WILLKIE FARR & GALLAGHER LLP

CLIENT ALERT

Concerns Over Heightened Cyber Threats Highlight the Need to Be Ready

February 28, 2022

AUTHORS

Daniel K. Alvarez | Laura E. Jehl | Richard M. Borden | Kari Prochaska
Amelia Putnam

In the days since Russian President Vladimir Putin announced his order for Russian military units to invade Ukraine, observers around the world have seen a significant surge in harmful cyber activity. In particular, key Ukrainian government officials, critical infrastructure, and civil society websites and networks have been under attack. Even prior to the invasion of Ukraine, however, numerous U.S. government officials, including Jen Easterly, Director of the Cybersecurity and Infrastructure Security Agency ("CISA"), began warning that disruptive cybersecurity attacks could reach well beyond the borders of Ukraine. Those warnings have continued and gained urgency in light of Russian military actions and threats, along with a strong, diversified Western economic response.

The Ukraine conflict has escalated quickly, and the cybersecurity threat landscape is fluid and rapidly evolving. To date, the response by the U.S. government has been focused on raising awareness and encouraging preparedness by government agencies and private sector entities who might be targeted by cyberattacks. In this client alert, we highlight some of the key issues raised by CISA and others, and describe steps that organizations should consider taking to reduce the likelihood of becoming victims of malicious cyber activity.

<u>U.S. Government Raising Cybersecurity Alarm Bells</u>

- On its "Shields Up" webpage, CISA notes that "Russia's unprovoked attack on Ukraine, which has involved cyber-attacks on Ukrainian government and critical infrastructure organizations, may impact organizations both within and beyond the region, particularly in the wake of sanctions imposed by the United States and our Allies. Every organization—large and small—must be prepared to respond to disruptive cyber activity."[1]

- In a joint advisory published on February 26, 2022, the Federal Bureau of Investigation ("FBI") and CISA highlighted specific examples of "destructive malware [deployed] against organizations in Ukraine to destroy computer systems and render them inoperable."[2] These malware incidents included:
    - "On January 15, 2022, the Microsoft Threat Intelligence Center disclosed that malware, known as WhisperGate, was being used to target organizations in Ukraine. According to Microsoft, WhisperGate is intended to be destructive and is designed to render targeted devices inoperable."
    - "On February 23, 2022, several cybersecurity researchers disclosed that malware known as HermeticWiper was used against organizations in Ukraine. According to SentinelLabs, the malware targets Windows devices, manipulating the master boot record, which results in subsequent boot failure." The malware, which is capable of erasing all data from infected systems, was discovered to have been installed on hundreds of systems across Ukraine.

- On February 25, 2022, the Conti group, a Russian-based ransomware group, announced its "full support" of the Russian government and issued a warning that "If anybody will decide to organize a cyberattack or any war activities against Russia, we are going to use all our possible resources to strike back at the critical infrastructures of an enemy."[3] Other ransomware groups soon followed, posting their own political allegiances and the predicted effect of those allegiances on their ransomware activities.

- Additionally, Ukrainian government authorities, banks, and other entities have experienced a number of distributed denial-of-service ("DDoS") attacks.[4] DDoS attacks can crash a website by flooding the website with requests. The effects of DDoS attacks are twofold: (i) critical websites can be knocked offline, and (ii) the attacks drive up fear in individuals, particularly in Ukraine, that major Ukrainian businesses and the government do not have sufficient control over critical infrastructure.

[1] *Shields Up*, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, available here.

[2] *Alert (AA22-057A) Destructive Malware Targeting Organizations in Ukraine*, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY and FEDERAL BUREAU OF INVESTIGATION (Feb. 26, 2022), available here.

[3] Christopher Bing, *Russia-based Ransomware Group Conti Issues Warning to Kremlin Foes*, REUTERS, (Feb. 25, 2022), available here. Two days later, however, an individual believed to be a Conti member began leaking data along with a strongly pro-Ukraine message.

[4] Joe Tidy, *Ukraine Crisis: 'Wiper' Discovered in Latest Cyber-Attacks*, BBC NEWS (Feb. 24, 2022), available here.

Cybersecurity Risks Abound

In the short term, the primary risks many companies face include operational, financial, and reputational risks associated with a potential incident. If companies fail to take steps to bolster their cybersecurity and are the victims of a cyberattack, they may also face increased legal risks, including enforcement actions by government authorities and litigation initiated by affected individuals or contractual partners. Failure to act now could open the door to liability under various state and federal data security laws. For example, depending on a company's business, it could face liability under the New York Department of Financial Services Cybersecurity Regulation, the Gramm–Leach–Bliley Act, the Health Insurance Portability and Accountability Act, the California Consumer Privacy Act, or be subject to enforcement action by the Federal Trade Commission or State Attorneys General for unfair or deceptive trade practices or for violations of other consumer protection laws. Companies may also have incident-specific considerations, such as data breach reporting for incidents involving personal information. Additionally, affected entities may have contractual obligations related to cybersecurity or business disruptions; to the extent that a data security incident causes a breach of these obligations, entities may be liable.

