The Computer & Internet Lawyer

Volume 38 ▲ Number 10 ▲ November/December 2021

Ronald L. Johnston, Arnold & Porter, Editor-in-Chief

New York Department of Financial Services Questions Its Regulated Entities on Responses to and Lessons Learned from the SolarWinds Cyberattack

By Ronald D. Lee, Michael A. Mancusi, Amber A. Hay, and Anthony Raglani

In December 2020, a cybersecurity company alerted the world to a major cyberattack against the U.S. software development company, SolarWinds, through the company's Orion software product ("SolarWinds Attack"). The SolarWinds Attack went undetected for months, as it has been reported that the hackers accessed the source code for Orion as early as March 2020.[1] Orion is widely used by companies to manage information technology resources, and according to SolarWinds Form 8-K filed with the Securities and Exchange Commission, SolarWinds had 33,000 customers that were using Orion as of December 14, 2020.

It is alleged that the SolarWinds Attack was one part of a widespread, sophisticated cyber espionage campaign by Russian Foreign Intelligence Service actors which focused on stealing sensitive information held by U.S. government agencies and companies that use Orion.[2] The hack was perpetuated through SolarWinds sending its customers routine system software updates.[3] SolarWinds unknowingly sent out software updates to its customers that included the hacked code that allowed the hackers to have access to customer's information technology and install malware that helped them to spy on SolarWinds' customers, including private companies and government entities, thereby exposing up to 18,000 of its customers to the cyberattack.

The New York Department of Financial Services ("DFS") alerted DFS-regulated entities of the

Ronald D. Lee, a partner in Arnold & Porter and a former general counsel of the U.S. National Security Agency and Associate Deputy Attorney General of the U.S. Department of Justice, represents clients in national security, cybersecurity and privacy, and government contracts matters. Michael A. Mancusi, a partner in the firm, represents domestic and foreign banks, credit unions, and other financial services clients in state and federal regulatory, compliance, and enforcement matters. Amber A. Hay, a senior associate at the firm, represents banks and nonbank financial services companies in bank regulatory matters. Anthony Raglani, a senior associate at the firm, counsels clients on financial regulatory matters. Resident in the firm's office in Washington, D.C., the authors may be contacted at *ronald.lee@arnoldporter.com*, *michael.mancusi@arnoldporter.com*, *amber.hay@arnoldporter.com*, and *anthony.raglani@arnoldporter.com*, respectively.

SolarWinds Attack on December 18, 2020 through the "Supply Chain Compromise Alert."[4] The Supply Chain Compromise Alert included guidance from the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, SolarWinds, and other sources, and reminded the regulated entities of their obligations under the New York Cybersecurity Regulation ("Cybersecurity Regulation"), adopted in 2017, which requires DFS-regulated entities, including New York banks, insurance companies and producers and other financial services firms, to develop a comprehensive cybersecurity program, implement specific cybersecurity controls, assess cybersecurity risks posed by third-party service providers, and notify the DFS of "cybersecurity events" (which includes certain unsuccessful cyberattacks) that carry a "reasonable likelihood" of causing material harm to the operations of the institution or otherwise require notice to any governmental or supervisory entity.[5]

The DFS followed up its Supply Chain Compromise Alert with its "Report on the SolarWinds Cyber Espionage Attack and Institutions' Response" ("SolarWinds Report"), released in April 2021.[6] In the SolarWinds Report, the DFS analyzes the remediation of approximately 100 of its regulated entities to the SolarWinds Attack, and the DFS's recommendations for ways that organizations can strengthen their cybersecurity practices to protect against future cyberattacks.

In general, the DFS found that its regulated entities responded "swiftly and appropriately" with 94 percent of impacted companies removing the vulnerable systems caused by the SolarWinds hackers from their networks (and or patching them) within three days of being notified of the attack. However, the DFS noted gaps in cybersecurity policies of several regulated entities, including irregularities in patching and patch management systems, identifying third-party service providers as critical vendors, and the need for more information sharing and transparency among the regulated entities with respect to cybersecurity breaches.

Interestingly, the DFS's observations as detailed in the SolarWinds Report, and specifically those related to the need for enhanced cybersecurity preparedness by companies and their third-party service providers and the need for more transparency and information sharing among companies regarding actual or perceived cyberthreats, align with the principles outlined in President Biden's "Executive Order on Improving the Nation's Cybersecurity,"[7] released on May 12, 2021, applicable to the federal government and government contractors. This could signal a new wave of state cybersecurity laws and regulations if not a federal regulation in the foreseeable future.

This article provides a brief overview of the DFS's findings detailed in the SolarWinds Report, and the outlook for the DFS's enforcement of the Cybersecurity Regulation, as well as potential changes to those rules, based on the DFS's findings and observations.

