means to live in a society where people never forget. This is the first time in the history of our civilization that we've had that possibility. Is that a good thing or not? I don't know.

**MP:** Many CIOs and ISOS are struggling with how to measure the success of their security programs. Are there metrics or methods that you recommend for demonstrating success to upper management?

Schnieer: This is hard. The hard part about demonstrating success is the lack of data, so one of two things happens. You have a good security program, and you don't get hacked. Is that because you have a good security program or because there's no risk? How do you prove one and not the other? It's very hard without data. On the streets, it's easy; you can go to your police department, or your newspaper, and get the crime statistics for the neighborhood you live in. You know exactly how safe you are.

You can't do that on the net. We just don't have that data, so it's very hard to demonstrate the success of a security program. It's even worse when you're dealing with rare events. If you have an event that happens very, very rarely, did you prevent it, or did it just not happen? We have this problem in our country with terrorism. It is a very rare event, and we do some really ridiculous things to try to prevent terrorism, but it's hard to prove whether these things were effective, because there's no data.

**MP:** Are there any ethical boundaries that we need to start thinking about in relationship to security, privacy, and the professionals who occupy security and privacy positions?

Schnieer: I tend not to rely on ethics. Ethics involve social norms. I like to see economic incentives. I think they work better than social norms. Social norms do work. There is less bicycle theft in Japan because people don't steal your bicycles, so you don't need as good a lock in Japan as you do in the United States. That's entirely a social norm providing security, and you see a lot of that in IT. But if you can get an economic incentive, I think you're doing better.

**MP:** If you could make one call to action for security professionals in higher education, what would it be?

Schnieer: To think of your networks dynamically. We're living in a world where things change all the time, and in universities, things change faster—not just because each year you have a new student body that is doing the new things that they've discovered no one else does, but also because you have, on the other side, the research professors who are doing the new things that haven't been talked about yet. There are a lot of dangers in that, and a lot of additional risks, but there are also a lot of opportunities for you to see solutions and ideas that might not come to the rest of us until a year or two later. So I want people to talk. I want people to write. I think the experiences in academia are things that the rest of us can really make use of. The more I read about your experiences, the better I am.

Bruce Schneier is Chief Technology Officer of BT Counterpane and the author of eight books, including the bestsellers *Beyond Fear: Thinking Sensibly about Security in an Uncertain World, Secrets and Lies, and Applied Cryptography.*