Bruce Schneier
Resilient Systems

The Security Value of Muddling Through

Of all the stories to come out of last year's massive Sony hack, the most interesting was the ineffectiveness of the company's incident response. Its initial reactions were indicative of a company in panic, and Sony's senior executives even talked about how long it took them to fully understand the attack's magnitude.

Sadly, this is more the norm than the exception. It seems to be the way Target and Home Depot handled their large hacks in 2013 and 2014, respectively. The lack of immediate response made the incidents worse.

It doesn't have to be this way. Crisis management was developed in the 1980s in response to large-scale industrial and environmental disasters. It includes procedures and best practices, professional organizations for industry, and a wide array of products and services. It's something IT incident response teams need to learn from, understand, and integrate with, as an Internet attack can quickly become a broader organizational crisis.

Good crisis management involves not only responding quickly and effectively but also having a mechanism in place for making on-the-spot decisions. This requires accurate information and the ability to synthesize it, ad hoc decision making, and the ability to act on those decisions. The most effective response organizations endlessly practice. The real incidents they'll be called on to respond to won't look exactly like the scenarios they've practiced, but the skills and relationships they've built during drills will be invaluable in a real incident.

In January 2014, the World Economic Forum (WEF) published a report titled "Risk and Responsibility in a Hyperconnected World," which looks at the growing risks in cyberspace to business and corporate networks due to the interconnection of everything as well as the inexorable links between government and corporate risks.

The report presents three scenarios. In the worst scenario, the growth of cyberspace is stunted because people and organizations are justifiably scared of increasing attack capabilities. In the middle scenario, called "Muddling into the Future," we continue to provide security much as we're doing today, without any overarching plan or even good data about future threats.

In the best scenario, governments and businesses worldwide work together to counter threats. I think the authors of this report put too much faith in formal systems of security response. I want to speak up for "muddling through."

In IT security, we muddle through all the time. We know that our security tools only go so far and that many attacks will quickly lead us outside any "playbook" we have in place. When they do, we rely on our skills and abilities to figure out what's happening. We use our established relationships to coordinate on the fly. And we figure out what to do in response.

Of course, there are better and worse ways to muddle through, and the ability to muddle through is a form of resilience. At the extreme, muddling through might be the best an organization can hope for. Never muddling through is no more achievable than perfect security.

We'll never prevent all attacks; sufficiently skilled, motivated, and funded attackers will always be able to get in. We need to get a lot better at incident response. We need to recognize that we'll need to muddle through these sorts of incidents and find tools and procedures to help us do so quickly and effectively. In the end, this is how we achieve security. ■

Bruce Schneier is the CTO of Resilient Systems. His new book is *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. Contact him at schneier@schneier.com.

Copublished by the IEEE Computer and Reliability Societies