NCSC Launches Campaign to Help Private Industry Guard Against Threats from Nation State Actors

The National Counterintelligence and Security Center (NCSC) is today disseminating videos, brochures, and other informative materials to help the private sector guard against growing threats from foreign intelligence entities and other adversaries.

“Make no mistake, American companies are squarely in the cross-hairs of well-financed nation-state actors, who are routinely breaching private sector networks, stealing proprietary data, and compromising supply chains. The attacks are persistent, aggressive, and cost our nation jobs, economic advantage, and hundreds of billions of dollars,” said NCSC Director William Evanina. “To enhance private sector awareness, we’re arming U.S. companies with information they need to better understand and defend against these threats.”

Recent examples underscore the foreign intelligence threats faced by U.S. companies:

- Last month, cyber actors associated with China’s Ministry of State Security were indicted by the U.S. for global computer intrusion campaigns targeting intellectual property, confidential business information, and other data at managed service providers, as well as at more than 45 U.S. technology companies and U.S. government agencies.

- In September 2018, U.S. charges were announced against a North Korean, state-backed hacker for his role in the Global WannaCry 2.0 ransomware, the cyberattack on Sony Pictures, spear-phishing attacks on U.S. defense contractors, and other activities.

- In March 2018, the FBI and Department of Homeland Security issued a joint technical alert about an ongoing intrusion campaign by Russian government cyber actors to reconnoiter U.S. energy sector networks.

- In March 2018, the U.S. levied charges against nine Iranians for a massive hacking campaign at the behest of Iran’s Islamic Republican Guard Corps that targeted intellectual property and other research at more than 144 U.S. universities.

“Know the Risk, Raise Your Shield”

Accordingly, NCSC is distributing its trademarked “Know the Risk, Raise Your Shield” materials specifically to raise awareness among private sector organizations and equip them with best
practices for protecting their data, assets, technologies, and networks. These materials were previously distributed to raise awareness in the federal workforce.

The “Know the Risk, Raise Your Shield” materials are featured on NCSC’s website (NCSC.gov) or at https://www.dni.gov/ncsc/knowtherisk/tools/ and include videos, posters, brochures, and flyers. They address numerous topics, including supply chain risks, economic espionage, social engineering, social media deception, spear-phishing, mobile device safety, and foreign travel risks. At a minimum, the materials provide basic tips to help mitigate risks faced by the private sector. These include:

- **Corporate supply chains** are growing targets of foreign intelligence entities. Adversaries are bypassing hardened corporate defenses by using less-secure suppliers and vendors as surreptitious entry points to surveil, sabotage, and steal information from companies’ networks. Supply chain security can be expensive, but lack thereof is costlier and can result in pronounced, long-lasting damage. This is a place where an ounce of prevention is worth a pound of cure. **TIP:** Know your suppliers, the equipment and services they provide, and their service providers. Ask the right questions before procuring their products or services. Integrate acquisition and procurement personnel into your organization’s enterprise-wide risk management and security program.

- **Spear-phishing e-mails**, in which the recipient is asked to click on a link or attachment, remain a common tool for foreign intelligence entities to compromise networks and access data. In October 2018, two Chinese intelligence officers and eight others were indicted for hacking U.S. and European aerospace firms over five years to steal trade secrets on commercial aircraft engines. They allegedly used spear-phishing and other tactics to penetrate company networks. **TIP:** Never click on suspicious links or attachments, particularly from unverified or unknown sources.

- **Social media deception** is another technique used to target private sector individuals. Adversaries may create fake profiles on social media, posing as a job recruiter or someone with a shared interest, to connect with and elicit information from business persons. China’s intelligence services use social media platforms to spot, assess, and target Americans with access to business or government secrets. A former CIA officer convicted of espionage conspiracy in 2018 was first approached by a Chinese intelligence operative posing as a job recruiter on social media. **TIP:** Maximize your social media privacy settings; use caution in what you share; never accept friend requests from strangers; and validate friend requests through other sources.

- **Foreign travel** presents critical risks to private sector individuals, particularly those bringing smart phones, laptops or other electronic devices. When abroad, don’t expect electronic privacy. Wi-Fi networks overseas are regularly monitored by security services and others who can insert malicious software into your device through any connection they control. They can also do it remotely if your device is enabled for wireless
connection. **TIP:** If possible, leave your electronic device at home. If you bring it, always keep it with you; the hotel safe isn’t really “safe.”

**Foreign Economic Espionage in Cyberspace**

Another resource available to the private sector is NCSC’s 2018 *Foreign Economic Espionage in Cyberspace* report, which provides the latest unclassified information on foreign intelligence efforts to steal U.S. intellectual property, trade secrets, and proprietary data via cyberspace.

Released in July 2018, the report identifies the most pervasive nation-state threat actors, including China, Russia and Iran; those U.S. industrial sectors of greatest interest to foreign threat actors; and several emerging threats that warrant attention, including:

- Software supply chain infiltration, which has already threatened the U.S. critical infrastructure and is poised to threaten other sectors.
- Laws in foreign countries, such as those in China and Russia, that can pose an increased intellectual property risk to U.S. companies doing business there.
- Foreign technology firms that are subject to foreign state influence or have links to foreign governments with high-threat intelligence services.

NCSC is a center within the Office of the Director of National Intelligence. NCSC is the nation’s premier source for counterintelligence and security expertise and a trusted mission partner in protecting America against foreign and other adversarial threats.

# # #