BRACEWELL

INSIGHTS

Quick Hit: Russian Sanctions and Cybersecurity

March 2, 2022

*By: **Matthew G. Nielsen***

On this episode of The Bracewell Sidebar, we look beyond Russia's invasion of Ukraine at the business and legal implications of the Russian sanctions, as well as at cybersecurity issues.

What do companies, organizations and individuals need to know about the rapidly evolving sanctions regime?

There are two primary methods of imposing sanctions: one by the Commerce Department, another by the Treasury Department. Treasury will issue sanctions to prevent people from doing business in certain regions of the world and with certain people and specifically also relating to financial business and banking relationships. Commerce is going to be involved in restricting selling certain types of goods and technology. So, there's a large scale coordinated effort here, not only with the US side, but with our partners around the world, including the EU, UK and other countries issuing similar sanctions in an unprecedented manner with such a large global power as Russia.

What's going to happen with the energy export market with Russia and the energy technology import market in Russia?

The United States is still holding out the possibility of targeting the energy sector. Europe has been a bit more aggressive on that. They're a little bit more reliant on Russian energy exports than the United States is. While there hasn't been a direct targeting of the Russian energy, what requires a license to export to Russia has been greatly expanded over this last weekend. The reality is that if you're trying to export goods or software to Russia, you need to pay close attention because military end use has been expanded significantly for the vast majority of exports. There's going to be prohibitions against exporting to certain people in certain regions, and there is a now presumption of denial of those exports.

There's been a ton of attention paid to the sanctions that have been added to deal with Russia, but not that much of a reminder put out that export controls, not necessarily sanctions, but export controls on technology with a direct or perhaps indirect but otherwise military application are still covered by a fairly detailed and, in some cases, time-consuming license application process.

On the Office of Foreign Assets Control side, what the US is doing and what our allies in Europe are doing is essentially shutting off Russian access to the financial markets and banking markets. We saw that the Russians have been removed from the SWIFT automation that allows them to easily transact business with banks throughout the world. The assets of the central bank and large, other closely held government banks have been blocked and are being held, so

the government can't offset these sanctions.

What might we expect to see specifically relating to potential cyberattacks?

From what initial reports look like, Ukraine was bombarded with a variety of different cyberattacks in the days leading up to Russia's invasion. The initial analytics of some of those attacks suggest that the systems that were affected had most likely been impacted or infected weeks and weeks ahead of time and that malicious code had been lying dormant in wait for this moment to happen. The effect is similar to ransomware in that systems are crippled. But there's a hugely significant difference in that ransomware is, at the end, a commercial transaction where hackers will presumably return systems to normal or near normal in exchange for money. In these politically motivated attacks like the hackers conducting the attacks on Ukrainian systems, they used data wiping malware rather than data encrypting malware. And they also distributed something called denial of service attacks, which are essentially flooding systems with false pings to cripple them and render them ineffective. So the systems really are not the final target of these kinds of politically motivated attacks. Instead, the idea is to target systems because they play a role in critical infrastructure, such as airport management or power grid management or other necessary communications and they essentially make it impossible for networked activities to function as normal, which creates uncertainty and in some cases, chaos.

What are the potential implications of the supply chain disruption?

It can start raising some legal issues if you essentially can't fulfill your contractual obligations because of circumstances beyond your control. And that certainly can be a possibility if the supply chain is disrupted, but this is a purely contractual matter. It's one in which you have to pay close attention to your particular contracts, because they may have notice requirements and preconditions to invoking that. But that's certainly something that people need to be on the lookout for is essentially either because of the effects of sanctions directly or indirectly, you're unable to get goods or services that are needed to fulfill your other contractual obligations.

Have questions about the potential business and legal implications of sanctions against Russia? Contact Bracewell's ***government enforcement and investigations team***.

The opinions expressed in this podcast are those of the speakers and do not necessarily reflect the viewpoint of their institutions or clients.