LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

COVID-19 Vaccine Hacking May Prompt Data Security Rethink

By **Allison Grande**

Law360 (July 24, 2020, 10:38 PM EDT) -- Warnings that cyberattackers backed by the Chinese and Russian governments are targeting COVID-19 vaccine research drive home the need for companies to think beyond their regulatory obligations to protect personal information and to ensure that their intellectual property is shielded from evolving cyber threats.

In a joint July 16 alert, government officials from the U.S., U.K. and Canada put companies on notice that a Russia-linked group known as Cozy Bear has carried out a series of attempted online attacks on organizations working to research and develop a vaccine for the coronavirus that causes COVID-19. The advisory came on the heels of a similar warning issued by U.S. officials in May that malicious users backed by the Chinese government are aiming to steal American research on vaccines and treatments for the virus.

The threats highlight the evolving, aggressive methods of nation-state-backed cyberattacks, but also the risks of holding sensitive information that is enticing to bad actors for its competitive value rather than for the more common motivations of making money or wreaking havoc.

"Companies need to move away from the mindset that all hackers care about is personally identifiable information, like credit cards and Social Security numbers," said Aaron Charfoos, a partner in the privacy and cybersecurity practice at Paul Hastings LLP. "They need to think about the new threat landscape that's out there, where hackers are going after confidential commercial information and critical systems, whether they contain personally identifiable information or not."

The attackers' objectives for targeting the West's COVID-19 research data — which both Chinese and Russian government officials have adamantly denied — remain unclear. But experts say it's more likely that the recent activity is cyber espionage designed to ensure that the countries don't miss out on the life-saving and economic benefits of a vaccine rather than an effort to damage or interfere with vaccine development.

"Anytime a company has something of value, it becomes a target for hacking," said Jena Valdetero, co-head of the data privacy and security team at Bryan Cave Leighton Paisner LLP. "The U.S. government is making clear that it won't tolerate such attacks on American companies."

Guarding Intellectual Property

The latest alerts also highlight the importance of protecting all the confidential information companies hold, attorneys say.

"When talking to companies that have an incident, their main concerns are usually hitting their regulatory obligations, and there's often a lack of awareness and concern about what other information might be involved and what impact that might have on the business," said Liz Harding, a shareholder at Polsinelli PC.

In recent years, laws like the European Union's General Data Protection Regulation and California's landmark Consumer Privacy Act have forced companies to ramp up protections for the personal consumer data that they hold or be subjected to enforcement actions, hefty regulatory fines and private litigation.

But the same requirements and regulatory risks don't apply to protecting intellectual property and other corporate data, meaning that these kind of threats — which malicious users typically execute using the same phishing and malware tactics they rely on to steal personal information — are more prone to fall through the cracks.

"What's gotten lost in cybersecurity for companies is the significance and potentially detrimental impact of IP theft, because there's been such an outsized focus on regulatory compliance with privacy directives and the protection of personal information," said Ed McAndrew, a former federal cybercrime prosecutor and current cybersecurity partner at DLA Piper. "But just because there aren't the same compliance burdens with respect to IP, that doesn't mean the threats to IP are any less important or severe."

While the health care industry was an enticing target for cyberattacks before the pandemic, they have spiked since COVID-19 emerged.

The World Health Organization reported a 500% increase in cyberattacks on its systems as the pandemic started to spread, and a biotech company disclosed in a securities filing in March that it had suffered a ransomware attack that involved the theft of certain company data, said Ashley L. Thomas, an attorney at Morris Manning & Martin LLP.

"The security challenges are heightened by the fact that many health care entities now have large remote workforces, which can expose security vulnerabilities and lead to cyberattacks," Thomas said. "Implementing effective cybersecurity policies and incident response procedures was a necessity before the pandemic, and it is critical now to adopt these measures."

'Risk to Their Own Livelihoods'

Ensuring that these vital corporate assets are being protected requires companies to take a more holistic view of what data they hold and ensure that their protections extend to all of this information.

