PHYS.ORG

Why the IRS was just hacked – again – and what the feds can do about it

February 16 2016, by Nir Kshetri, University Of North Carolina - Greensboro

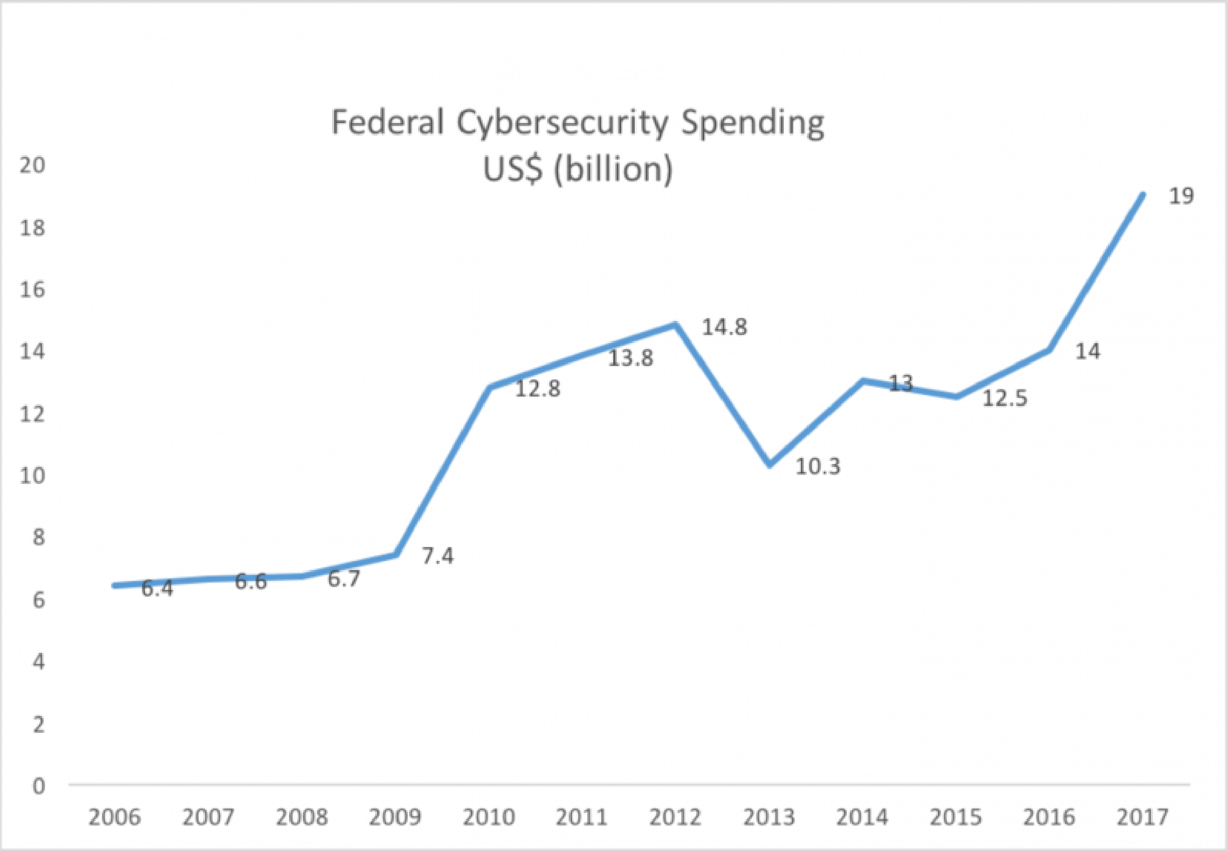
Federal computer systems are under near-constant attack from hackers and cyberthieves. Is our information protected well enough? Credit: Colin/Wikimedia Commons, CC BY-SA

Last month hackers stole Internal Revenue Service data belonging to more than 100,000 taxpayers. This sort of attack on the IRS and other federal computer systems keeps happening – and succeeding – because the government's cyberdefenses are not strong enough to resist.

Hacking of U.S. government electronic databases is a near-constant threat. Attacks allegedly come from criminal gangs in Russia and Central and Eastern Europe, often seeking financial information from systems like the IRS, which holds personal data on hundreds of millions of taxpayers.

Other cyberattacks can come from skilled foreign operatives, such as hackers allegedly working for the Chinese government, trying to extract high-value intellectual property or gather intelligence. In one such case, a 2015 hack of Office of Personnel Management (OPM) data exposed the personal information of 22 million current and former federal employees. Other hackers attack U.S. sites independently in hopes of selling what they find to interested buyers.

