

ISSUES TO WATCH

To outwit today's cybercriminals, security professionals must think as cunningly as their adversaries. But doing so requires a change in perspective, says CDG Senior Fellow Morgan Wright.

Wright is an adviser to the U.S.

Congress House Science, Space and Technology Committee.

He previously served as a senior adviser in the U.S. State Department Antiterrorism

Assistance Program and was senior law enforcement adviser for the

2012 Republican National Convention.

Here's what Wright had to say about thinking differently about security.



We've seen some highly disruptive attacks in the past year – Colonial Pipeline, SolarWinds and others. Is something new happening?

There is nothing new under the sun.

The tactics are the same; only the tools have changed. The problem is the way we think about the problem. SolarWinds is a perfect example. Until SolarWinds, industry best practice was to put an application into a sandbox, monitor it for three days, and if nothing bad happens, push it into the production environment. What did the attackers do? They waited 10 days. They just out-thought us. The other thing is we place too much trust in things like cryptographically signed software updates, even when we have no idea of what's inside them. If I've got a nuclear bomb inside a sealed container, it's still a nuclear bomb whether or not the seal has been tampered with. We need to know what's actually inside of that container.

How can government organizations counter these tactics?

We need to take time to think about the problem. We also don't spend enough time looking at the problem through the eyes of our adversaries. If you want to stop a bank robbery, do you talk to the bank tellers or the bank robbers? To use an overused phrase, we have to think outside the box. The SolarWinds

SHUTTERSTOCK.COM



Changing Your Perspective on Security

attack came from that kind of thinking. They said, "We're going to attack the way they think about backups, and we're going to take advantage of the fact that they place way too much trust in encrypted updates."

How do you get perspective on what your adversaries are thinking?

You need to get out of the office. With people working so much, they don't have time to sit still, to stare off into space and think about how to think differently about the problem. A lot of people get "aha" moments in the shower because they're not working. Their mind is somewhere else, and they suddenly make a connection between two seemingly unrelated things. When I worked in government, I would tell people, "I want you to attend a conference that has absolutely nothing to do with your work; if you're into gardening, go to a gardening conference." It's also important to remove the mental constraints. You don't get in trouble for drawing something out on a whiteboard. Throw caution to the wind and say, "If we really wanted to disrupt something, what would we do?"

What issues should we be paying more attention to?

There was a joke when I was working inside the government: "Yesterday's technology tomorrow." Procurement is still the 800-pound gorilla that nobody wants to address. When you look at some of the procurement schedules, by the time you've baked in a

solution, it's outdated and can't meet current needs, so you've got to spend more taxpayer money. Again, the problem is the way we think about the problem. We think we need an RFP that's very prescriptive. But if you and I want to meet somewhere for dinner, I don't tell you what kind of transportation to use. We decide on a place and a time, and we each figure out the most cost-effective way to get there. In procurement, we need to start thinking about statements of objectives and the outcomes we want. We can't smother innovation with the blanket of bureaucracy.

Where do AI and ML come into all of this?

We cannot hire our way out of this problem. Even if people have the skills we need, we don't have enough people with those skills to address the problem. We have to get better at using automation, artificial intelligence and machine learning to defend our networks. Instead of legacy, anti-virus pattern-matching approaches, we need to look at behaviors and ask if a particular activity is appropriate given the context. In terms of automation, machine-speed attacks need machine-speed responses. If ransomware gets a foothold in your organization, it takes milliseconds for it to start spreading. If you wait for a human to try and determine whether something bad is happening, you've already lost. Your organization is already infected.