Protective Steps to Take

As the risk of cybersecurity attacks increases, particularly related to Russian cyber activity, companies should immediately evaluate their cybersecurity practices and prepare for potential cybersecurity attacks. Proactively, companies should take these key steps:

- **Bolster cyber defenses.** In its alert, CISA highlights at least five steps companies can take in the short term:

  1. Enable multifactor authentication;
  2. Set antivirus and anti-malware programs to conduct regular scans;
  3. Enable strong spam filters to prevent phishing emails from reaching end users;
  4. Update software; and
  5. Filter network traffic.

CISA provides additional technical guidance resources on its website, located here.

- **Monitor ongoing alerts from the FBI, CISA or other U.S. government sources.** The conflict in Ukraine is evolving rapidly and the cyber threat landscape is likely to change along with it. Companies should consider designating certain personnel to monitor alerts from the federal government. For quick reference, CISA's latest alerts on its Shields Up website are located at https://www.cisa.gov/shields-up.

- **Test cyber defenses.** Regular penetration and vulnerability testing is an important part of a data security program and also central to compliance with a number of data security and cybersecurity laws and regulations. CISA offers many free tools, located on its website at https://www.cisa.gov/free-cybersecurity-services-and-tools, to help companies perform these important tasks. Director Easterly has encouraged companies of all sizes to take advantage of these resources.

- **Assess backup restoration capability.** A company's data backup capabilities are crucial, particularly in light of the potential use of HermeticWiper, which has been used in Ukraine and is known to destroy all of the data on a data system. In the event of a ransomware or wiper attack, companies must have in place strong backup procedures that allow systems to be recovered in the event that data on a local system is destroyed or encrypted.

- **Advise employees to be on heightened alert for any anomalous activity.** Immediately address the importance of employee vigilance with respect to phishing or other attempts to gain access, and train employees to immediately escalate such incidents according to the company's vulnerability and incident response policies and procedures. Early identification of potential incidents is key to limiting the impact of malicious activity.

- **Prepare for a cybersecurity incident.** Implement a response plan to respond to security incidents, including to ensure business continuity in the event that key communications and other systems are compromised as part of an attack. Companies should also identify and consider retaining forensic security, legal, and communications resources to consult in the event of an incident, including a quick reference of the contact information for the company's cyber liability insurance carrier. Third parties, including those with whom companies do not have a direct relationship, may pose the greatest risks. Consider fourth parties (e.g., third parties of third parties) and others in the incident response plan.

- **Focus on ransomware incidents and DDoS attacks.** Ransomware is likely to be an attractive option for entities in Russia seeking access to liquidity after the imposition of U.S. sanctions against Russia. Certain ransomware groups are already sanctioned entities to whom payments are prohibited. It is possible that other ransomware groups could be added to the sanctions list if the U.S. government believes that payments to those groups could be used to circumvent existing sanctions against Russia. Additionally, DDoS attacks are potentially disruptive cyber activity that companies should be aware of and prepared for if they rely on their websites or any other system that could be overwhelmed by a DDoS incident. To secure against DDoS attacks, companies should assess and may need to reconfigure their hardware.

- **Review key customer contracts.** Companies should assess where key customer contracts are stored on its systems and be prepared to review potential notification and business disruption obligations if either (i) the company or (ii) the services of an important partner, vendor, or supplier are interrupted by a cyberattack.

- **Maintain oversight responsibilities.** Company boards and executives should recalibrate their oversight and reporting approach for cyber issues and incidents to ensure key people in their organizations have access to the best and most accurate information.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Daniel K. Alvarez 202 303 1125 dalvarez@willkie.com	**Laura E. Jehl** 202 303 1056 ljehl@willkie.com	**Richard M. Borden** 212 728 3872 rborden@willkie.com	**Kari Prochaska** 312 728 9080 kprochaska@willkie.com
Amelia Putnam 202 303 1089 aputnam@willkie.com			

This alert is provided by Willkie Farr & Gallagher LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This alert may be considered advertising under applicable state laws.

Willkie Farr & Gallagher LLP is an international law firm with offices in Brussels, Chicago, Frankfurt, Houston, London, Los Angeles, Milan, New York, Palo Alto, Paris, Rome, San Francisco and Washington. The firm is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our fax number is (212) 728-8111. Our website is located at www.willkie.com.