THOMSON REUTERS
Westlaw®

Protecting your most valuable intellectual property from cyberattacks

By Rose Cordero Prey, Esq., and Sandra L. Applebaum, M.D., J.D., *Greenberg Traurig LLP*

MARCH 12, 2021

Innovation and ingenuity captured by companies in the form of intellectual property (IP) can be some of the greatest corporate assets and as such, require protection. Trade secrets, in particular, are sensitive intellectual property rights because they consist of proprietary information that maintains its value based on its confidentiality or secret status.

If stolen, the loss of any economic or competitive advantage provided by a company's confidential information and trade secrets could be devastating. Corporate IP theft threatens not only businesses, but it could also have effects on our global economy and national security.

As the workplace has evolved, there has been an increase in employee mobility, interconnectivity, digitization, and reliance on the cloud for data storage, networking, and computing services. These developments have accelerated dramatically in response to the coronavirus pandemic and the related shutdowns requiring the vast majority of the workforce to work remotely, often from home.

Additionally, these events have increased the risk of cyber intrusion activity and IP theft. Cyber criminals are perpetrating attacks on electronic repositories containing proprietary IP and trade secret information. One of the most significant cyberattacks in the United States was the recent breach of the SolarWinds Orion software, targeting both government agencies and private companies.

I. THE SOLARWINDS BREACH

SolarWinds Inc. is based in Austin, Texas. The company develops software for businesses to help manage their networks, systems, and information technology (IT) infrastructure. As of December 2020, the company reported having about 300,000 customers, including most Fortune 500 companies and many federal agencies.[1]

On December 13, 2020, the Washington Post disclosed that Orion, a SolarWinds software platform for centralized monitoring and managing all IT resources, was the focus of a global cyberattack allegedly perpetrated by Russian intelligence.[2] Because of the severity of the attack, the Cybersecurity and Infrastructure Security Agency (CISA) issued an Emergency Directive, advising all federal civilian agencies to disable Orion.[3]

The attack persisted undetected for months until December of 2020, and was initially only known to have affected the U.S. Treasury Department and the National Telecommunications and Information Administration, part of the U.S. Department of Commerce.[4] Additional details about the breadth and scope of the compromised systems continue to surface daily.

In an SEC filing, SolarWinds revealed that malware tainted its Orion updates that were released between March 2020 and June 2020.[5] It was reported that hackers inserted "malicious code [creating a backdoor] into legitimate software updates for the Orion software that allow an attacker remote access into the victim's environment."[6]

> Even solely viewing source code could provide hackers insight toward subverting widely used products or services.

FireEye, a cybersecurity company impacted by the breach, stated that the attacks used limited malware to accomplish the intrusion while avoiding detection, "going to significant lengths to observe and blend into normal network activity; and conducting reconnaissance, consistently covering their tracks, and using difficult-to-attribute tools."[7]

Some researchers believe that "at least 1,000 very skilled, very capable engineers" worked on the SolarWinds hack, and it is the largest and most sophisticated operation seen to date.[8] As is now known, the campaign was widespread, with victims including governments and consulting, technology, telecom and other entities in North America, Europe, Asia and the Middle East.[9]

During the U.S. Senate Intelligence Committee hearing on February 23, 2021, top executives from SolarWinds and other companies impacted by the breach, including FireEye, defended their conduct in breaches blamed on Russian hackers and sought to shift responsibility for the cyberattack.[10]

Representatives from the impacted companies told Senators that the true scope of the intrusions is still unknown because most victims are not legally required to disclose attacks unless

they involve sensitive information about individuals. They argued for greater information-sharing about breaches with corporate liability protections and a system that does not punish those who come forward, similar to airline disaster investigations.

Lawmakers spoke about how threats can more easily and confidentially be shared among competitors and the government to prevent large hacks like this in the future. "Congress has considered in the past whether to require companies to report that they have been the victim of a hack, but it has triggered legal concerns, including whether they could be held liable by clients for the loss of data."[11]

Providing additional resources and authority to the CISA or other government agencies is also being considered as a way to help prevent future breaches.

II. IP TARGETED IN THE SOLARWINDS CYBERATTACK

The SolarWinds supply chain attack affected more than 200 government agencies and businesses, and it has been difficult to determine the IP and specific corporate trade secrets acquired by the hackers as a result of the attack. Thus far, only a few specific incidences of IP theft have been reported, but they seem significant.

On December 8, 2020, FireEye reported that there had been a cyberattack on their systems, and they were able to determine that the inventory of their Red Team tools was stolen.[12]

FireEye has noted that the objective of its Red Team "is to improve enterprise cyber security by demonstrating the impacts of successful attacks and by showing the defenders how to counter them in an operational environment. ... [Over time, the Red Team] built up a set of scripts, tools, scanners, and techniques to help improve our clients' security postures.

Unfortunately, these tools were stolen by a highly sophisticated attacker. The stolen tools range from simple scripts used for automating reconnaissance to entire frameworks."[13] FireEye noted that these tools could potentially be used by a hacker against unsuspecting victims. In addition, FireEye said it lost valuable resources that likely gave the company a competitive advantage in cyber-security.

