The New York Times

OPINION

GUEST ESSAY

Why the F.B.I. Is So Far Behind on Cybercrime

Nov. 6, 2022

By Renee Dudley and Dan Golden
Ms. Dudley and Mr. Golden are reporters at ProPublica.

There are many factors behind the stunning rise of ransomware. Our reporting found that one of the most important is the Federal Bureau of Investigation's outmoded approach to computer crime targeting people and institutions in the United States.

State and local police generally can't handle a sophisticated international crime that locks victims' data remotely — from patients' medical histories and corporate trade secrets to police evidence and students' performance records — and demands payment for a key. Many police departments have themselves been hamstrung by ransomware attacks. Federal investigators, especially the F.B.I., are responsible for containing the threat. They need to do better.

When ransomware gained traction a decade ago, individual attackers were hitting up home users for a few hundred dollars. In 2015, as the crime was evolving into something more, the bureau still dismissed ransomware as an "ankle biter." That year, about a dozen frustrated Cyber Division agents warned James Comey, who was then the director of the F.B.I., that institutional lack of respect for their skills was spurring their departures. Now well-organized gangs, with hierarchies mirroring those of traditional businesses, are paralyzing the computer networks of high-profile targets and demanding millions of dollars in ransom.

The F.B.I. didn't prioritize ransomware until May 2021, when an attack on the Colonial Pipeline halted the flow of nearly half of the fuel consumed on the East Coast. The F.B.I. director, Christopher Wray, compared ransomware to the Sept. 11 terrorist attacks, but by then the bureau was far behind the curve. Earlier this fall, when the Los Angeles Unified School District, the second largest in the nation, spurned a ransom demand, a hacker group leaked hundreds of thousands of stolen files. Last month's attack on CommonSpirit Health, one of the country's largest hospital operators, disrupted care and knocked patients' health records offline.

The situation could turn even more dire. Evidence is mounting that some ransomware gangs are linked to and protected by enemy governments, such as those of Russia or Iran. Hackers who steal data before locking it could turn over the digital spoils to their patrons — giving foreign powers access to records that could compromise everything from intellectual property to national security.

One reason the F.B.I. can't keep pace is that it lacks enough agents with advanced computer skills. It has not recruited as many of these people as it needs, and those it has hired often don't stay long. Its deeply ingrained cultural standards, some dating to the bureau's first director, J. Edgar Hoover, have prevented it from getting the right talent.

Emblematic of an organization stuck in the past is the F.B.I.'s longstanding expectation that agents should be able to do "any job, anywhere." While other global law enforcement agencies have snatched up computer scientists, the F.B.I. tried to turn existing agents with no computer backgrounds into digital specialists, clinging to the "any job" mantra. It may be possible to turn an agent whose background is in accounting into a first-rate gang investigator, but it's a lot harder to turn that same agent into a top-flight computer scientist.

The "any job" mantra also hinders recruitment. People who have spent years becoming computer experts may have little interest in pivoting to another assignment. Many may lack the aptitude for — or feel uneasy with — traditional law enforcement expectations, such as being in top physical fitness, handling a deadly force scenario or even interacting with the public.

The minority of agents with deep technical skills described the frustration of having to dumb down reports to superiors and needing to train colleagues who are not technically savvy, we found in our reporting. Plus, the F.B.I.'s macho culture has scorned digital skills. Cyber Division agents are nerds in a sea of jocks. The bureau has hired civilian computer scientists separately, but they are viewed as helpers, who typically command even less respect than Cyber Division agents.

The "anywhere" expectation is also misguided. Unlike agents on crimes such as bank robberies, cyberinvestigators usually don't need to be near a crime scene to collect evidence. Still, F.B.I. agents typically span the country, changing posts every few years, for career advancement.

The F.B.I.'s emphasis on arrests, which are especially hard to come by in ransomware cases, similarly reflects its outdated approach to cybercrime. In the bureau, prestige often springs from being a successful trial agent, working on cases that result in indictments and convictions that make the news. But ransomware cases, by their nature, are long and complex, with a low likelihood of arrest. Even when suspects are identified, arresting them is nearly impossible if they're located in countries that don't have extradition agreements with the United States.

All of these aggravations cause computer experts to leave the F.B.I. It's an easy transition because their skills are both immediately transferable to the private sector and in high demand.

The F.B.I. should study the success of the Dutch National Police's High Tech Crime Unit. Because of its fast internet and favorable legal conditions, the Netherlands has long been a popular spot for hackers to set up the servers they use to commit crimes. The Dutch responded by launching the H.T.C.U. 15 years ago. Since then, it has become one of the world's leading law enforcement forces in fighting cybercrime. Beyond arrests, it has prioritized anything that reduces hackers' return on investment, seizing criminals' servers, disrupting ransomware-spreading botnets and notifying victims of impending attacks.

From its early days, the H.T.C.U. hired tech experts with no background, or even interest, in traditional policing. When some talented digital recruits couldn't pass the physical fitness tests or didn't want to use weapons, H.T.C.U. leadership changed the requirements, allowing computer experts to join without passing the usual exams. But they left the job titles unchanged: Digital staff remained eligible for promotion to nearly any job in the H.T.C.U.

The H.T.C.U. also specified that half its staff must be cyberexperts. Each one is paired with a traditional law enforcement officer, and they work cases as a team. As John Fokker, who once served as digital coordinator of the H.T.C.U.'s ransomware team, told us, "the old school with the new school made it work."

That approach works for the Dutch. If it is willing to let go of the "any job, anywhere" mantra, it could work for the F.B.I., too.

More on ransomware

A Rare Win in the Cat-and-Mouse Game of Ransomware

White House Warns Companies to Act Now on Ransomware Defenses

Don't Ignore Ransomware. It's Bad.

Renee Dudley, a technology reporter at ProPublica, and Daniel Golden, a senior editor and reporter at ProPublica, are the authors of "The Ransomware Hunting Team: A Band of Misfits' Improbable Crusade to Save the World From Cybercrime."