Know Your Risk Amid Tensions with Iran, CISA Advises

The agency encourages all organizations to review its cyber and physical security procedures.

James Mersol

Fri, 01/10/2020 - 12:42

Photo Credit: alexsl/iStock

The first days of 2020 have been a roller coaster for those involved with and adjacent to defense and national security issues. Following the American strike on Iranian general Qassem Soleimani, experts have speculated about the prospect of war or sustained conflict with Iran, amid a flurry of deployments, debates, counterstrikes, announcements and tweets. As some of these experts discussed the risk of Iran retaliating through a cyberattack, DHS' Cybersecurity and Infrastructure Security Agency (CISA) issued insight on increased geopolitical tensions and threats and what they mean for securing networks and infrastructure in the U.S.

"Review your organization from an outside perspective and ask the tough questions," the notice recommends. "Are you attractive to Iran and its proxies because of your business model, who your customers and competitors are, or what you stand for?"

This levelheaded approach echoes what CISA Director Chris Krebs stressed at the 2019 CISA Cybersecurity Summit last September.

"Stop selling fear," he said. "Fear sells, but we have so much more to offer."

While there are fundamental risks in the infrastructure that both the public and private sector should be aware of, he added, discussing ways to mitigate that risk is a far more practical strategy than focusing on the fear, which merely undermines confidence.

The latest CISA insight discusses potential threats to infrastructure as well. CISA recommends that all organizations ask 15 questions, listed on its website, regarding both cyber and physical security. It offers guidance on developing and refining response plans to an active shooter or bomb threat, underscoring "plans must be exercised to be effective." Other guidance sits at the intersection of cyber and physical security, encouraging organizations to inventory "keys, access cards, uniforms, badges and vehicles" and review the management processes governing these items.

CISA's guidance should be treated as an opportunity to review organizational security posture rather than a warning of an imminent attack. Earlier in the week, experts said that the threat of an offensive waged wholly online is unlikely. Last year, James Andrew Lewis of the Center for Strategic and International Studies wrote, "Iran has probed U.S. critical infrastructure for targeting purposes. How successful an attack would be is another matter."

Unlike conventional weaponry, a worm, virus or other information threat vector is only effective once, and after it is used (if not before), the vulnerability it exploits is patched. While Iran is a capable actor, the U.S. also has a robust defensive capability, Lewis said. Most high-value targets on federal networks are protected against current-day threat vectors, and Iranian cyber operators are unlikely to see the value in launching ransomware against a local utility company or regional network like a school district.

A larger-scale attack — say, one that causes a turbine at a major U.S. power plant to explode — is physically possible but much more likely to be considered an escalation, said Lewis.

Thomas Rid, a professor at the Johns Hopkins University School of Advanced International Studies, agrees. In his 2011 article and 2013 book, Cyber War Will Not Take Place, he challenged the conventional wisdom at the time that future wars might take place entirely in cyberspace. Rather, Rid said, cyberspace is a new domain of warfare that would accompany conventional warfare instead of replacing it. Additionally, most attacks are difficult to attribute, and most intrusions take the form of espionage or sabotage, not destruction of life and physical property.

Should the U.S. declare war upon Iran or vice versa, Iran is a sophisticated enough actor that offensive measures such as distributed denial of service attacks on American networks and takedowns of industrial control systems are not out of the question, he added.

For now, however, CISA advised agencies and other organizations to take the following action steps:

-

"Prepare your organization for rapid response by adopting a state of heightened awareness." Along with the second action step below, CISA recommends “reviewing your security and emergency and preparedness plans” to ensure there are no stumbles should the need to execute it arise.

- “Increase organizational vigilance” — take the time to do an audit of your security practices to ensure your capabilities cover known vulnerabilities, and ensure your teams know how to look for indicators of compromise (IOCs) connected to Iranian actors. Most importantly, ensure everyone knows the procedures for responding to security incidents.
- “Confirm reporting processes” — have a plan for reporting in place. As HHS CISO Janet Vogel said on CyberCast, reporting incidents to relevant federal agencies like CISA and HHS allows them to provide assistance in how to respond and to share that information across the federal space to protect others from the threat.
- “Exercise your incident response plan” — while most if not all organizations already have an incident response plan in place, CISA advises practicing that plan to ensure that “personnel are positioned to act in a measured, calm and unified manner.”
- “Confirm offline backup” — especially in the case of ransomware, restoring systems from backups may take several days and result in substantial lost business, but nowhere near the time and money lost to an attack with no way of recovery.

Emphasizing its role as “the nation’s risk advisor,” CISA encourages any organizations that have questions, information about a potential compromise, or a need for help in protecting its physical and online presence to reach out for assistance.

View printer friendly version
cybersecurity
infrastructure security
cisa
Iran
Standard