The Cybersecurity 202: The government's facing a severe shortage of cyber workers when it needs them the most

Marks, Joseph . The Washington Post (Online) , Washington, D.C.: WP Company LLC d/b/a The Washington Post. Aug 2, 2021.

FULL TEXT

with Aaron Schaffer

The government is struggling to hire cybersecurity workers at the same time it is facing an unprecedented slate of hacking threats.

The dearth of cyber workers is making it harder to protect government data from being stolen by adversaries and diminishing its ability to help improve cybersecurity in industries vital to national and economic security. It also worsens the dangers posed by the government's notoriously outdated technology systems.

Top officials have described the slow pace of cyber hiring as a national security threat.

The government's cyber workforce has grown by about 8 percent since 2016. A hiring sprint at the Department of Homeland Security resulted in nearly 300 new cyber hires and about 500 more job offers between May and July. But that's nowhere near sufficient to meet the threats. By DHS's own calculations, there are about 1,700 more cybersecurity vacancies it needs to fill at the department.

"We need leadership to pay attention and to see it as their responsibility to own getting the right [cyber] talent into government, and by and large they don't do that and it's a big problem," Max Stier, head of the Partnership for Public Service, told lawmakers during a House Homeland Security Committee hearing on cyber hiring.

Stier's testimony highlighted deep problems in the government's cyber workforce.

The cyber workforce since 2016 has actually shrunk at some federal agencies, including the Labor and Agriculture departments.

Just 25 percent of government cyber workers are female.

There are 16 times more federal IT workers older than 50 than there are younger than 30.

His suggested fixes:

Hold top government officials accountable when their agencies can't retain cyber workers.

Create more paid internships for young cybersecurity professionals and make it easy to move from internships to government jobs.

Make it easier to pay government cyber professionals higher salaries that compete with the private sector.

Another idea from Post Columnist Jennifer Rubin: Replace political appointees in key cyber roles with career government workers.

Jen Easterly, director of DHS's Cybersecurity and Infrastructure Security Agency, has made near-daily appeals for cyber pros to join the agency on her newly launched Twitter profile.

Government is not the only employer struggling to hire and retain cyber workers.

There are nearly 465,000 unfilled cyber jobs across the nation, according to data gathered under a Commerce Department grant.

But the situation in government is particularly dire. There's a shortage of about 36,000 public-sector cyber jobs across federal, state and local governments, according to that same data set.

The government's cyber hiring is hampered by pay that's not competitive with the private sector, inflexibility that turns off younger workers, and a lengthy and arcane hiring process that is frustrating and difficult to navigate.
DHS expects to roll out a system this year that will speed up cyber hiring and make it easier to increase pay for cyber workers. But that has taken wading through nearly insurmountable bureaucracy.
Indeed, the legislation authorizing the hiring program, called the Cyber Talent Management System, passed Congress in 2014.
"That's too long," Stier said. "You can't wait seven years for this kind of action."

Government work is also a poor fit for many younger cybersecurity pros –both for political and cultural reasons.

On the political side, cyber pros have balked at National Security Agency surveillance. Def Con, one of the industry's largest annual conferences, went so far as to ask federal employees not to attend in 2013, the year NSA leaker Edward Snowden revealed several expansive spying programs.
The decision to ask DHS Secretary Alejandro Mayorkas to keynote this year's conference, which takes place next week in Las Vegas, drew mixed reactions from the cyber community.
The typically countercultural cyber community has also clashed with straitlaced government culture.
Former FBI Director James Comey complained in 2014 that it was difficult to hire top cyber talent at the bureau because of background checks that barred marijuana smokers.
"I have to hire a great workforce to compete with those cyber criminals, and some of those kids want to smoke weed on the way to the interview," he said at a conference hosted by the New York City Bar Association. He said the FBI was "grappling" with amending its hiring policies to be more tolerant of past marijuana use.
Comey later backpedaled and said he was "trying to be both serious and funny" after the comment raised hackles at the Senate Judiciary Committee.

The keysRussian government hackers breached more than two dozen federal prosecutors' offices.

The Kremlin hackers behind the SolarWinds cyberattack were able to spy on email accounts in federal prosecutors' offices around the country for eight months last year, the Justice Department said. Some of the accounts were in prosecutors' offices in Los Angeles, Miami and D.C., which handle high-profile cases.
New York offices, which also prosecute prominent cases, were hit especially hard. The email accounts belonging to at least 80 percent of employees working for the four U.S. attorney's offices in New York were breached, the Justice Department said.
The electronic filing system used by the U.S. court system was also "apparently" breached, court officials said in January. Less than 3 percent of Justice Department email accounts appeared to be compromised, the agency said at the time.

An Israeli lawyer called an emergency meeting of spyware vendors amid international scrutiny.

