

Cyber Security Advisory

Feb. 1, 2022

AHA Warns of Increased Cyber Risk to U.S. Health Care Due to Russia/Ukraine Geopolitical Tensions

The AHA is closely monitoring the potential for increased cyber risks to the U.S. health system due to a possible military conflict in the Russia/Ukraine region. As part of AHA's efforts, John Riggi, the association's national advisor for cybersecurity and risk, and a former senior executive in the FBI's cyber division, is in close coordination with the FBI, the Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Health and Human Services regarding related threats which may pose a risk to U.S. health care.

There are three concerns for the field, each stemming from the possibility that Russia/Ukraine geopolitical tensions result in increased Russian-borne cyber threats:

- 1) hospitals and health systems may be targeted directly by Russian-sponsored cyber actors;
- 2) hospitals and health systems may become incidental victims of, or collateral damage to, Russian-deployed malware or destructive ransomware that inadvertently penetrates U.S. health care entities; and
- 3) a cyberattack could disrupt hospitals' mission-critical service providers.

AHA's concerns are heightened by the Russian military's previous behavior of utilizing cyber weapons in support of military actions against the Ukraine; such behavior ultimately inflicted disruptive collateral damage to the U.S. health care system, resulting in the U.S. government's [2020 indictment](#) of six Russian military intelligence officers for the development and deployment of the destructive NotPetya malware three years prior. The malware was initially launched against the Ukraine and subsequently spread globally, disrupting operations at a major U.S. pharmaceutical company, a major U.S. health care communications company and U.S. hospitals.

The AHA has served as a platform to amplify and provide guidance related to recent government warnings and advisories:

- The AHA on Jan. 28, 2022, received an [FBI request for information](#) regarding Russia's recent buildup of armed forces along its shared border with the Ukraine.
- CISA Jan. 16 issued an [advisory](#) urging review of a [Microsoft blog](#) on destructive malware identified on networks in the Ukraine and to take action to strengthen their networks against potential cyber threats.

- The AHA and the Health-Information Sharing and Analysis Center Jan. 14 [issued](#) a joint advisory strongly recommending organizations identify, and consider blocking, any direct or third-party business associate connections and email contacts based in the Ukraine and that region of the world.
- The FBI and National Security Agency on Jan. 11 released [recommendations](#) to help health care and other critical infrastructure organizations prevent, detect and respond to common Russian state-sponsored cyber threats.

NEXT STEPS

Hospitals and health systems should review the above-identified alerts and bulletins for guidance on risk mitigation procedures, including increased network monitoring for unusual network traffic or activity, especially around active directory. Additionally, it is important to heighten staffs' awareness of increased risk of receiving malware laden phishing emails.

Geo-fencing for all inbound and outbound traffic originating from, and related to, Ukraine and the surrounding region may help mitigate direct cyber risks presented by this threat; however, it will have limited impact in reducing indirect risk, in which malware transits through other nations, proxies and third parties.

AHA also recommends that organizations identify all internal and third-party mission-critical clinical and operational services and technology; in doing so they should put into place four-to-six week business continuity plans and well-practiced downtime procedures in the event those services or technologies are disrupted by a cyber attack.

At this time, it is also critical that a cross-function, leadership-level cyber incident response plan be fully documented, updated and practiced. This should include emergency communications plans and systems.

FURTHER QUESTIONS: If you have any questions or information regarding these issues, contact John Riggi at jriggi@aha.org.