Due to their nature, position and size, federal networks need stronger security measures than most organizations. So far the cybersecurity resources devoted are not in proportion with the risks. How can U.S. government agencies be better prepared to protect their sensitive data?



Federal cybersecurity spending, FY2006 to FY2017.

Recent action to increase protection

Several policy measures and initiatives are aimed at tackling cyberthreats . Last year, President Obama announced a plan for government agencies and private companies to better share information about pending and ongoing cyberthreats. In December, Congress codified that process in law.

Just last week, the White House released a Cybersecurity National Action Plan. It includes a multifaceted cybersecurity effort within the federal government, extending through the private sector and even with recommendations for individual behavior to improve personal cybersecurity.

These efforts complement other policies and programs adopted in recent years. The 2010 National Strategy on Trusted Identities in Cyberspace aims to increase confidence in online transactions. The 2011 National Initiative on Cybersecurity Education program seeks to train more people to do cybersecurity jobs. The 2011 International Strategy for Cyberspace,promotes international collaboration to fight often-elusive digital attackers.

Government spending on cybersecurity and fighting cybercrimes has also increased, to US$19 billion for cybersecurity in fiscal 2017, which is 35 percent more than in fiscal 2016. Some agencies' funding has been increasing for years. For example, in 2005 the FBI spent $150 million on fighting cybercrimes, or 3 percent of its $5 billion budget. Ten years later in 2015, the FBI's cyber budget was $470 million, amounting to 5.7 percent of the agency's $8.3 billion budget request that year.

A big legacy to overcome

Even with bigger budgets, it's difficult for federal agencies to keep up with cybercriminals. Many federal agencies use antiquated computer systems, which are difficult to update and secure against today's threats. For instance, the OPM's personnel files were stored using a decades-old database system that was last updated when it was fixed for the Y2K bug. The system had limited encryption options.

In addition, many agencies lack high-level officials responsible for cybersecurity. That results in a lack of leadership and coherent vision to properly protect government information. The Cybersecurity National Action Plan has called for the creation of a federal chief information security officer position, but the job may take time to fill.

Further, there are not enough people to fight the threat. More than 30,000 open cybersecurity positions existed in federal agencies in 2014. As far back as 2011, the National Institute of Standards and Technology predicted that by 2015, the U.S. public and private sectors combined would need 700,000 more cybersecurity professionals than were available. Training is so scarce that many cybersecurity specialists with practical computer expertise are self-taught.

Another major challenge is that many cybercriminals targeting the U.S. operate from countries that lack strict law enforcement or have little or no cooperation with the U.S. regarding cybercrime and cybersecurity. The U.S.–China Business Council has asked the U.S. and Chinese governments to work together to address cyberattacks, regardless of what country they come from. Specifically, the council urged the two countries to hold a regular annual summit to discuss cybersecurity issues.

The weakest links

Although security is often cast as a largely technical problem, employees are often the weakest links. For instance, in a State Department hack reported in 2015, an employee reportedly clicked a malicious link within a phishing email. After the malware was downloaded to the employee's computer, the attackers penetrated into networks across the U.S. and foreign locations, including embassies.

Weak security practices of federal agencies' contractors are also a concern. For example, foreign hackers allegedly hacked the defense contractor Lockheed Martin and several subcontractors in 2009, allegedly stealing terabytes of data related to the Pentagon's next-generation fighter jet, the F-35, including design details and operational capabilities.

Strong cybersecurity requires a multipronged approach. The government must teach all its employees about strong cybersecurity practice, and ensure they follow proper procedures. The training must include all the 22 million federal, state and local government employees – and all employees of government contractors.

In the long run, efforts should be concentrated on developing a better prepared cyber workforce. Most importantly, it is necessary to strengthen cooperation and coordination with countries that are hotspots for cyberattacks targeting the U.S.

For instance, allegations and counterallegations have been persistent themes in dialogues and discourses in the China-U.S. relationship involving cybercrimes and cybersecurity. One way to improve this is to work with China to address typical problems such as cybercrimes that are common to both countries. The two countries' law enforcement agencies could share experience, expertise and information to fight cybercrimes. It might lead to more substantial cooperative cybersecurity relationships in the future. An improved China-U.S. relationship on the cyber front may also make some Chinese hackers targeting U.S. networks feel less protected.

This article was originally published on The Conversation. *Read the* original article.

Source: The Conversation

Citation: Why the IRS was just hacked – again – and what the feds can do about it (2016, February 16) retrieved 26 April 2024 from https://phys.org/news/2016-02-irs-hacked-feds.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.