US cyber pros test skills in exercise meant to stop attacks

March 8 2016, by Tami Abdollah

Secret Service Director Joe Clancy speaks during the kick off Cyber Storm V in Washington, Tuesday, March 8, 2016. More than 1,100 cybersecurity professionals across the country and from Wyoming, Missouri, Mississippi, Georgia, Maine, Nevada, Oklahoma and Oregon, are participating in the Homeland Security Department's simulation to test their ability to deal with a cyberattack, said Touhill, the agency's deputy assistant secretary for Cybersecurity Operations and Programs at DHS. (AP Photo/Tami Abdollah)

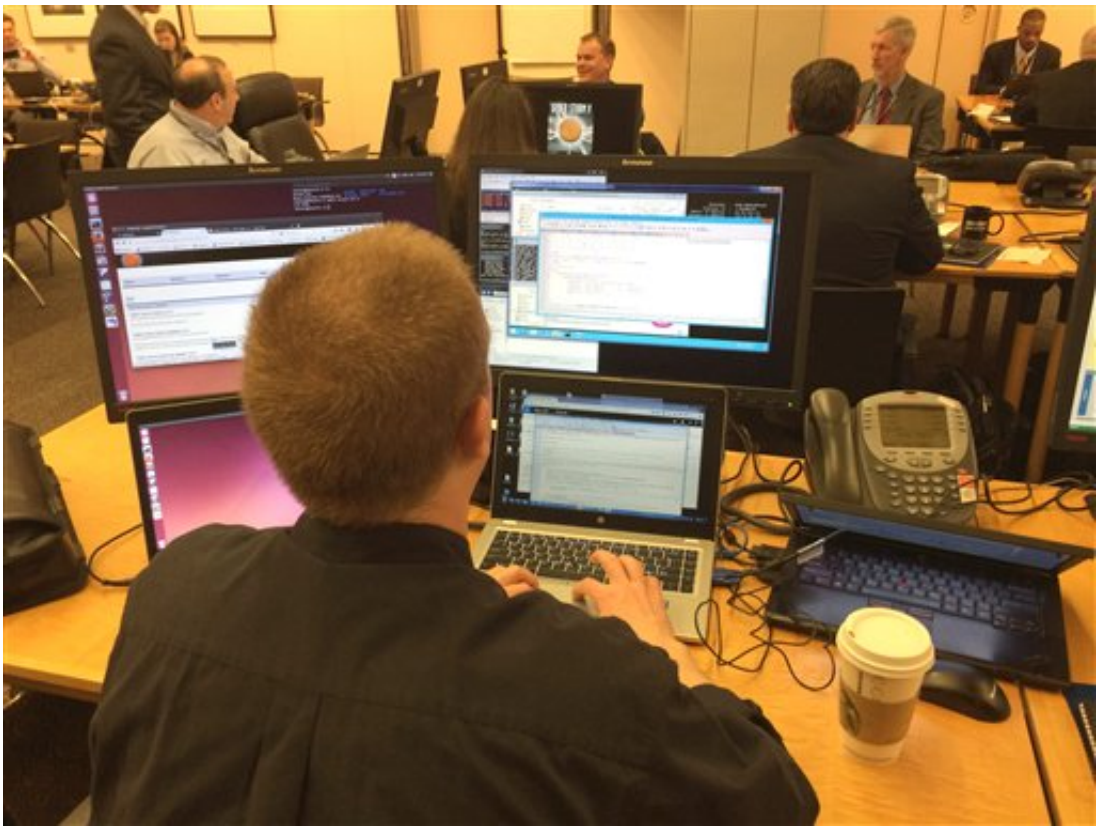
The moment a U.S. official pressed a computer key Tuesday, dozens of security experts who gathered in an underground control room girded themselves for a cyberattack—a drill meant to thwart the kinds of intrusions that have recently crippled health networks and retail giants.

The weeklong event run by the Homeland Security Department and hosted by the U.S. Secret Service is now a decade old. But officials say this week's exercises are becoming more important as both the government and private sector have reeled from breaches of personal data.

More than 1,000 U.S. cybersecurity professionals are participating in—and testing how well they respond to—a mock attack, said Gregory Touhill, a Homeland Security Department deputy assistant secretary for cybersecurity protection. They'll be working together for three days in Washington and across the nation.

"Retail and health care have been in the headlines—and, frankly, in the crosshairs for a lot of criminals," Touhill said. Household names like Target Corp., The Home Depot, UCLA Health Systems and Anthem Inc. have all faced recent cyberattacks that compromised millions of their customers' data.

U.S. officials wouldn't detail the attack scenarios unfolding this week because they said it would tip off the drill's participants. But they said their event has one, overarching scenario, with roughly 1,000 smaller events—spurred by a phone call, an email or a news article—that could be indicators of an looming cyberattack.



Mission control at Cyber Storm V in Washington, Tuesday, March 8, 2016. More than 1,100 cybersecurity professionals across the country and from Wyoming, Missouri, Mississippi, Georgia, Maine, Nevada, Oklahoma and Oregon, are participating in the Homeland Security Department's simulation to test their ability to deal with a cyberattack, said Touhill, the agency's deputy assistant secretary for Cybersecurity Operations and Programs at DHS. (AP Photo/Tami Abdollah)

Suzanne Spaulding, a top Homeland Security cyber official, said the "challenge is here and now." She pointed to a "nightmare" scenario last December, in which hackers attacked the Ukrainian electrical grid and cut power to about a quarter-million people.

During previous U.S.-led tests, officials found what they called areas for improvement. Touhill said at least two areas from a previous test are still

being addressed, including ensuring people have and follow protocols, and security personnel share information effectively.

Secret Service Director Joseph Clancy described the event Tuesday as a way to stay one step ahead of criminals who've taken advantage of new and changing technology, and who have changed their own tactics.

In addition to eight participating state governments—Wyoming, Missouri, Mississippi, Georgia, Maine, Nevada, Oklahoma and Oregon—officials from five countries are also observing the exercises. The Homeland Security Department wouldn't reveal the countries involved.

Other participants include health companies, Internet service providers, telephone companies and retail organizations. The aim is to test human response and coordination, not necessarily the participants' technical skills.

"We're looking to find the failure points, to raise the bar in every scenario," Touhill said.

Recent attacks have also hammered the financial sector, in which a 2014 data breach at JPMorgan Chase affected more than 76 million households and 7 million small businesses. The bank said hackers may have stolen names, addresses, phone numbers and email addresses.

Meanwhile, U.S. officials told Congress last year the Office of Personnel Management didn't take basic steps to secure their computer networks. That allowed to Chinese-linked hackers to steal private information about nearly every federal employee, as well as detailed personal histories of millions who had security clearances.

© 2016 The Associated Press. All rights reserved.

Citation: US cyber pros test skills in exercise meant to stop attacks (2016, March 8) retrieved 20 September 2024 from https://phys.org/news/2016-03-cyber-pros-skills-meant.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.