CISA
CYBER+INFRASTRUCTURE

January 6, 2020

CISA INSIGHTS

Increased Geopolitical Tensions and Threats

The Threat and How to Think About it

Increased geopolitical tensions and threats of aggression may result in cyber and physical attacks against the Homeland and also destructive hybrid attacks by proxies against U.S. targets and interests abroad. Knowing how you, your organization, and your personnel may be exposed or targeted during increased tensions can help you better prepare. In many cases, implementing the Cybersecurity and Infrastructure Security Agency (CISA) Cyber Essentials can dramatically improve your defenses. Should an incident occur, engage with partners, like CISA, and work with cyber or physical first responders to gain technical assistance. Review your organization from an outside perspective and ask the tough questions—are you attractive to Iran and its proxies because of your business model, who your customers and competitors are, or what you stand for?

Iranian Threat Profile and Activity

Recent Iran-U.S. tensions have the potential for retaliatory aggression against the U.S. and its global interests. Iran has exercised increasingly sophisticated capabilities to suppress social and political perspectives deemed dangerous to its regime and to target regional and international adversaries. Iran and its proxies and sympathizers have a history of leveraging cyber and physical tactics to pursue national interests, both regionally and here in the United States, such as:

- **Disruptive and destructive cyber operations** against strategic targets, including finance, energy, and telecommunications organizations, and an increased interest in industrial control systems and operational technology.
- **Cyber-enabled espionage and intellectual property theft** targeting a variety of industries and organizations to enable a better understanding of our strategic direction and policy-making.
- **Disinformation campaigns** promoting pro-Iranian narratives while pushing anti-U.S. sentiments.
- **Improvised explosive devices (IEDs)**, which are a staple tactic of the Islamic Revolutionary Guard Corps (IRGC), its Quds Force (focused on external, global operations), and proxy entities such as Hizbollah.
- **Attacks against U.S. citizens and interests abroad** and similar attacks in the Homeland.
- **Unmanned aircraft system (UAS) attacks** against hardened and soft targets.

CISA strongly urges you to assess and strengthen your basic cyber and physical defenses to protect against this potential threat

Things to do Today

1. **Prepare your organization for rapid response by adopting a state of heightened awareness** — This ranges from reviewing your security and emergency preparedness plans, consuming relevant threat intelligence, minimizing coverage gaps in personnel availability, and making sure your emergency call tree is up to date.
2. **Increase organizational vigilance** — Ensure your security personnel are monitoring key internal security capabilities and that they know how to identify anomalous behavior. Assess your access control protocols. Flag any known Iranian indicators of compromise and tactics, techniques, and procedures for immediate response.

3. **Confirm reporting processes** — Ensure your personnel know how and when to report an incident. The well-being of your workforce and cyber infrastructure depends on awareness of threat activity. Consider reporting your cyber incidents to CISA as part of an early warning system.
4. **Exercise your incident response plan** — Ensure your personnel are familiar with the key steps they need to take during an incident. Do they have the accesses they need? Do they know the processes? Are your various data sources logging as expected? Make sure personnel are positioned to act in a measured, calm, and unified manner.
5. **Confirm offline backup** — Ensure you have an offline backup of information critical to operations.

Actions for Cyber Protection

Ask the following questions about your organization to help mitigate cyberattacks:

1. **Backups:** Do we back up all critical information? Are the backups stored offline? Have we tested our ability to revert to backups during an incident?
2. **Incident Response:** Do we have an incident response plan and have we exercised it?
3. **Business Continuity:** Are we able to sustain business operations without access to certain systems? For how long? Have we tested this?
4. **Risk Analysis:** Have we conducted a cybersecurity risk analysis of the organization?
5. **Staff Training:** Have we trained staff on cybersecurity best practices?
6. **Account Protections:** Have we implemented multi-factor authentication and are we minimizing account privileges?
7. **Vulnerability Scanning and Patching:** Have we implemented regular scans of our networks and systems? Do we have an automated patch management program?
8. **Network Traffic Monitoring:** Are we monitoring the network traffic crossing the boundary of critical networks, including industrial control systems?
9. **Application Whitelisting:** Do we allow only approved programs to run on our networks?

Actions for Physical Protection

Ask the following questions about your organization to help mitigate physical attacks:

1. **Connect:** Do we have the right relationships in the community, including local law enforcement and your local Protective Security Advisor? Having these relationships established before an incident occurs can help speed up the response when something happens.
2. **Plan:** Do we have a plan for how we will handle a security event, such as an active shooter or bomb-related incident? (You can find guidance and technical assistance at CISA.gov to inform your plans.)
3. **Train:** Have we provided employees with training resources and exercises? Plans must be exercised to be effective.
4. **Report:** Do we know who to call, including local law enforcement, if we notice suspicious activity in or near a facility's entry/exit points, loading docks, parking areas, garages, and vicinity? "If You See Something, Say Something™" is more than just a slogan.
5. **Monitor and control:** Do we know who is entering our workplace, including current employees, former employees, commercial delivery, and service personnel?
6. **Store, lock, and inventory:** Do we effectively manage the organization's keys, access cards, uniforms, badges, and vehicles?

CISA's Role as the Nation's Risk Advisor

In collaboration with industry and government partners, CISA helps organizations understand and counter the risk of nation-state and non-state actors' malicious activity. CISA is providing recommendations to help partners stay vigilant and protected against potential cyber and physical threats.

Please visit CISA.gov for more information. We ask our partners with any relevant information or indication of a compromise to immediately contact us at cisaservicedesk@cisa.dhs.gov.