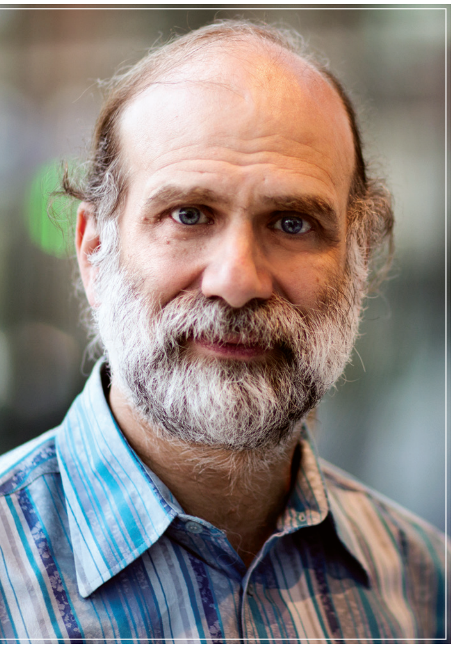

Bruce Schneier
Co3 Systems

The Future of Incident Response

Security is a combination of protection, detection, and response. It's taken the industry a long time to get to this point, though. The 1990s was the era of protection. Our industry was full of products that would protect your computers and network. By 2000, we realized that detection needed to be formalized as well, and the industry was full of detection products and services.

This decade is one of response. Over the past few years, we've started seeing incident response (IR) products and services. Security teams are incorporating them into their arsenal because of three trends in computing. One, we've lost control of our computing environment. More of our data is held in the cloud by other companies, and more of our actual networks are outsourced. This makes response more complicated, because we might not have visibility into parts of our critical network infrastructures.

Two, attacks are getting more sophisticated. The rise of APTs (advanced persistent threats)—attacks that specifically target for reasons other than simple financial theft—brings with it a new sort of attacker, which requires a new threat model. Also, as hacking becomes a more integral part of geopolitics, unrelated networks are increasingly collateral damage in nation-state fights.

And three, companies continue to underinvest in protection and detection, both of which are imperfect even under the best of circumstances, obliging response to pick up the slack.

Way back in the 1990s, I used to say that "security is a process, not a product." That was a strategic statement about the fallacy of thinking you could ever be done with security; you need to continually reassess your security posture in the face of an ever-changing threat landscape.

At a tactical level, security is both a product and a process. Really, it's a combination of people, process, and technology. What changes are the ratios. Protection systems are almost all technology, with some assistance from people and process. Detection requires more-or-less equal proportions of people, process, and technology. Response is mostly done by people, with critical assistance from process and technology.

Usability guru Lorrie Faith Cranor once wrote, "Whenever possible, secure system designers should find ways of keeping humans out of the loop." That's sage advice, but you can't automate IR. Everyone's network is different. All attacks are different. Everyone's security environments are different. The regulatory environments are different. All organizations are different, and political and economic considerations are often more important than technical considerations. IR needs people, because successful IR requires thinking.

This is new for the security industry, and it means that response products and services will look different. For most of its life, the security industry has been plagued with the problems of a lemons market. That's a term from economics that refers to a market where buyers can't tell the difference between good products and bad. In these markets, mediocre products drive good ones out of the market; price is the driver, because there's no good way to test for quality. It's been true in antivirus, it's been true in firewalls, it's been true in intrusion detection systems (IDSs), and it's been true elsewhere. But because IR is people focused in ways protection and detection are not, it won't be true here. Better products will do better because buyers will quickly be able to determine that they're better.

The key to successful IR is found in Cranor's next sentence: "However, there are some tasks for which feasible, or cost effective, alternatives to humans are not available. In these cases, system designers should engineer their systems to support the humans in the loop, and maximize their chances of performing their security-critical functions successfully." What we need is technology that aids people, not technology that supplants them.

The best way I've found to think about this is OODA loops. OODA stands for "observe,

cont. on p. 95

1540-7993/14/$31.00 © 2014 IEEE

cont. from p. 96

orient, decide, act," and it's a way of thinking about real-time adversarial situations developed by US Air Force military strategist John Boyd. He was thinking about fighter jets, but the general idea has been applied to everything from contract negotiations to boxing—and computer and network IR.

Speed is essential. People in these situations are constantly going through OODA loops in their head. And if you can do yours faster than the other guy—if you can "get inside his OODA loop"—then you have an enormous advantage.

We need tools to facilitate all of these steps:

- Observe, which means knowing what's happening on our networks in real time. This includes real-time threat detection information from IDSs, log monitoring and analysis data, network and system performance data, standard network management data, and even physical security information—and then knowing which tools to use to synthesize and present it in useful formats. Incidents aren't standardized; they're all different. The more an IR team can observe what's happening on the network, the more they can understand the attack. This means that an IR team needs to be able to operate across the entire organization.
- Orient, which means understanding what the attack means in the context of both the organization and the greater Internet community. It's not enough to know about the attack; IR teams need to know what it means. Is there a new malware being used by cybercriminals? Is the organization rolling out a new software package or planning layoffs? Has the organization seen attacks from this particular IP address before? Has the network been opened to a new strategic partner? Answering these questions means tying data from the network to information from the news, network intelligence feeds, and other information from the organization. What's going on in an organization often matters more in IR than the attack's technical details.
- Decide, which means figuring out what to do *at that moment*. This is actually difficult because it involves knowing who has the authority to decide and giving them the information to decide quickly. IR decisions often involve executive input, so it's important to be able to get those people the information they need quickly and efficiently. All decisions need to be defensible after the fact and documented. Both the regulatory and litigation environments have gotten very complex, and decisions need to be made with defensibility in mind.
- Act, which means being able to make changes quickly and effectively on the networks. IR teams vneed access to the organization's network—all of the organization's network. Again, incidents differ, and it's impossible to know in advance what sort of access an IR team will need. But ultimately, they need broad access; security will come from audit rather than access control. And they need to train repeatedly, because nothing improves a team's ability to act more than practice.

Pulling all of these tools together under a unified framework will make IR work. And making IR work is the ultimate key to making security work. The goal here is to bring people, process and, technology together in a way we haven't seen before in network security. It's something we need to do to continue to defend against the threats. ■

Bruce Schneier is the CTO of Co3 Systems. You can reach him online at www.schneier.com.