MAYER | BROWN

February 23, 2022

Legal Update

Russian Military Action in Ukraine: Measures to Mitigate Related Cyber Risk

After months of diplomatic engagement, the early morning of February 24, 2022 saw what President Biden called an "unprovoked and unjustified attack by Russian military forces" on Ukraine. Numerous news reports also have described significant cyber attacks against Ukrainian systems. According to those reports, these attacks follow multiple waves of cyber attacks in the past few weeks that have targeted Ukrainian banks and government websites, including those of the Ukrainian parliament, and ministries of foreign affairs and defense.[1] As Ukrainian systems are targeted, businesses around the world are at risk of spillover effects, the spread of any new malware beyond Ukraine's borders, and the risk of increased ransomware attacks. In this Legal Update, we highlight recent security recommendations that can serve as resources for companies working to protect their systems during this period of acute cyber risk.

The United States and many other nations have already taken action in response to Russian actions, including imposing sanctions that have significant implications for private sector businesses. (We discuss these sanctions here and further information can be found at our Ukraine Crisis portal.) In addition, US federal agencies are advising that Russian cyber attacks will not be limited to Ukraine. In a recent Shields Up notice, the Cybersecurity and Infrastructure Security Agency (CISA) advised that "every organization in the US is at risk from cyber threats that can disrupt essential services and potentially result in impacts to public safety."[2] While CISA advised that, at that time, it saw no "specific credible threats to the US," it was "mindful of the potential for the Russian government to consider escalating its destabilizing actions in ways that may impact others outside of Ukraine."[3] Businesses will likely benefit from continued monitoring for any further recommendations from CISA in the coming weeks on mitigating these cyber risks.

US government agencies also have recently stepped up outreach to private sector entities, including critical infrastructure, through broad-based channels and private engagement to stress the importance of maintaining an enhanced cybersecurity posture. Anne Neuberger, Deputy National Security Advisor for Cyber and Emerging Technology, stated, "we've been working with the private sector, engaging, sharing specific information, requesting that they act to reduce the cybersecurity risk of their organization, and providing very focused [sic] advice on how to do so."[4] Earlier this year, CISA, the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA) issued a joint advisory warning critical infrastructure entities to remain vigilant against Russian state-sponsored

attacks and outlined a number of mitigations organizations should consider implementing to help reduce cyber risk. The advisory was quickly endorsed by the UK intelligence agency, National Cyber Security Centre, a division of Government Communications Headquarters.

Additionally, leading cybersecurity firms, including CrowdStrike, Microsoft, Palo Alto Networks, and Mandiant likewise reported increased cyber activity linked to Russia and recommended implementing a variety of security hardening measures to better safeguard an organization's systems and data, many of which overlap with the recommendations listed in government advisories.

Key recommended hardening measures include:

- Implement multi-factor authentication for all users, without exception,
- Secure credentials and set a strong password policy for service accounts,
- Update software and prioritize patching known exploited vulnerabilities,
- Ensure backup data is offline and secure,
- Disable all unnecessary ports and protocols,
- Use network monitoring tools and host-based logs and monitoring tools, such as endpoint detection and response, and
- Create, maintain, and exercise a cyber incident response and business continuity plan.

In addition, below are some key steps to take if your organization has systems or data in Ukraine, based on input from our leading cybersecurity partners:

- Ensure that Ukraine-related data is backed up in a secure location outside of Ukraine,
- Ensure that off-site backups are not accessible from the Ukraine-based systems in an over-writable fashion,
- Ensure systems are segmented appropriately,
- Assess third-party/vendor access to your organization's systems, and
- Be on heightened alert for insider threats (both malicious and unwitting) at this time.

News reports continue to highlight the cyber risks to US and multinational businesses arising from the military action in Ukraine. Businesses, especially those with Ukraine-based IT and data exposure and those that operate US critical infrastructure, will be well-served to continue to carefully consider cybersecurity guidance from relevant governments and private-sector experts and to engage through available cyber threat information-sharing channels such as information sharing and analysis centers (ISACs) or direct government engagement.

For more information about the topics raised in this Legal Update, please contact any of the following lawyers.

Rajesh De
+1 202 263 3366
rde@mayerbrown.com

David A. Simon
+1 202 263 3388
dsimon@mayerbrown.com

Marcus A. Christian
+1 202 263 3731
mchristian@mayerbrown.com

Stephen Lilley
+1 202 263 3865
slilley@mayerbrown.com

Vivek K. Mohan
+1 650 331 2054
vmohan@mayerbrown.com

Veronica R. Glick
+1 202 263 3389
vglick@mayerbrown.com

Meredith L. Lussier
+1 202 263 3480
mlussier@mayerbrown.com

Joshua M. Silverstein
+1 202 263 3208
jsilverstein@mayerbrown.com

Endnotes

[1] Ines Kagubare, *Ukraine government websites down in latest cyberattack*, THE HILL (Feb. 23, 2022), https://thehill.com/policy/cybersecurity/595520-ukraine-government-websites-down-in-latest-cyberattack; Eric Tucker, *US, Britain Accuse Russia of Cyberattacks Targeting Ukraine*, AP NEWS (Feb. 18, 2022), US, Britain accuse Russia of cyberattacks targeting Ukraine | AP News.

[2] CISA, *Shields Up* (2022).

[3] Id.

[4] Anne Neuberger, *Online Press Briefing with Anne Neuberger, Deputy National Security Advisor for Cyber and Emerging Tech*, US DEPARTMENT OF STATE (Feb. 2, 2022), Online Press Briefing with Anne Neuberger, Deputy National Security Advisor for Cyber and Emerging Tech - United States Department of State.