Robinson+Cole

Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

Department of Homeland Security Warns of Cyber-Attacks by Iran

The Department of Homeland Security (DHS) issued a grave warning to U.S. businesses and critical infrastructure operators on January 6, 2020, alerting the public that Iran poses a cyber terrorism threat to the United States following the death of Iranian Quds Force commander Gen. Qassem Soleimani. *Read more*

New York DFS Issues Risk Alert Concerning Possible Iran Cyber-Attacks

In view of Iran's vows to retaliate against the United States for the death of Quassem Soleimani, the NYDFS has issued an industry letter to all regulated entities regarding the need for heightened cybersecurity precautions. *Read more*

Health Information Sharing and Analysis Center Warns Health Systems to Be Wary of Iranian Cyber-Attacks

Following the escalation of tensions between the United States and Iran in the past week, the Health Information Sharing and Analysis Center (H-ISAC) is warning hospitals and health systems that Iran could attack health organizations, which are considered critical infrastructure, and that they make sure their systems are being updated with patches. *Read more*

Iranian Cyber-Attacks and the End of Support for Windows 7 and Windows Server 2008

After the killing of Qassem Soleimani on January 3, 2020, by the U.S. government, the cybersecurity news industry has been abuzz about whether Iran will engage in cyber terrorism, and if so, to what degree, as part of its pledge to strike back at the U.S. On January 5, Forbes reported that the first instance of Iranian cyber terrorism took place the day before. Hackers claiming to be associated with Iran defaced the home page of the Federal Depository Library Program website. The website was quickly taken down, but what do all this chatter and the possible increases of Iranian cyber espionage mean for U.S. businesses? *Read more*

January 9, 2020

FEATURED AUTHORS:

Linn Foster Freedman
Sean Lawless
Kathryn M. Rattigan
Norman H. Roos

FEATURED TOPICS:

Cybersecurity
Drones
New + Now
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

NEW + NOW

States and Municipalities on High Alert for Iranian Originated Cyber-Attacks

The Department of Homeland Security (DHS) is warning critical infrastructure operators to be on high alert for Iranian backed cyber-attacks because of the vulnerability of state and municipal computer systems, they are at high risk for attack from Iranian-based hackers. *Read more*

DRONES

FAA's Proposed Rule for Drone Remote Identification

The Federal Aviation Administration (FAA) released its unmanned aircraft system (UAS or drone) remote identification Notice of Proposed Rulemaking (Proposed Rule) on December 31, 2019. This is a huge step toward the integration of drones into the national airspace and an effective unmanned traffic management system. There is a 60-day public comment period; if you have a stake in the unmanned industry, you must submit comments before February 29, 2020. *Read more*

PRIVACY TIP #221

How Do We Personally Prepare for a Cyber-Attack on Critical Infrastructure?

This week's Privacy Tip is for those concerned that at some point in the future, we will experience a massive cyber-attack that may affect critical infrastructure that we depend on every day. *Read more*