CQ&A: Why Cyber Attacks Keep Happening, and What Can Be Done to Prevent Them

By Ryan Lucas, CQ Roll Call

The Obama administration said Thursday that a massive cyber attack, apparently conducted by China-based hackers, managed to penetrate government computer systems and access the data of up to 4 million federal employees. The attack compromised information from the Office of Personnel Management, which handles human resources for the government, including background checks for security clearance.

This is not the first time in recent months that government computer systems have been hacked. In March 2014, hackers penetrated the OPM's database, and months later broke into unclassified computer networks at the White House. CQ talked to Paul Stockton, a former assistant secretary of Defense for homeland defense who is now managing director at the security and economics consulting firm Sonecon, and Randy Sabett, a former NSA crypto-engineer who is now the vice chairman of the privacy and data protection practice at Cooley, to find out more.

Q. Why do cyber attacks like the one that targeted the OPM keep happening?

Stockton: Because the incentives for the attackers to steal such valuable data are overwhelming. And because there are so many attack surfaces, there are so many ways of attempting to break in that protecting all federal networks is an extraordinary challenge. That's not to let the federal government off the hook in terms of strengthening the protection, but there's a basic problem here, and that is that for a foreign power, access to this kind of data held by OPM, especially if there's data on the security clearance system as well as the people in it, is so useful. It's an overwhelming incentive for the adversary to keep sharpening their means of attack, keep improving their ways of penetrating U.S. defenses, and then use the information that they steal in order to further sharpen their ability to attack.

Let me give you a prime example: assuming that some of this information contains deep and sensitive and identifiable information, especially if the attackers were able to get access to the material used in the security clearance and background investigations system, that same data will enable the attackers later on to build very sophisticated spear phishing campaigns against individuals, where if you were to look at the email sent to you by the attacker, you'd say 'ah, it's from somebody that I know well referencing something that we both know that we're working on' and asking me to click on the attachment just as I do every day.

Sabett: It's a very complex set of systems that we're dealing with. This is not an A + B = C kind of problem. From a vulnerability perspective, it's a multi-level system that has significant complexity, and invariably when you're dealing with systems that are that complex and oftentimes built on commercial software, they have not been through necessarily as rugged a process [as necessary], and so there may be vulnerabilities in there that get exploited over time.

You've probably heard the phrase "zero day" attack. A "zero day" attack is named that because somebody discovers a vulnerability, which means there is some sort of problem with the software or firmware or whatever it is we're talking about, and it's exploited that same day. On the zero day . . . an attack is structured and put in place, and those are very hard to defend against. And because those are complex systems they are hard to find in the first place.

Q. What can be done to prevent such attacks from happening again?

Stockton: The government needs to continue to deploy EINSTEIN 3 [a cybersecurity program for government agencies], which is a vastly improved way of providing for a perimeter defense. The government also needs, and the private sector, to continue to understand that because the attackers have such sophisticated weapons to break in and then to steal the data and send it back, that we need more than just a perimeter defense. We need more than the attitude that if we build our security systems that that is going to take care of us in the future. We need to be able to have effective cyber response capabilities. We need to be able to strengthen the kinds of systems and the kinds of technical skills that assume that the bad guys will be able to break into our infrastructure systems, attempt to steal data, disrupt industrial control systems, destroy networks if they can, and even destroy computers, turn computers into bricks.

We need, in short, not only to strengthen our perimeter defenses around our networks, but to assume that despite our best efforts, those networks are going to be penetrated, and [we need to] strengthen our ability to respond and get our systems back up and running after a successful attack.

Sabett: I think the first high-level answer is you will never stop these kinds of things from happening unless you unplug your cable or shut down your wireless router. . . . You will always have systems that are technically fallible, and likewise you'll have humans that are fallible. Can we make things better? I think the answer is yes. Will we get to a point where we can totally stop these? I know the answer is no.

We can make the system better. We can get better, but we'll never get to perfect. So if we can agree on that, I think the question becomes: How do we better prepare for the inevitable?

I used to be at the NSA, and I was on the defensive side of things, I was helping to protect our stuff. And I think the mindset has to be, when you're trying to actively protect yourself, there are two aspects to it. There's making sure people don't get in, but there's also being ready for an attack when it occurs.

Q. Looking at the cyber protection act (HR 1560) that the house passed this year, would it prevent hacks like this from occurring?

Stockton: The information-sharing provisions of the proposed legislation, and many of its other features, I believe will be helpful. Sharing threat signatures and making sure that both the public and private sector have a better understanding of what the adversary is trying to do — that's pure goodness. On the other hand, I think that even with those improvements we need to press forward on the broader cyber resilience side, and that is to make sure that if despite our best efforts, despite the improvements that the legislation would make possible in information-sharing, if the bad guys still break in, that we can get our cyber systems and everything that they enable back up and running.

Sabett: I think it could contribute to lowering the likelihood of a success of this sort of an attack, but completely preventing it, not likely. . . . There is no such thing as perfect security. The corollary that I think applies here is that you're not going to prevent these kinds of things from happening. But could you reduce the likelihood? Yes. But the other thing you could do, and I think this is where the bill could help a little bit, is [that] by making the preparedness phase for something to occur, you're going to be more prepared, so I think that's where it could help.