The conference in Tel Aviv is being hosted by Israeli lawyer Daniel Reisner, who represents several spyware firms, Haaretz's Amitai Ziv reports. It will focus on "possible courses of action" the firms can take in the wake of revelations by The Washington Post and 16 media partners that NSO Group's Pegasus spyware targeted journalists and human rights activists worldwide.
The developments come as NSO has temporarily blocked some government clients from using its technology, an NSO employee told NPR's Daniel Estrin. The employee would not give additional information such as the name or number of clients, citing Israeli defense regulations. NSO has dismissed the Pegasus Project's reports but the company's CEO, Shalev Hulio, pledged to investigate potential cases of wrongdoing.
Meanwhile, the investment fund that owns NSO Group may change hands. The largest investors in the fund selected California firm Berkeley Research Group to take control of it after conflicts with the previous management, two people familiar with the matter tell Kaye Wiggins and Anna Gross of the Financial Times. The decision has not been finalized and investors have until Friday to vote on the future of the fund.
The ownership shake-up was not related to the Pegasus Project. But Berkeley Research Group could determine the future of NSO if it takes control of the fund. The firm declined to comment.

Nigeria's "super cop" supported a cybergang, the FBI said.

Nigeria Police Force Deputy Commissioner Abba Alhaji Kyari is wanted in the United States on charges related to wire fraud and money laundering, Danielle Paquette reports. The newly unsealed charges came after Nigerian scammer Ramon Abbas, who is also known as "Hushpuppi," said Kyari accepted a bribe to arrest someone who double-crossed the cybergang.

The Nigerian police force said it has launched an investigation into the FBI allegations but did not say whether Kyari had been suspended. Kyari has denied wrongdoing. Abbas pleaded guilty to fraud-related charges in April and faces up to 20 years in prison. His gang tricked employees at U.S. companies into paying them money by using phony email addresses, prosecutors said.

The Justice Department declined to say if they're requesting Kyari's extradition.

Hill watch

A $1 trillion bipartisan infrastructure proposal that senate negotiators unveiled last night contains more than $1 billion in cyber funding. Details from Politico's Sam Sabin:

Cyber insecurity

Women allege that NSO spyware was used to steal and leak private photos (NBC News)

Hackers leak full EA data after failed extortion attempt (The Record)

Privacy patch

E.U. regulator hits Amazon with $887 million fine for data protection violations (Taylor Telford)

Zoom reaches $85 million settlement over user privacy, 'Zoombombing' (Reuters)

Global cyberspace

Hackers shut down system for booking vaccinations in Italy's Lazio region (Reuters)

Industry report

FTC's 'right-to-repair' ruling is a small step for security researchers, giant leap for DIY hackers (CyberScoop)

Mentions

Allan Friedman, director of cybersecurity initiatives at the National Telecommunications and Information Administration, is joining CISA, where he plans to focus on "scaling and operationalizing" his work on software bills of materials.

Daybook

The Atlantic Council holds an event on why the United States needs a Bureau of Cyber Statistics today at 2:30 p.m.

Deputy national security adviser Anne Neuberger speaks at the Aspen Security Forum on Wednesday.

The Senate Homeland Security and Governmental Affairs Committee discusses cybersecurity legislation on Wednesday at 10:30 a.m.

CISA Director Jen Easterly and Homeland Security Secretary Alejandro Mayorkas speak at the Blackhat hacking conference on Thursday.

Easterly, Mayorkas and CISA executive assistant director Eric Goldstein speak at the DEF CON conference on Friday.

Secure log off

DETAILS

Subject:	Talent management; Internships; Hiring; Political activism; National security; Computer security; Employment; Public prosecutors; Workforce; Internet crime; Federal employees; Political appointments; Data encryption; Privacy; Electronic filing; Congressional committees
Business indexing term:	Subject: Talent management Hiring Employment Workforce

Location:	United States--US New York Nigeria
People:	Mayorkas, Alejandro
Company / organization:	Name: NSO Group; NAICS: 561611; Name: Berkeley Research Group LLC; NAICS: 541690; Name: Federal Bureau of Investigation--FBI; NAICS: 922120
Publication title:	The Washington Post (Online); Washington, D.C.
Publication year:	2021
Publication date:	Aug 2, 2021
Section:	Politics
Publisher:	WP Company LLC d/b/a The Washington Post
Place of publication:	Washington, D.C.
Country of publication:	United States, Washington, D.C.
Publication subject:	General Interest Periodicals--United States
ISSN:	26419599
Source type:	Blogs, Podcasts, &Websites
Language of publication:	English
Document type:	News
ProQuest document ID:	2557315496
Document URL:	https://www.proquest.com/blogs-podcasts-websites/cybersecurity-202-government-s-facing-severe/docview/2557315496/se-2?accountid=44910
Copyright:	Copyright WP Company LLC d/b/a The Washington Post Aug 2, 2021
Last updated:	2021-08-03
Database:	U.S. Major Dailies