Texas Council Risk Management Fund

In the Cyber War, Russia is our Top Enemy

In the wake of Russia's invasion of Ukraine, it makes sense to wonder: Should America be worried about cyberattacks right now? A variety of attacks and scenarios are a possibility.

One way to gauge what potential Russian attacks could look like is to analyze past events. Since 2015, when a Russian attack took out Ukraine's electrical grid, Ukraine has worked hard to shore up its digital defenses. But in 2017, NotPetya, a Russian cyberattack against Ukraine that spread around the world, still caused billions of dollars in damages. There was also the 2021 Solar Winds attack, which targeted American companies like Microsoft and Intel, as well as various American federal agencies, including the Pentagon, the Department of Homeland Security, and the National Nuclear Security Administration, leaving them exposed.

Now, with America imposing sanctions on Russia, many fear a retaliatory attack. On March 17th, the FBI and CISA, the Cybersecurity and Infrastructure Security Agency, warned that they were "aware of possible threats to U.S. and international satellite communication (SATCOM) networks," and they urged network providers and customers to harden their defenses. CISA has been advising American entities to put their "shields up" to deter attackers, and in March, Congress approved legislation that requires critical infrastructure companies to report cyber intrusions within seventy-two hours of an attack and to report within twenty-four hours after paying a ransom. The new requirements will give CISA a better understanding of how our adversaries are targeting entities such as pipelines, dams, and the electric grid, and allow the agency to warn other entities of ongoing threats.

Aside from cyber intrusions and breaches, Americans can expect to see Russian-sponsored cyber activities working in tandem with propaganda campaigns. These activities are aimed at preventing a united response to Russian aggression in Ukraine. The specific plans aim to bolster narratives, people and groups that support Russian interests and undermine those that go against Russian interests. The activities, which include dismissing and distorting information and undermining opinion leaders, are carried out in the press and on social media.

History shows that Russia is most likely to recruit proxies to carry out cyberattacks that disrupt decision-making so that the attacks don't point directly back to the Russian Government. The "Fog of War" is enhanced with the use of cyberspace. That is one of the main benefits of cyberspace as an element of warfare – a cyberattack almost always allows for plausible deniability. On January 14, 2022, Russia arrested members of the Russian-based cyber gang REvil who were responsible for the 2021 ransomware attacks against meat supplier JBS Foods, headquartered in Greeley, Colorado, and the Colonial Pipeline, headquartered in Alpharetta, Georgia. The move caused cybersecurity analysts to wonder about Russia’s motive, including speculation about making it easier for the government to deny a connection to the cyberattacks.

Businesses and governmental agencies responsible for critical infrastructure and high-profile targets should ensure they are adequately prepared with best practice prevention, detection, and incident response measures to deal with advanced persistent threats.

- Assess infrastructure technologies, procedures, and recovery plans to ensure they are up to date and hardened.
- Reinforce key controls and gaps found in assessments.
- Confirm backups and restoration procedures are successful. Test backups as part of a monthly maintenance window.
- Review existing agreements with third party entities such as network providers and contractors.
- Review all technologies involved with remote workforce operations. Confirm all remote or external access points are hardened and covered with current versions of end-point detection technologies.
- Leverage credible cyber threat intelligence for information and news regarding threats. The CISA “Shields Up” (https://www.cisa.gov/shields-up) website provides information on how to improve cybersecurity and protect critical assets, along with immediate recommendations of cyberattack prevention actions for all U.S. businesses.

You may access member only cyber security resources including policies, procedures, and best practices by visiting the TCRMF website page, Cyber Security, located at the top of the page. This is a secure, member only page that requires a login. If you need to obtain login credentials, you can request one at this link: Login Request Form.

For information on the Texas Council Risk Management Fund Cyber Risk Control Program or IT Risk Assessments, contact Lee Cain, IT Risk Control Consultant, by email: Lee.Cain@sedgwick.com or by phone: 512-427-2322 or 800-580-6467 extension 12322.