BARNES & THORNBURG LLP

ALERTS

Is Your Business Prepared For A Possible Iranian Retaliatory Cyberattack?

January 13, 2020 | Southeast Michigan | Atlanta | Chicago | Columbus | Dallas | Delaware | Elkhart | Fort Wayne | Grand Rapids | Indianapolis | Los Angeles | Minneapolis | Raleigh | Salt Lake City | San Diego | South Bend | Washington, D.C.

Current tensions between Iran and the United States, coupled with Iran's history of retaliatory cyber activities, have prompted the U.S. government to issue warnings about the possibility of such cyberattacks.

On Jan. 2, 2020, the United States carried out a lethal strike in Iraq, killing a top Iranian general. In response, Iranian leadership and several affiliated violent extremist organizations stated their intent to retaliate against the U.S.

The Cybersecurity and Infrastructure Security Agency (CISA) recently issued an alert regarding the "Potential for Iranian Cyber Response to U.S. Military Strike in Baghdad," recounts numerous prior actions by Iran through its Islamic Revolutionary Guard Corps (IRGC) against a variety of American industries, "including financial services, energy, government facilities, chemical, healthcare, critical manufacturing, communications, and the defense industrial base." For example:

- In late 2011 to mid-2013, Iranian actors performing work on behalf of the IRGC conducted website defacement and distributed denial of service (DDoS) attacks against the public-facing websites of U.S. banks, which prevented customers from accessing their accounts and cost the banks millions of dollars in remediation
- In February 2014, the Sands Las Vegas Corporation was hacked and customer data was stolen, including credit card,

RELATED PEOPLE

Jason A. Bernstein
Partner
Atlanta

P 404-264-4040
F 404-264-4033
jason.bernstein@btlaw.com

Scott N. Godes
Partner
Washington, D.C.

P 202-408-6928
F 202-289-1330
scott.godes@btlaw.com

Todd G. Vare
Partner
Indianapolis, Chicago

P 317-231-7735
F 317-231-7433
todd.vare@btlaw.com

Brian J. McGinnis
Partner
Indianapolis

P 317-231-6437
F 317-231-7433
brian.mcginnis@btlaw.com

RELATED PRACTICE AREAS

Social Security and driver's license numbers; the corporation's computer systems also were wiped clean

- In March 2018, the U.S. Department of Justice (DOJ) indicted nine Iranian actors for conducting a massive cyber theft campaign involving dozens of incidents involving hundreds of entities, including U.S. universities, domestic companies, the U.S. Department of Labor, the state of Hawaii, the state of Indiana, and more

The United States designated the IRGC as a Foreign Terrorist Organization on April 15, 2019, for its direct involvement in terrorist plotting. As a recent CISA bulletin discussing the terrorism threat to the U.S. notes, "Iran maintains a robust cyber program and can execute cyberattacks against the United States. Iran is capable, at a minimum, of carrying out attacks with temporary disruptive effects against critical infrastructure in the United States." The bulletin further warns that an "attack in the homeland may come with little or no warning."

Is your business prepared for a state-sponsored cyberattack ... or any cyberattack? There are things you should consider doing to help prevent and prepare for such an incident.

1. **Increase Vigilance and Awareness:** Ensure that business operations and information regarding possible threats are being carefully monitored. Assess whether there are new phishing exploits and follow best practices for restricting attachments via email.
2. **Incident Response Plan:** If your business does not already have an incident response plan, one should be put in place as soon as possible. It is best practice to include protocols on how and when personnel should report an incident, so there is a playbook to follow in the event of an attack.
3. **Data Backups:** A critical component to averting disaster in the event of an attack on your company's data is to back up essential data offline regularly and appropriately. Make sure the backups are stored in an easily retrievable location and test your ability to revert to backups during an incident.
4. **Employ MFA:** Implement multi-factor authentication (MFA) processes to help protect accounts.
5. **Password Strengthening:** Require strong passwords with regular change intervals. Do not use the same password for multiple accounts. Do not use common names or sequences in passwords.
6. **Penetration Testing:** If you have the capabilities internally, or through an experienced firm, attempt to breach the security of your business' systems to identify vulnerabilities. Also ensure that regular scans of your systems are done.
7. **Vulnerability Patching:** After you have tested your systems to assess potential vulnerabilities, any gaps in security should be patched immediately. In addition, consider an automated patch management program.
8. **Application Whitelisting:** Only allow approved programs to run on your networks.
9. **Ports and Protocols:** Continually monitor common ports and protocols for command and control activity. Review

network security device logs regularly to determine whether to disable unnecessary ports and change protocols.

For more information, contact the Barnes & Thornburg attorney with whom you work or Jason Bernstein at 404-264-4040 or jason.bernstein@btlaw.com; Scott Godes at 202-408-6928 or scott.godes@btlaw.com; Todd Vare at 317-231-7735 or todd.vare@btlaw.com; or Brian McGinnis at 317-231-6437 or brian.mcginnis@btlaw.com; or Adam Gajadharsingh at 404-264-4007 or adam.gajadharsingh@btlaw.com.

This Barnes & Thornburg LLP publication should not be construed as legal advice or legal opinion on any specific facts or circumstances. The contents are intended for general informational purposes only, and you are urged to consult your own lawyer on any specific legal questions you may have concerning your situation.