

Cybersecurity

Air Force cyber unit ramps up training

By **NICOLE BLAKE JOHNSON**
njohnson@federaltimes.com

Before airmen are deemed competent defenders and operators of Air Force networks, chances are they've undergone academic and simulation training at the Air Force's 39th Information Operations Squadron in northwest Florida.

The cyber operations and information training unit is now ramping up its cyber training model to mirror techniques used to prepare pilots and aircrews, said Lt. Col. Brian Denman, commander of the 39th Information Operations Squadron.

"The cyber domain is broad,"

Denman said. "The threats are increasing. The one-size-fits-all nature of our previous training wasn't sufficient to the need."

After identifying gaps in training and the skills required in the field, the unit has been working over the past year to provide more tailored training and to ensure airmen can better manage and defend the network and detect intrusions, said Skip Runyan, technical adviser for the Air Force unit.

The government as a whole, especially the Defense Department, is steering away from general cybersecurity certifications and is finding greater value in more specific credentials as indicators of competency, said Jeff Frisk, direc-

tor of the Global Information Assurance Certification program, which issues information security credentials.

Among the cyber certifications offered through the program are incident handling — that is, the ability to properly respond to a incident by patching holes and determining whether an intruder is still in the system, for instance — firewall analyst and intrusion analyst.

Unlike other fields — medical, law enforcement and others — there is no standard government-wide training required for cyber professionals.

A cybersecurity bill introduced in 2009 by Sen. John Rockefeller IV, D-W.Va., would have tasked the Commerce Department with developing a certification program for cybersecurity professionals and made it illegal to operate federal networks without meeting the program's standards.

"That's an interesting concept, but the wheels turn so slowly to establish rules," Frisk said. "In order to have an industry and set standards, they have to be established for some amount of time."

In the cybersecurity field, training and certification requirements change constantly with the threat.

"What we used to teach and con-

sider the advanced course is now the basic course," Denman said of Air Force cyber training. "We've increased the skill level that we train to."

Alan Paller, director of research for the SANS Institute, said the framework developed by the National Initiative for Cybersecurity Education is a step in the right direction.

The cybersecurity framework — open for public comment until Dec. 16 — is intended to better define and describe cybersecurity work in the federal government. A lack of these standards hinders the government's ability to identify skill gaps, develop cybersecurity talent and prepare the future workforce, according to the framework.

"If people cared about security the way they cared about medicine, they would actually have skills we can count on," Paller said.

He said adequate training for a cyber professional should run agencies and companies \$3,000 to \$4,000 a year.

A recent survey of 200 federal workers and contractors found that half of the agencies ranked software tools to identify system vulnerabilities as their top cyber-related investment. Investments in

training lagged behind with 37 percent.

The study, conducted by Market Connections Inc. for Cisco and released this month, interviewed managers and executives from all military services and 25 civilian and independent agencies, including the Homeland Security and Treasury departments, the General Services Administration and the U.S. Postal Service.

New cybersecurity reporting requirements issued by the Office of Management and Budget could prompt more training for agencies as they move to continuous monitoring of their networks for security problems and monthly cybersecurity reporting, said Don Berbari, president of Learning Tree International.

OMB Director Jack Lew directed agencies in a Sept. 14 memo to begin reporting cybersecurity data into a DHS system called CyberScope.

Previously, agencies compiled spreadsheets of data to fulfill annual reporting requirements under the 2002 Federal Information Security Management Act.

"It may increase the visibility to weaknesses or areas that need to be focused on," Berbari said. "Do we [agencies] have people needed to deal with these issues?" □

DoD gets proactive in fight against cyber attacks

By **ZACHARY FRYER-BIGGS**
zbiggs@federaltimes.com

Tired of playing "whack-a-mole" with hackers, the Defense Department is trying to spot their telltale signs before they can do substantial damage.

Instead of relying upon passive cyber defense systems, DoD is turning to proactive defensive measures as attacks increase. The agency is also quietly advancing its offensive cybersecurity capabilities and readiness.