"No matter what industry they're in, when we talk to clients we say, 'What are your crown jewels? What are the things that if they're taken or compromised would cause you the biggest harm?'" said Laura Jehl, who heads the privacy and cybersecurity practice at McDermott Will & Emery LLP.

While larger companies like the pharmaceutical giants funding vaccine research typically have the means to conduct such an analysis, smaller entities like the nonprofit academic institutions conducting key research may lack the resources, particularly if they've been hit hard economically by the COVID-19 pandemic, said Linda Malek, chair of the health care and privacy and cybersecurity practices at Moses & Singer LLP.

"Putting resources into beefing up cybersecurity perhaps hasn't been at the top of the list, but those priorities have to shift now because it's not just a compliance risk but a risk to their own livelihoods, and it's going to become very important for these organizations to prioritize putting resources into incorporating stronger and more robust security measures," Malek said.

The importance of medical research companies having strong security protections in place is further demonstrated by the nature of the cyber threat they're facing, which includes the type of information-gathering activities that nations have traditionally aimed at defense contractors and other businesses that are closely tied to national security, said Sumon Dantiki, a King & Spalding LLP partner and former federal cybercrime prosecutor.

The recent alerts show that "the target list has expanded, such that research of this type is as much of a target as some of the most sensitive military data," Dantiki said. He added that this shift is likely to require pharmaceutical and research companies to follow the security model set by defense contractors and build stronger protections into their operations "in a way that hasn't been on their radars in the past."

King & Spalding partner Seth H. Lundy pointed out that foreign nations have the means to reach every facet of the vaccine research and development chain, and that many involved in this space are primarily focused on improving public health and "are just not ready or aware of all the different types of vulnerabilities they face from the potential intrusion of foreign governments."

"These are novel issues for them that they're going to have to grapple with or face serious risks," Lundy said.

Jim Koenig, who co-chairs the privacy and cybersecurity practice at Fenwick & West LLP, noted that he's seen biotech companies "significantly stepping up efforts to further enhance and test their cybersecurity programs" in the wake of mounting threats like those highlighted in the recent vaccine alerts.

"What's at stake here is the ability to jump-start solutions for vaccines, testing and treatments for COVID-19, which means the country that develops this first will have both economic success and healthier people sooner. Positively, there's a lot at stake here globally," Koenig said.

Educating Employees

Because criminals often gain access to a corporate network through "social engineering" attacks that rely on tricking employees to reveal their credentials or other key personal information, making sure workers are up to date on the risks and how to identify them is a good and relatively inexpensive way to reduce exposure, attorneys say.

Comprehensively taking stock of the information that's on hand, strengthening agreements with vendors and ensuring that appropriate measures like strong passwords, penetration testing and patch management protocols are in place are also vital, particularly since attackers are looking to exploit vulnerabilities created by workers going remote, experts added.

"Most hacks don't occur through terribly sophisticated means, but instead happen because the company didn't employ basic security measures that would have prevented an attack, like multifactor authentication, proper vendor management and open [remote desktop protocol] ports," Bryan Cave's Valdetero said. "Companies should look at their security measures and ensure that they are taking at least baseline precautions."

Health care firms in particular should "double down on end-user education and awareness for social engineering campaigns and should check login attempts and access to vaccine research regularly," said Theresa Payton, former White House chief information officer and now CEO of cybersecurity consultancy Fortalice Solutions. She also said they could consider creating "honeypots," traps aimed at enticing attackers, to allow security teams to "learn much more about who is behind the attacks and what their skill levels and preferred tactics are" if bad actors take the bait.

"Health care, in a race for the cure, must collaborate across researchers, firms and more," Payton said. "It's in the complexity of communication that attackers will strike."

'Using Every Tool in Their Toolbox'

Those engaged in this research are likely to find the alerts put out by the Western governments to be helpful, given the level of detail they include about what these attackers are doing and what methods they're using to infiltrate systems, attorneys said.

