Cold Storage Cyber Custodial Care

December 2020

THE THREAT AND HOW TO THINK ABOUT IT

As America prepares for distribution of coronavirus vaccines, the security and integrity of facilities that will receive, house, and distribute COVID-19 vaccines has come into focus. Physical or cyber disruptions to the ability of the nation to maintain supplies of COVID-19 vaccines at sufficiently cold temperatures could interfere with the nation's ability to protect its citizens from illness and further delay full economic recovery.

Cyber threat actors have shown an interest in targeting IT assets that support the vaccine cold chain and cold storage facilities. (See CISA's recent alert on cyber adversaries targeting cold chain facilities.) CISA recommends that owners/operators of cold storage facilities prepare for attacks targeting the cold chain, remain vigilant to alerts and activity in this space, have contingency plans in place, and know who to contact for help.

CYBER MITIGATIONS

To assist in the potential mitigation of these threats, CISA is providing a cold storage operator checklist designed to help assess resiliency against attacks and readiness for recovery. Use of the checklist is not a requirement, nor is the checklist all encompassing. Rather, it is designed as a guide to further self-assess your defensive posture.

- Remote connectivity of your cold storage may expose you to accidents and adversaries; if you are not using it, consider disabling it. If you are using it, please take steps to mitigate that exposure.
- Engage your manufacturers of cold storage systems on attack surface reduction and hardening best practices.
- Avoid the use of default or maintenance passwords. (Some manufacturer's contracts written prior to COVID-19 may have discouraged changing default passwords: please seek exceptions.)
- Ensure that the cold chain assets are not visible on search engines for internet-connected devices (i.e., Shodan and Censys).
- Consider use of an additional, less exposed thermometer as independent verification of required temperature.
- Identify alternative custodians of your supply of vaccines and/or access to dry ice providers.
- Remain vigilant for state, federal, and private sector alerts related to cold chain attacks and mitigations.

INCIDENT RESPONSE CAPABILITIES

- Review, rehearse, and enhance incident response and crisis management plans for a cold chain disruption event scenario.
- Document and review who to call for assistance across all state and federal jurisdictions and authorities.

CISA'S ROLE AS THE NATION'S RISK ADVISOR

As the nation's risk advisor, the Cybersecurity and Infrastructure Security Agency (CISA) leads the nation's efforts to ensure the cybersecurity, physical security, and resilience of our critical infrastructure. CISA works with partners across government and industry to defend against today's threats and collaborates to build more secure and resilient infrastructure for the future.

Please visit the CISA COVID-19 Resource Page for more information. Victims of cold storage cyberattacks should report it immediately to CISA at Central@CISA.DHS.GOV, your local FBI Field Office or Secret Service Field Office. Federal and state assistance is also available through State Homeland Security Advisors and Emergency Management agencies.