Government Executive

UNDERWRITTEN BY

DELL

Quest Software
is now a part of Dell

DLT SOLUTIONS

5 Strategies for Countering Cyber Threats

By Aliya Sternstein

The federal government is out to stop cybercrooks—by reaching potential victims before they do. Public outreach is one of the best countermeasures against hacking, according to agencies and experts. As cybercrime escalates, "the FBI has arrested hundreds of groups in this space," says Shawn Henry, the bureau's former cyber chief. "What about all the intelligence that could have been shared with these victims before they were victims?" Now, the government is trying to arm computer users with the tools and information necessary for the long-term battle against cyber threats.

Here are five key public service efforts under way to strengthen cybersecurity.

PUBLIC AWARENESS

The FBI routinely alerts the public to cyber scams through Homeland Security Department bulletins and the Internet Crime Complaint Center, an FBI-led public private partnership. For example, Homeland Security's Computer Emergency Readiness Team warned in August that fraudsters were posing as officials from U.S. Cyber Command and other federal agencies to scare Internet users into paying bogus fines. A CERT notice said malicious software triggers a computer screen that claims a federal agency has determined the user is involved in criminal activity. The message directs the victim to either pay a fine or lose access to the computer. IC3 had warned of similar schemes that essentially hold computers hostage until victims pay the bogus fine. The August incident apparently was the first time scammers had used the identities of Cyber Command officials to collect ransom. The CERT bulletin closed with instructions for victims on how to recover from viruses and file a complaint with IC3.

Federal authorities also are sharing cybercrime findings before closing cases to teach the public how to fix compromised computers. For almost a year, the FBI and DHS have maintained Web pages with directions on checking computers for a virus called DNSChanger, which the bureau partially neutralized after Operation Ghost Click. During that investigation, the FBI and international authorities quashed a botnet—a network of computers that crooks remotely commandeer without the owners' knowledge. The instigators were redirecting people to bogus websites. Agents seized the offenders' servers and in November 2011 replaced

them with safe servers that would navigate victims to their desired online destinations. But there was a catch. Unless victims removed the DNSChanger infection, they always would be dependent on the special servers for surfing the Web. So, several agencies published recommendations on how to expunge the worm.

SHARING LEADS

Each year, the Secret Service shares information on computer intrusions with Verizon for the telecom giant's annual data breach report. The analysis details population groups while protecting the names of individuals and organizations. The goal of the study is to help law enforcement officials, citizens and Internet service providers fight cybercrime.

Usually businesses are hesitant to report breaches if their reputations are on the line. So, U.S. government authorities submit incident data using a standard digital questionnaire that asks only for general demographics, such as the size of an organization's workforce and

number of information technology staffers. The data amassed is wiped of any information that might identify firms or individuals before the hand-off to Verizon's research team for analysis.

"When the Secret Service sends that information over to Verizon, we don't know that it took corrective measures," says Chris Porter, principal for Verizon's RISK Team. "We get a lean picture of what's happening without having to share information that could potentially embarrass an organization."

Separately, bureau officials say they are mindful of privacy when approaching companies for leads on hacks. "The FBI understands that the private sector has practical concerns about reporting breaches to law enforcement. Where necessary, the FBI, working with the Justice Department, seeks protective orders to preserve trade secrets and business confidentiality," spokesman Dean Boyd says.

HACKER CRACKDOWN

Justice Department officials are cracking down on scams large and small to cap damages before they skyrocket. In June, officials unsealed charges against a 23-year-old Pennsylvania man, alleging that he and others hacked into computer networks at RNK Telecommunications Inc. in Massachusetts, the Energy Department and other organizations nationwide—and then sold access to those systems.

In March, federal investigators released lengthy indictments of six hackers, including one government informant, who allegedly are tied to the vigilante group Anonymous. Four of them were charged with compromising computers at Fox Broadcasting Co., PBS and Sony Pictures Entertainment, while a fifth suspect pleaded guilty. Another associate was charged with stealing confidential information, including credit card data, from about 860,000 clients and subscribers of global intelligence publisher Stratfor.

In May, the ringleader of an international computer hacking scheme was sentenced to five years in jail for defrauding banks. The defendant opened numerous Bank of America accounts in her name at a variety of branches and transferred $14,000 to those accounts through email fraud that led to charges against 100 individuals—the largest number of defendants ever charged in a cybercrime case.

All of these enforcement actions were made public.

OPEN DOOR POLICY

At conferences and other open venues, senior FBI officials are being frank about the cyber threat. Computer hacks will supersede terrorism as the "No. 1 threat to the country," FBI Director Robert Mueller has said.

Seán McGurk, former director of the National Cybersecurity and Communications Integration Center at the Homeland Security Department, has said openness actually benefits national security. "Providing direct feedback to the public really allows us to do our job better," he says. "Sharing often is a good thing because it speeds all our activities along."

TRAINING CYBER KIDS

The government is funding initiatives for children in schools nationwide to build the country's future cyber corps and quash budding hackers. Federal agencies need tens of thousands of computer whizzes educated in network protection and offensive techniques who are able to exploit flaws in an adversary's networks, as well as detect weaknesses in the government's own networks. Agencies are sponsoring competitive cybersecurity games to immunize kids against the temptations of computer fraud.

The Air Force Association's nationwide CyberPatriot contest, partially funded by the service's research laboratory, starts out by teaching high schoolers cyber ethics and cyber citizenship, says CyberPatriot Commissioner Bernie Skoch, a former Air Force information technology director. The cyber defense competition aims to discourage malicious activity by "explaining the legal consequences, the career consequences of someone in their adolescence doing the wrong thing," he says. The program is viewed as an inoculation against moral confusion. "I liken what we're doing to 4-H and to Girl Scouts of America and what we see in church groups across the nation," Skoch adds. "We want to reach them very young so that when they confront a potential dilemma it's not a dilemma at all."

During the past few years, many universities and nonprofits have sponsored school and professional contests that teach penetration testing or ethical hacking. There is always the risk the cybersecurity scholars may be up to no good. But computer experts say one of the most important jobs in defending U.S. national security is detecting network vulnerabilities.

The U.S. Cyber Challenge, designed for high school and college students, urges youths to find flaws during competitions. "We include in our curriculum an ethics panel discussion with the campers, which include panelists from the U.S. Secret Service and the FBI," says Cyber Challenge National Director Karen Evans, who held what is now the federal chief information officer position during the George W. Bush administration. The contest provides students with legal information so they will use their talents appropriately.