"These kind of alerts have more actionable information that provides the attackers' fingerprints or signatures, which is something that helps potential victims, particularly larger companies, to better defend themselves because they can put this information into their own internal security protocols and scan their systems to look for these types of threats and signatures," said Guillermo Christensen, a partner in the data security and privacy group at Ice Miller LLP and a former CIA intelligence officer.

Providing these technical details and threat signatures also "provides the justification and attribution" for these warnings, which is "important so companies take this seriously," Christensen said. He added that the alert about Russia has even more weight behind it because it had the backing of three governments, which gives the warning "added credibility" and removes some of the "political heat" compared to past COVID-19 alerts involving China.

U.S. government agencies such as the FBI, the Department of Homeland Security and the National Security Agency have been ramping up their efforts to share cyberthreat information with businesses across a wide range of critical infrastructure and other sectors in recent years. Congress helped to expedite these efforts in 2015 when it passed the Cybersecurity Information Sharing Act to foster the voluntary exchange of cyberthreat information between the public and private sectors.

"There's been a concerted effort by the U.S. government to warn companies about the highly aggressive campaigns of foreign governments to get their hands on critical company intellectual property and other assets, and these governments are using every tool in their toolbox to do so," said Zack Harmon, a partner at King & Spalding and former FBI chief of staff.

Malek, the Moses & Singer partner, added that companies often view government officials as being "an enforcer as opposed to a partner" in the cybersecurity space, but that these recent alerts indicate that there's been a shift in terms of trust and aligned interests "that will allow for more partnership between the government and privacy industry in this context."

Taking Threats Seriously

The government has also shown support for business in recent years by bringing criminal charges against malicious users from countries such as Russia, China, Iran and North Korea. The U.S. Department of Justice built on that trend Tuesday, announcing that it had charged two Chinese nationals with a decade of cyberattacks targeting human rights activists and businesses around the world, including companies working on treatments for COVID-19.

While the defendants are unlikely to ever face these charges in U.S. court because they live in China, which does not extradite its citizens, the move to name and shame them signals that the U.S. government is taking these threats seriously.

"We need the international community to call out this behavior to not only warn potential victims and enable them to better protect their own networks, but also to assert the norms of acceptable cyber behavior," DLA Piper's McAndrew said. "What we're seeing here is these countries saying it's not acceptable to be stealing this research on such a critically important global health issue."

The alerts additionally illustrate the evolving nature of the cyberthreats that companies face from states such as China and Russia.

China has long been accused of targeting foreign companies to steal their intellectual property for commercial gain. In 2015, President Barack Obama and Chinese President Xi Jinping acknowledged this reputation when they announced an agreement to mutually refrain from knowingly engaging in or supporting intellectual property exploits that targeted private businesses and to work more closely to combat these threats.

"Unfortunately that détente was short-lived, and as we see from recent reports, these and other types of cyberattacks continue, and they will carry on unless and until the costs of such attacks become too high," said Paul Rosen, a Crowell & Moring LLP partner and former chief of staff at the Department of Homeland Security.

Russia, on the other hand, has been more focused in recent years on hacking to sow discord and cause disruption, including through its well-known efforts to interfere with the 2016 U.S. presidential elections.

With the reported attempts to steal COVID-19 research, these models are merging, with Russia signaling its interest in valuable IP data and the possibility looming that both countries could use the information they obtain to launch vaccine misinformation campaigns and sow chaos on a global scale.

"It makes sense for the hackers to take what they've been doing and apply it in the context of COVID-19 research, and for companies that means that the threat landscape is increasing significantly," Paul Hastings' Charfoos said. "Companies used to be able to encrypt credit card information and focus on that as the one thing they had to worry about, but now they have to protect all these different parts of the organization, which is much more difficult and expensive."

--Editing by Kelly Duncan and Brian Baresch.