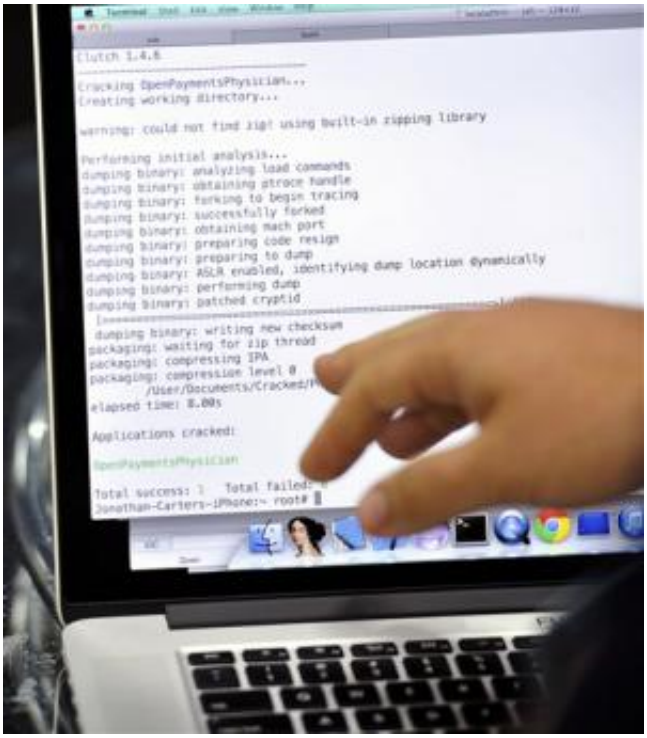
Federal government struggles against cyberattacks

November 10 2014, by Martha Mendoza



In this Aug. 6, 2014, photo, Joe Abbey, Arxan Technologies' director of software engineering, displays on his computer how he hacked into a phone app during a demonstration at the Black Hat USA 2014 cyber security conference, in Las Vegas. Federal systems grow more susceptible to attack as the government's online offerings expand to user-friendly websites and apps, experts say. (AP Photo/David Becker, File)

A $10 billion-a-year effort to protect sensitive government data, from

military secrets to Social Security identification numbers, is struggling to keep pace with an increasing number of cyberattacks and is unwittingly being undermined by federal employees and contractors.

Workers scattered across more than a dozen agencies, from the Defense and Education departments to the National Weather Service, are responsible for at least half of the federal cyberincidents reported each year since 2010, according to an Associated Press analysis of records.

They have clicked links in bogus phishing emails, opened malware-laden websites and been tricked by scammers into sharing information.

One was redirected to a hostile site after connecting to a video of tennis star Serena Williams. A few act intentionally, most famously former National Security Agency contractor Edward Snowden, who downloaded and leaked documents revealing the government's collection of phone and email records.

Then there was the contract worker who lost equipment containing the confidential information of millions of Americans, including Robert Curtis of Colorado.

"I was angry, because we as citizens trust the government to act on our behalf," he said. Curtis, according to court records, was besieged by identity thieves after someone stole data tapes that the contractor left in a car, exposing the health records of about 5 million current and former Pentagon employees and their families.

At a time when intelligence officials say cybersecurity trumps terrorism as the No. 1 threat to the U.S., the federal government isn't required to publicize its own data losses.

In this Tuesday, Sept. 9, 2014, photo, Phyllis Schneck, deputy undersecretary for cybersecurity at the Department of Homeland Security, speaks to the Associated Press at the National Cybersecurity and Communications Integration Center (NCCIC) in Arlington, Va. A $10 billion-a-year effort to protect sensitive government data, from military secrets to Social Security numbers, is struggling to keep pace with an increasing number of cyber attacks and is unwittingly being undermined by federal employees and contractors. (AP Photo/Manuel Balce Ceneta)

Last month, a breach of unclassified White House computers by hackers thought to be working for Russia was reported not by officials but The Washington Post. Congressional Republicans complained even they weren't alerted to the hack.