Source code, the underlying set of instructions that run a piece of software or operating system, is typically among a technology company's most closely guarded secrets. At least one large American technology company reported that hackers accessed parts of its source code repositories looking to discovery the inner workings of its products.[14]

While an intrusion can be limited to solely viewing source code repositories and not altering them, even solely viewing source code could provide hackers insight toward subverting widely used products or services.[15]

In addition to the private sector, the SolarWinds Orion cyberattack appears to have compromised the Administrative Office of the United States Courts (AO) network infrastructure, the agency that developed and maintains the case management and electronic court filing system (CM/ECF).[16]

In most patent and trade secret cases, the parties seek a protective order from the court to govern the production and disclosure of trade secrets and other confidential documents. Documents that contain truly sensitive or confidential information are typically filed and maintained under seal because the public disclosure of this information can affect the parties that provided the information.

On January 6, 2021, the AO stated that it was "working with the Department of Homeland Security on a security audit relating to vulnerabilities in the Judiciary's [CM/ECF] that greatly risk compromising highly sensitive non-public documents stored on CM/ECF, particularly sealed filings ... Due to the nature of the attacks, the review of this matter and its impact is ongoing."[17]

While the AO has declined to comment on specific questions about their breach disclosure, federal courts have imposed new procedures for the submission of court filings containing confidential information under seal.

For example, under General Order 21-02 in the Eastern District of Texas, highly sensitive confidential information is no longer to be electronically submitted via the Court's electronic filing system. Instead, electronic filing of such documents is prohibited, and the new procedure requires they be filed in person or delivered to the court by courier.

The SolarWinds situation highlights the importance of taking measures to prevent cyberattacks and protect digital trade secrets.

III. CAN YOU PREVENT THEFT OF IP IN RESPONSE TO CYBERATTACK?

Cyber criminals want to steal digital IP, trade secrets, and know-how because they may be some of a company's most valuable assets. The shift to remote working and increased corporate use and reliance on portable devices if not done properly can create vulnerabilities, which can be exploited by threat actors. Can you really prevent the theft of corporate secrets and proprietary IP by cyberattack?

- **Inventory your IP.** If IP is the driver of your company's growth and competitiveness, then you need to know exactly what IP your company has and where it is stored. Take stock of your company's IP and classify according to confidentiality and risk. In this way, trade secret and sensitive IP that requires enhanced protection can easily and readily be identified. Knowing what IP your company has, where it is found, and how it is being safeguarded, can help you take the next steps to protect it.

- **Information Security Policies should include provisions to protect your IP.** Your overall IP management strategy should include an information security policy that puts in place security measures that safeguard your most sensitive and secret IP. By understanding the priority of IP for your company, investments can be made in protections that align with those priorities. Controlling and limiting access to your proprietary IP and trade secrets are reasonable measures that can protect your critical assets. These measures can include implementing physical security, digital security and legal measures to protect the secrecy of your IP. These should apply to IP in existence, as well as, new IP and trade secrets in development.

Physical security measures may include segmenting or isolating the portions of your network where your trade secrets are kept by restricting unnecessary connections between your network and outside sources including the internet, storing trade secrets on computers that are not connected to the company network, or restricting access to the location of those computers.

Only preauthorized individuals or those with a need to know should have access to your trade secrets and other sensitive company IP. Secure physical locations where computers house trade secrets, including by using security cameras and keycards to prevent or monitor access.

In the simplest form, digital security measures include utilizing file encryption, strong passwords, and multi-factor authentication for access. Additional digital security measures such as the use of firewalls, access control lists, and other enhanced network configurations can further help to prevent access to your trade secrets.

Cyber monitoring your network traffic for anomalies in bandwidth consumption or suspicious connections can also be used to prevent intrusion and theft. While your company may have these security measures in place, its information security program may be centered around the protection of personal information, and not specifically be considering the security controls necessary to protect the company's IP and trade secrets.

In addition, your company can implement legal measures that include requiring employees to sign confidentiality and non-disclosure agreements and non-compete agreements for employment. It is also important to implement and train employees on company policies and procedures for safeguarding the company's trade secrets from their creation to storage and subsequent handling.

In addition, for any third-party vendors who require access to your network and trade secrets, confirm they are aligned (and contractually bound) with company policies for safeguarding sensitive information and secrets.

- **Verify that your IP is protected.** Implementing cybersecurity measures and educating employees about the company policy for the treatment and protection of trade secret information can be effective in protecting IP. However, monitoring and policing are required. Conducting periodic assessments of network vulnerabilities and tabletop exercises are important to ensure that the cybersecurity protections are not compromised, your team is prepared to handle a cyber incident, and any weaknesses in your security program or incident response plan are addressed to prevent a cyber-theft. Likewise, auditing compliance with employee training around company cybersecurity policies can identify areas where additional training or refresher courses may be necessary.

