Executive Viewpoint

SECURITY FOR THE MODERN WORLD

National Archives and Records Administration takes a multipronged approach to ensuring comprehensive cybersecurity policies and technologies.

NEIL CARMICHAEL
DIRECTOR, INSIDER THREAT PROGRAM, OFFICE OF THE CHIEF OPERATING OFFICER, NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (NARA)

Federal agencies across the board have made great strides toward improving their overall cybersecurity postures. The recent Cyber Sprint, in particular, helped many agencies identify and remediate vulnerabilities, but there is still much to be done.

FCW caught up with Neil Carmichael, Director, Insider Threat Program, Office of the Chief Operating Officer, National Archives and Records Administration (NARA), to hear his thoughts on the current state of cybersecurity.

What are the primary types of threats agencies face today, and how well do they understand those threats?

The external threat is always going to be there, but the "new" threat people must come to grips with is the insider threat. That threat has always been there, but what's new about it is the vast amount damage that can now be done. If you go back 30 or 40 years, people could compromise just a few documents at a time. Now they can walk out the door with gigabytes of data.

I think agencies do understand the risk they face from this type of threat. There's the malicious person who does something with intent. Then there's the person who means no harm, but for one reason or another, doesn't follow the rules or policies and inadvertently releases information they shouldn't. Then there are people—particularly newer and younger employees—who have no fear of what they put online. They want to do a good job, they're frustrated by all the government rules, and they look for ways to get around them.

Would the definition of insider threat extend to government contractors with credentials that allow access to agency networks?

Our policy at NARA is that "insider" includes anybody with access. So that does include contractors. We monitor their activities, just as we do our own employees. It would also include other government agencies with contractors who do work at the Archives and elsewhere and anyone who has security clearance. For that reason, I have to work closely with other agency's insider threat programs as we're only going to see a small portion of their activity.

How effective are technology-driven programs such as Continuous Diagnostics and Mitigation?

For insider threats, pretty much all we do is monitoring. It has to be part of any good insider threat program. We're looking for things that are out of the norm of what people do.

You have to assume there's always going to

"For insider threats, pretty much all we do is monitoring. It has to be part of any good insider threat program. We're looking for things that are out of the norm of what people do."

"Training is most effective when you don't do it in a heavy handed way ... We need to get them to stop and think about things, and we're getting much better at that."

be someone who's going to make a mistake. They're not paying attention and they do something that needs to be corrected. Then it's a matter of how fast can you respond and mitigate things or stop it before any damage is done.

I think we are getting better at that, but I don't think we'll ever get to the point where we'll be able to say we're 100 percent protected. The target is always changing. It's all about moving the goalposts.

Where does employee training come into this?

I think you can overdo the training, to the point where they become desensitized. It's more a matter of striking the right balance. On one hand, you have to educate them about the issues. Then you have to make sure you follow up.

We've also found training is most effective when it's targeted. For example, through analysis we identified several offices in NARA that tend to have more security issues than others. We first engaged the managers, because the front-line supervisors are the key to handling this. We told them we were noticing certain trends. Then we saw noticeable improvements handling it that way.

Training is most effective when you don't do it in a heavy-handed way. It's when we use a, "Hey, do you know this?" type of approach. We need to get them to stop and think about things, and we're getting much better at that.

Most people, at least here at the National Archives, want to do a good job and protect the assets with which we're entrusted. When security issues arise though, I don't think it's through apathy or anything like that. It's more a case of fatigue. People are working hard just to do their jobs. So you have to keep things in the forefront, but not to the point where you get the eye-roll and a "Here we go again with the training," kind of response.

What about programs like the 30-day Cyber Sprint run in 2015? Would more of those on a regular basis be helpful?

As a way of putting issues in the forefront and bringing them to the attention of everybody, I certainly believe those types of programs don't hurt. They can't be done obtrusively though. They are best done in a targeted, specific manner. Every agency is different in terms of the impact of those kinds of programs. You have to do it frequently enough and with a focus on certain aspects of security, such as external and internal threats. It's a delicate balance.

How effective are current government-wide policies and regulations in helping you with security? Is anything else needed?

A lot of the time, I think government tends to overthink things. For the National Archives, I try to determine what's already out there that we can leverage from the perspective of insider threats. Are there other offices already collecting information? Are there any agencies already looking at violations of policy and regulation? How can we latch onto those?

I think the tools are already there for us to use. It's a matter of breaking down some internal stovepipes so we can maintain a good information flow about issues within the organization. At NARA, we have gotten really good at breaking down those stovepipes. I think overall, the federal government is getting better at getting information out to those who need it most.

Do you see any future technology developments that will help you better secure your agency?

There are always new tools being developed. And there are a lot of good tools out there now that can be helpful. With many of them, though, you've got to balance the employee's personal privacy with the right of the government to know what the employee is doing. So it's not so much a matter of what are the better tools out there, but how do you utilize them.

The oversight we put on tools are extremely important. There's no question though, there are some tools that are going to help wash out the noise and be very beneficial. In the end, it all boils down to a single analyst sitting in a cubicle using the technology who is going to make the determination whether or not a threat is legitimate. We have to keep that human component in mind. Sometimes, agencies lose sight of that.