To determine the extent of federal cyberincidents, the AP filed dozens of Freedom of Information Act requests, interviewed hackers,

cybersecurity experts and government officials, and obtained documents describing digital cracks in the system.

That review shows that 40 years and more than $100 billion after the first federal data protection law was enacted, the government is struggling to close holes without the knowledge, staff or systems to outwit an ever-evolving foe.

This March 5, 2012 file photo provided by the Cook County Sheriff's Department in Chicago shows Jeremy Hammond. Once the FBI's most-wanted cybercriminal, Hammond is serving one of the longest sentences a U.S. hacker has received, 10 years, the maximum allowed under his plea agreement last year. (AP Photo/Cook County Sheriff's Department, File)

Fears about breaches have been around since the late 1960s, when the federal government began shifting its operations onto computers. Officials responded with software designed to sniff out malicious programs and raise alarms about intruders. And yet, attackers have always found a way in, exposing tens of millions of sensitive and private records that include employee usernames and passwords and veterans' medical files.

From 2009 to 2013, the number of reported breaches just on federal computer networks—the .gov and .mils—rose from 26,942 to 46,605, according to the U.S. Computer Emergency Readiness Team. Last year, US-CERT responded to a total of 228,700 cyberincidents involving federal agencies, companies that run critical infrastructure and contract partners. That's more than double the incidents in 2009.

And employees are to blame for at least half of the problems.

In this Wednesday, Aug. 6, 2014, photo, Arxan Technologies' Joe Abbey, left, director of software engineering; Jodi Wadhwa, vice president of marketing and Jonathan Carter, technical director, prepare for a hacking demonstration during the Black Hat USA 2014 cyber security conference in Las Vegas. Federal systems grow more susceptible to attack as the government's online offerings expand to user-friendly websites and apps, experts say. (AP Photo/David Becker)

Last year, for example, about 21 percent of all federal breaches were traced to government workers who violated policies; 16 percent who lost devices or had them stolen; 12 percent who improperly handled sensitive information printed from computers; at least 8 percent who ran or installed malicious software; and 6 percent who were enticed to share private information, according to an annual White House review.

In this Wednesday, Aug. 6, 2014, photo, Joe Abbey, Arxan Technologies' director of software engineering, displays on his computer how he hacked into a phone app during a demonstration at the Black Hat USA 2014 cyber security conference, in Las Vegas. Federal systems grow more susceptible to attack as the government's online offerings expand to user-friendly websites and apps, experts say. (AP Photo/David Becker)

Reports from the Defense Department's Defense Security Service, tasked with protecting classified information and technologies in the hands of federal contractors, show how easy it is for hackers to get into DOD networks. One military user received messages that his computer was infected when he visited a website about schools. Officials tracked the attacker to what appeared to be a Germany-based server.

"We'll always be vulnerable to ... human-factor attacks unless we educate the overall workforce," said Assistant Secretary of Defense and

cybersecurity adviser Eric Rosenbach.

In this Tuesday, Sept. 9, 2014, photo, specialists work at the National Cybersecurity and Communications Integration Center (NCCIC) in Arlington, Va. A $10 billion-a-year effort to protect sensitive government data, from military secrets to Social Security numbers, is struggling to keep pace with an increasing number of cyberattacks and is unwittingly being undermined by federal employees and contractors. (AP Photo/Manuel Balce Ceneta)

Although the government is projected to spend $65 billion on cybersecurity contracts between 2015 and 2020, many experts believe the effort is not enough to counter a growing pool of hackers whose motives vary. Russia, Iran and China have been named as suspects in some attacks, while thieves seek out other valuable data. Only a small fraction of attackers are caught.

For every thief or hostile state, there are tens of thousands of victims

like Curtis.

"It is very ironic," said Curtis, himself a cybersecurity expert who worked to provide secure networks at the Pentagon. "I was the person who had paper shredders in my house. I was a consummate data protection guy."

In this Wednesday, Aug. 6, 2014, photo, conference attendees arrive at the Black Hat USA 2014 cyber security conference in Las Vegas. Federal systems grow more susceptible to attack as the government's online offerings expand to user-friendly websites and apps, experts say. (AP Photo/David Becker)