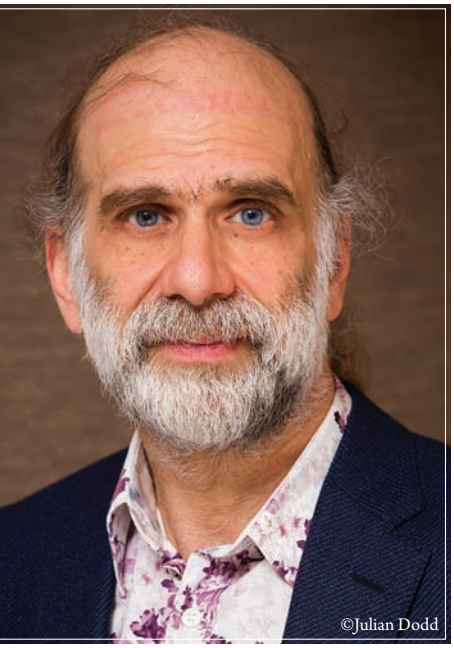

The Internet of Things Will Upend Our Industry

Bruce Schneier
Harvard University

Everything is becoming a computer. Your microwave is a computer that makes things hot. Your refrigerator is a computer that keeps things cold. Your smartphone is a portable computer that makes phone calls. Your car is a distributed system with more than 100 computers plus four wheels and an engine. More alarmingly, a nuclear power plant is a computer that produces energy. This is happening at all levels of our lives and all over the world.

As everything turns into a computer, computer security becomes everything security. This will upend the IT security industry, because our knowledge and experience with computer security will be much more broadly applicable, and the restrictions and regulations from the physical world will be applied to the computer world. The beachhead for all of this is the Internet of Things (IoT), which I liken to a world-sized robot—one that can kill people and destroy property.

When speaking to more general audiences, I list five truisms from our world that are coming to theirs. One: most software is poorly written and insecure—as an industry, we've prioritized speed and price over quality, and security has suffered as a result. Two, three, and four: the extensibility, complexity, and interconnectedness of computerized networked systems make them very hard to secure. Five: the vulnerabilities and failure modes of computers are different from those of the more manual systems they replace.

We know about how computer attacks scale, class breaks, and the dangers of software monoculture. But this comes as a complete surprise to others: from auto and medical-device manufacturers to the companies making low-cost IoT devices like DVRs, webcams, and toys. The cybersecurity skills shortage of today is only going to get worse as these devices' insecurities start causing real-world damage.

Fear of that damage will cause the next big change to our industry: government regulation. The IT industry has mostly been left alone by governments because we've been providing a steady stream of amazing technological innovations that largely didn't affect the world in a direct physical manner. That's about to change in a big way. Even though it's the same OS and maybe even the same vulnerability, there's a fundamental difference between losing your data when a spreadsheet crashes and losing your life when a car crashes.

Once governments start regulating, they tend to have a limited toolbox. They can regulate before the fact (product and category rules, licensing, and testing requirements) and after the fact (fines and liabilities). They can mandate disclosure (product labeling, testing, and forensics agencies). They can also shape the environment by funding research and education or using their procurement to drive improvement. What will work, and how, is unclear—and fraught with fear and anxiety. But it's a conversation we must have.

What will it take? Automobile ransomware at speed? A distributed denial-of-service attack that takes out a power plant? Murder via a medical device? IoT sensors used to identify and arrest a minority group? None of these scenarios is science fiction, and many more of these real-world risks loom in the near future.

Our choice is no longer one of government regulation versus no government regulation. Our choice is smarter government regulation versus stupider government regulation. As an industry, we have to start thinking about the pros and cons of the different approaches so we're not surprised when something is forced on us. We're no longer in our separate IT world. We're part of the real world, and that world is part of us. We need to start acting that way. ■

Bruce Schneier is a security technologist, a Fellow at the Berkman Klein Center for Internet and Society at Harvard University, chief technology officer of IBM Resilient, and Special Advisor to IBM Security. Contact him via www.schneier.com.

Copublished by the IEEE Computer and Reliability Societies