- **Be vigilant.** To maintain the secrecy of your most sensitive IP and its value, constant vigilance is required. Regularly monitor network behavior for anomalous activity and promptly investigate anything that is not considered "normal." Defensive measures can then be taken as swiftly as necessary.

With each of the measures described above, the goal is to protect your corporate secrets and proprietary IP from a cyberattack to keep your company's potential economic and competitive advantage afforded by such IP intact.

IV. HOW YOU CAN MITIGATE THE RISK OF A CYBERATTACK THAT STEALS YOUR IP?

If your company and its IP are the subject of a cyberattack, the losses can be significant. In addition to the lost value of the stolen IP itself, there can be disruptions to your company operations, loss of the IP/competitive advantage resulting in potential lost contracts, devaluation of your company's reputation, and other long-term costs, including possible higher insurance premiums.

When it is discovered that a threat actor has stolen your IP, there are three phases to effective risk mitigation: Triage, Reaction, and Recovery.

- **Triage.** Once a security incident has occurred resulting in the loss of trade secrets or other sensitive IP, there will be a flurry of activity to quickly analyze what happened, how it happened, what defensive measures need to be taken, and what will be the legal and public ramifications. To ensure these assessments are made carefully and without compromising any forensic evidence, you will likely need to have attorneys and forensic experts to investigate the incident. It may also be necessary to hire a cybersecurity firm to help remediate the breach, and public relations counsel to control the messaging around the incident with stakeholders and to preserve the company's reputation and image. Once your IP loss is confirmed and preliminary assessments underway, you can begin to manage the impact of the incident.

- **Reaction.** Managing the impact of an IP theft requires taking action to minimize the direct consequences of the incident. To reduce your risk exposure, your company will want to take steps to mitigate the disruption to your day-to-day business and prioritize the defensive activities that will remediate your damages. To recover, you will need to repair and restore your network infrastructure and cybersecurity, as well as affected business operations, corporate identity, and business relationships.
- **Recovery.** After the initial reaction to the incident is complete, there may be legal challenges to resolve, investigations to complete, and infrastructure to improve to prevent subsequent cyberattacks. Business strategies going forward will have to address the impact of the incident and the damages suffered to create initiatives that will aim to prevent further risks to the company and its most sensitive IP.

Cyber intrusions may cause more damage to our national security and global economic prosperity than any other attack on the United States. The targets of the SolarWinds Orion attack and the compromised IP and corporate trade secrets acquired by the hackers will continue to be uncovered. Due to the high value of IP and trade secrets, cyber criminals will also continue perpetrating attacks on electronic repositories containing valuable proprietary IP and trade secret information.

Even if your company was not impacted by the SolarWinds attack it can use this as a warning, and take measures to prevent the theft of your most sensitive and secret corporate assets by developing a strategy that includes an information security policy that takes into consideration and puts in place security controls to ensure your IP is protected.

Inventorying your proprietary IP and taking steps to limit access are reasonable measures to protect your critical assets and are good first steps, but once security measures are in place, companies should continue to be vigilant and verify that IP is protected. While it may be impossible to eradicate all vulnerabilities, proactive protective measures and rapid response plans can save a company from financial harm and more.

Notes

[1] https://bit.ly/3qHY6Vh

[2] https://wapo.st/3eH7iXF

[3] https://bit.ly/3l7nAtP

[4] https://reut.rs/3rJAtwz; https://bloom.bg/30QOJbn

[5] https://bit.ly/3t4wYkA

[6] https://bit.ly/3vadi0R

[7] https://bit.ly/38tRx2j

[8] https://bit.ly/3tb1GsE

[9] https://zd.net/3l5144V

[10] https://reut.rs/3rJI3Yo

[11] https://bit.ly/3bGSBBH

[12] https://bit.ly/30zZZZu

[13] https://bit.ly/3t8xFJH

[14] https://bit.ly/3rFeeb9

[15] https://cnb.cx/3eulyS0

[16] https://bit.ly/3rEJEyz

[17] https://bit.ly/3l6S3bn

This article was published on Westlaw Today on March 12, 2021.

ABOUT THE AUTHORS

Rose Cordero Prey, Esq. (L), is a shareholder in the Intellectual Property Group at **Greenberg Traurig LLP**'s New York office. She counsels clients on invention protection, portfolio management, patent litigation, licensing and due diligence in the mechanical, electrical, computer science and life science industries. With more than 15 years of experience in high-tech intellectual property litigation, she has represented both plaintiffs and defendants in patent infringement and related litigation involving a wide array of technologies. She can be reached at preyr@gtlaw.com. **Sandra L. Applebaum, M.D., J.D.** (R), is a member of the Intellectual Property Litigation Practice at the firm's New York office. With more than 17 years practicing allergy medicine as a licensed physician, she began a career in law focusing on complex patent litigation. Her patent litigation experience includes medical devices, ANDA/Hatch-Waxman matters, consumer products, electronics and a variety of software-based technologies. She can be reached at applebaums@gtlaw.com.