COVID-19: Sophisticated Cyberattacks Increasingly Targeting Pharmaceutical Research and Health Data Related to Vaccines, Treatments and Testing

July 17, 2020

AUTHORS

Daniel K. Alvarez | Heather M. Schneider | Elizabeth P. Gray | Elizabeth Bower
Richard M. Borden | Philip F. DiSanto

Sophisticated state-sponsored cyberattacks are increasingly targeting major pharmaceutical companies, research institutions, and other organizations researching COVID-19 vaccines, treatments, and testing. On July 16, 2020, U.S., U.K., and Canadian national security authorities warned that a Russian state-sponsored cyberespionage group ("Cozy Bear") is specifically targeting organizations with the "highly likely . . . intention of stealing information and intellectual property relating to the development and testing of COVID-19 vaccines." This joint warning follows a May 13, 2020 warning from the FBI and U.S. Cybersecurity and Infrastructure Security Agency ("CISA") that Chinese state-sponsored cyber actors are also targeting COVID-19-related research. Both national security warnings noted the serious risk that such cyberattacks are jeopardizing the development and delivery of safe and effective COVID-19 treatments in the midst of the global pandemic.

Organizations involved in pharmaceutical, biotechnology, and healthcare research and development—particularly those developing potential COVID-19-related vaccines and treatments—should be aware of the potentially significant cyber-risks in the current environment and take measures to protect against those risks.

Prior Cyberattacks Against Pharmaceutical and Biotechnology Organizations

Pharmaceutical and biotechnology organizations have long been targeted by sophisticated cyberattacks due to the valuable research and IP held by such organizations. Because the development of a new vaccine or treatment often involves many years of research, hundreds of millions (if not billions) of dollars, and rigorous governmental approval processes that require significant supporting data, a single cyberattack can have a major impact on both development of the specific product and on the organization itself.

Sophisticated state-sponsored actors have been responsible for some of the most serious cyberattacks on pharmaceutical and biotechnology organizations in recent memory. For example, since at least 2013, Chinese state-sponsored groups have reportedly targeted pharmaceutical and biotech-related research organizations, as well as cancer research organizations and conferences, with zero-day exploits and targeted spear-phishing campaigns designed to steal or exfiltrate data. As another example, the 2017 "NotPetya" malware attack—which was purportedly released by Russian intelligence services—caused a worldwide shutdown in numerous companies' operations for weeks or months, including in the pharmaceutical industry. Another purportedly state-sponsored cyberattack that affected the pharmaceutical industry in 2019 involved malware designed to provide remote access to internal company networks.

Recent COVID-Related Cybersecurity Warnings

The two recent national security warnings concerning ongoing cyberattacks against organizations performing COVID-related research indicate that such attacks are focused on the identification and theft of valuable research and IP. In particular, authorities have warned that at least one state-sponsored actor recently exploited vulnerabilities in Citrix and VPN systems and used spear-phishing campaigns to obtain login credentials to internet-accessible login pages for the organizations targeted. After obtaining access to a target organization's systems, a bad actor can deploy custom malware designed to exfiltrate data from those systems.

Prior cyberattacks against major pharmaceutical companies demonstrate that organizations conducting COVID-related research are also at high risk of sophisticated ransomware attacks. As discussed in a recent webinar hosted by Willkie and featuring a colleague from KPMG, ransomware is now often deployed in targeted attacks to encrypt a victim's data and then hold that data hostage. As companies and nation-states race to develop effective vaccines and treatments for COVID-19, there is a significant risk that such attacks could be used to impede research and development, manufacturing, and other operations for competitive advantage.

Responding to the Increased Risk of Sophisticated Cyberattacks

Pharmaceutical, biotechnology, and other research organizations can take several measures to protect against and mitigate the risks of sophisticated cyberattacks. These measures may include:

- **Maintaining a Comprehensive Information Security Program.** Comprehensive written information security programs should be designed to protect the security, integrity, and availability of the company's data and information technology systems, as well as the confidentiality of the data stored on those systems. Business continuity is a particular issue to consider with ransomware. Public companies and other regulated organizations should also consider applicable guidance from government agencies and regulatory organizations concerning the contents of such a program.

- **Developing and Testing an Incident Response Plan.** A flexible incident response plan helps to ensure that a company is prepared for a cyber-incident by putting procedures in place to identify what happened, what aspects of the company were affected, and what steps need to be taken to control, mitigate damage, and recover from the incident. Testing the incident response plan through simulated tabletop exercises also helps to ensure that an incident response plan is appropriately tailored to the organization.

- **Practice Remote Work Cybersecurity Hygiene.** The recent government warnings indicate that cyber actors are attempting to exploit technologies that are essential to the COVID-19 remote work environment, such as VPN and other remote access software. As a result, practices such as patch management, active vulnerability scanning, and multi-factor authentication remain important to protecting against unauthorized access.

- **Actively Synthesize IP and Cybersecurity Strategies**. To protect valuable research and IP through all phases of the new drug pipeline or product development cycle, companies can ensure that their cybersecurity programs, policies, and protections are tailored to the company's IP portfolio and strategy. As companies incorporate additional internet-connected, IoT, and operational technology (OT) equipment and AI solutions into research and development processes and products, the potential cyberattack vectors may continue to multiply. Ensuring that systems holding the most valuable research data, as well as the equipment used to generate that data or conduct clinical trials, have adequate cybersecurity measures in place will help to ensure that a company's most valuable research and IP are protected through inception, regulatory approval, and commercialization.

These are only some of the measures that companies can take to protect against the increased threat of cyberattacks targeting COVID-related research. We are available to help you address the specific cybersecurity and IP issues that you are facing through the COVID-19 pandemic and to develop and implement appropriate measures to respond to those specific issues.

Willkie has multidisciplinary teams working with clients to address coronavirus-related matters, including, for example, contractual analysis, litigation, restructuring, financing, employee benefits, SEC and other corporate-related matters, and CFTC and bank regulation. Please click here to access our publications addressing issues raised by the coronavirus. For advice regarding the coronavirus, please do not hesitate to reach out to your primary Willkie contacts.

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

Heather M. Schneider
212 728 8685
hschneider@willkie.com

Elizabeth P. Gray
202 303 1207
egray@willkie.com

Elizabeth Bower
202 303 1252
ebower@willkie.com

Richard M. Borden
212 728 3872
rborden@willkie.com

Philip F. DiSanto
212 728 8534
pdisanto@willkie.com