"This is now commander's business; this is no longer admin tech business," said Brig. Gen. John Davis, who directs operations at U.S. Cyber Command (USCYBERCOM).

DoD is re-evaluating and modifying its cyber strategy, an effort that began after CYBERCOM stood up last year, and which gained pace with Deputy Secretary William Lynn's July announcement that cyber would be deemed an operational domain. The attackers' target list has broadened in recent years, breaching the less defended networks of contractors and subcontractors to extract some of the same sensitive data housed on DoD networks.

CYBERCOM's placement at Fort Meade, Md., home to the National Security Agency, is a nod to the realization that cybersecurity personnel need access to intelligence.

"By partnering us with NSA, that enables us to have access to that information for the purpose of defending much more quickly," Davis said. "The information has been there; it's the sharing of that in real time that has improved."

Army Gen. Keith Alexander, commander of USCYBERCOM, called the relationship crucial.



Army Gen. Keith Alexander, commander of U.S. Cyber Command, said it is important for cybersecurity personnel to have access to the latest intelligence, and that "active defense is where we have to go."

"The professionals that provide the information assurance side of our mission and the offensive side of our mission, the key folks who operate on the network and know the technical aspects, the mathematicians, the electrical engineers, the computer scientists, about 800 Ph.D.s reside at NSA," Alexander told an audience Sept. 13 at the InfoWarCon conference.

Alexander emphasized the new direction of cybersecurity: "The active defense is where we have to go."

Seeking out threats

Traditional network defenses — firewalls and anti-virus programs — are easily de-

feated these days, experts said.

Firewalls are routinely avoided using a technique called spear phishing. A target receives an email that appears to be from a known sender, and follows the instructions to download a file or enter login details at a third-party site. Once armed with a valid username and password, the attackers can move about all but undetected. Because this technique does not rely upon a failure of technology but rather a failure of the user to recognize the scam, it is essentially impossible to stop.

The ubiquitous anti-virus programs rely upon libraries of information on previously detected malicious files. But an attacker can keep watch on the libraries, and as soon as his virus is added, the attacker changes tactics.

"He escalates to the minimum level of awesome that he needs to out-awesome you, the defense, and then he'll stay there until the defense gets better and he's been detected," said Michael Graven, a director at the cybersecurity company Mandiant. "Then he'll go a little further and use something that's a little more sophisticated."

Graven says security experts need to exploit the fact that intruders are boxed into the victim's network, and they need to actively and routinely search.

"When you have a remote attacker, he has to expose his activity in the network," he said. "It means that his tools are on the victims' computers, which if you can look, you can find."

Going on the attack

In addition to improving defensive approaches, USCYBERCOM is also pushing into offensive territory, although officials re-

main mum on the details.

"We need the capabilities to do things offensively in cyber; that's because our joint war fighters have identified these requirements to build those capabilities, everybody acknowledges that, but how we specifically employ that in an operational context is classified," a USCYBERCOM official said.

No offensive operations or programs have been publicly exposed. Still, the branch-specific subcommands are planning to allow the expansion of this offensive capacity.

"Right now, our focus is really on ensuring that we're ready by providing training for the forces, so we're hard at recruiting and training those capabilities to provide to Cyber Command," said Lt. Gen. Rhett Hernandez, commander of Army Cyber Command.

Much of the hush over offensive operations is grounded in the murky legal territory in which they reside. A U.S. government cyber attack on another country or citizens of another country is likely not covered in any existing international treaty, and even the domestic authority of the DoD to wage cyberwarfare is a legitimate question. To help alleviate the concern over the latter, the House of Representatives included clauses in its 2012 National Defense Authorization Act that expressly authorizes the secretary of defense to engage in military and clandestine cyber activity.

Alexander said that he sees clear reasons to have the offensive capacity, even if full war is not part of the plan.

"I think there are response actions that you would take ... that are logical," he said. "What I would be concerned about is getting ourselves in a position where you escalate a cyber issue to a military kinetic issue. And so what I think we have to do is thoughtfully go down that road." □