cyberscoop

Top U.S. counterintelligence official: Kaspersky's move to Switzerland doesn't matter

William Evanina, the Director of the National Counterintelligence and Security Center, told CyberScoop that the damage has been done with regards to the Moscow-based company.

The ongoing fight between the U.S. government and Moscow-based Kaspersky Lab led the company to begin moving "a good part" of its infrastructure to Switzerland in a highly-visible move toward transparency in the face of spying accusations. The U.S.'s top counterintelligence official, however, says Kaspersky's move to Switzerland makes no difference to him.

William Evanina, the Director of the National Counterintelligence and Security Center, looks at the way the U.S. government handles Kaspersky — which is now banned from the U.S. federal government and is losing ground in the private sector — as "an opportunity to create a model," he said. "This will not be the last time this happens. I think there will be more to come along, I call them 'nation-state threats that emanate through the global business process.' "

Kaspersky's opening of a "Transparency Center" in Switzerland is significant but leaves open a wide range of questions. The company has described numerous independent review processes but there's no information yet about who will actually be conducting reviews. A Kaspersky spokesperson did, however, tell CyberScoop that "U.S. and U.K. government representatives are welcome" to "explore and review the source code, updates and software assembler, as well as the way the data center is designed and managed."

Government pressure against Kaspersky has consistently ramped up in the past year. In addition to the U.S. federal ban, the U.K. is cutting the company out of sensitive systems. The Dutch government is phasing the company out as well.

Within the last few weeks, a European Union parliamentary resolution was introduced proposing to ban Kaspersky products, which it referred to as "confirmed as malicious." The pressure on Kaspersky comes amid a growing emphasis from Western countries on supply chain threats. In addition to Kaspersky, Chinese companies like Huawei and ZTE have been deemed "national security threats" by the U.S. government due to ties to Chinese intelligence agencies.

Evanina says his top priority is taking the intelligence gathered by the U.S. government and informing organizations of various threats. It's a process that's been ongoing for years: Briefings from law enforcement and intelligence agencies in 2016 and 2017 warned U.S.-based companies to cut ties with Kaspersky.

Evanina's office works with the FBI and DHS to provide "one-time read ins" to private sector executives on cyber threats or, on some occasions, penetrations already in progress. Evanina tries to "illustrate the consequences" that would drive a company to act.

"We've done this a few times," he said. "We worked with SEC and FCC to bring telecoms in. We've brought energy firms in twice, we're doing it against next month." In the case of Kaspersky, the briefings directly resulted in U.S. energy firms avoiding the Russian cybersecurity giant, according to people with knowledge of the situation. The read-ins are a key element in a saga where the evidence the U.S. government reportedly has against Kaspersky has not been presented because, U.S. intelligence officials say, it would put key sources and methods at risk. That

makes it virtually impossible for anyone without access to classified information to render an informed decision. The lack of details has provoked both skepticism and criticism from many in the tech sector and even former intelligence officials.

“I hope we have a reason [for banning Kaspersky],” former NSA Director Michael Hayden told CyberScoop. “A real reason. Obviously if that’s our logic, we legitimate people all over the world to possibly reject American technology simply because it’s American. I hope to God we have a case rather than just a concern.”

With the possibility of U.S. sanctions against Kaspersky still hanging in the air, Hayden called for more transparency “to undercut the reciprocal argument where other countries chuck out stuff simply because it’s American.”

The possibility of significant, worldwide effects on U.S. companies was emphatically shrugged off by Evanina, who said that countries like China already stifle U.S. companies and that “our competitors around the world need U.S. business capabilities.” Currently his office will brief about 25 executives from a specific sector at a time. The goal is to raise that number and expand beyond the usual major industry and critical infrastructure suspects to sectors like academia to better defend “the threat to academia with our science and research and development.”