DFS-Regulated Entities' Response to the SolarWinds Attack and Weaknesses Identified in Patch Management Systems

As detailed in the SolarWinds Report, the DFS found that its supervised companies generally responded to the SolarWinds Attack swiftly and appropriately, by clearing their systems of the infected software within three days of notification by disconnecting, patching, or applying a mitigation script. The remediation steps that were taken by more than half of the regulated companies to mitigate risks associated with the SolarWinds Attack included, but were not limited to:

- Evaluated system integrity and audit logs for indicators of compromise;
- Disconnected affected systems from their networks; and
- Applied security patches to affected systems.

About a quarter or less of the DFS-regulated entities took the following remediation steps:

- Isolated affected systems by blocking access to the internet;
- Isolated affected systems by blocking specific external DNS domains, based on guidance by Cybersecurity and Infrastructure Security Agency;
- Decommissioned Orion and replaced it with another monitoring product; and
- Applied mitigation scripts to affected systems, as recommended by SolarWinds.

While these remediation steps allowed the DFS-regulated entities to address the risks associated with the SolarWinds Attack once identified, the DFS found that several companies could have addressed the risks posed by the SolarWinds Attack (if not preventing it altogether) by implementing a mature patch management system.

According to the DFS, several DFS-regulated companies' patch management programs were immature at the time of the cyberattack, and the lack of proper "patching cadence"[8] likely resulted in a delay in the

ability of the companies to ensure timely remediation of high-risk cyber vulnerabilities.

For example, it is reported that the cyberhackers inserted the malware referred to as "Sunburst" into SolarWinds's software Orion in February 2020, and SolarWinds unknowingly distributed updates of the Orion software with the Sunburst malware to its customers between March and June 2020.[9] The DFS found that some of the companies found to be vulnerable to Sunburst malware in December 2020 had not applied patches released by SolarWinds in August and October 2020 that would have eliminated Sunburst, and some companies had not patched since 2018, with two companies having not patched since 2017.

Fortunately, there have been no reports that the hackers exploited the vulnerabilities caused by the Sunburst (or Supernova) malware;[10] however, supervised entities need to ensure proper patching cadence to prevent against material harm from vulnerabilities that may result from future cyberattacks.

DFS's Recommendations for Regulated Entities Going Forward

The DFS includes in its reports key observations and recommendations for DFS-regulated entities to prevent against supply chain attacks and reduce supply chain risks, based on industry standards on cybersecurity measures. The key recommendations noted by the DFS include that supervised entities should:

- Ensure that third party service provider and other vendor risk management policies and procedures should include processes for due diligence and contractual protections that will ensure the company can monitor the cybersecurity practices and overall cyber hygiene of critical vendors. These policies should include provisions requiring third-party service providers to immediately notify the regulated company when a cyber event occurs that impacts or could potentially impact an organization's information systems or non-personal information that is maintained, processed or accessed by the vendor.

- Adopt a "Zero Trust" approach and assume that any software installation and any third-party service provider could be compromised and used as an attack vector. In this regard, third party service providers' access to a company's network systems or nonpublic information ("NPI") should be limited to only what is needed and systems should be monitored for anomalous or malicious activity. Regulated entities are also expected to implement multiple layers of security for extra protection for sensitive information to limit compromises.

- Have a vulnerability management program that prioritizes patch testing, validation processes, and deployment, including which systems to patch and the order or priority of patching. In addition, a regulated entity's patch management strategy should include performing tests of all patches to the internal system environment with defined rollback procedures if the patch creates or exposes additional vulnerabilities.

- Have an effective and tested incident response plan with detailed procedures and playbooks. The DFS also notes that cybersecurity fundamentals such as knowing your environment and understanding where assets reside in the environment, including their versions and configuration, should be incorporated into playbooks. To address supply chain compromises or attacks, the incident response plans should include, at a minimum:

    - Procedures to isolate affected systems;

    - Procedures to reset account credentials for users of all affected assets and users of assets controlled by compromised software;

    - Procedures to rebuild from backups created before the compromise;

    - Procedures to archive audit and system logs for forensic purposes; and

    - Procedures to update response plans based on lessons learned.

The DFS recommends that regulated entities engage in "table top" exercises to test and refine incident response plans, and notes that incident response plans should be aligned with an organization's business continuity plan.

The DFS also notes in the SolarWinds Report that there is a need for more transparency and effective information sharing amongst the DFS-regulated entities regarding cybersecurity breaches, which would have allowed organizations that detected the intrusion earlier than December 13, 2020 to alert the others. DFS found that some of its regulated entities publicly revealed that they blocked an intrusion prior to the intrusion becoming widely known by others. Based on this finding, the DFS has indicated that it plans to improve information

sharing and transparency, which suggests that future changes to the Cybersecurity Regulation may encourage DFS-regulated entities to share information on cyberattacks. Financial institutions are currently able to share information one with another and report to the federal government activities that may involve money laundering or terrorist activity (including those that involve or tied to cyberattacks) under Section 314(b) of the USA PATRIOT Act ("Section 314(b)"). DFS could adopt a voluntary information sharing approach similar to that under Section 314(b) of the USA PATRIOT Act for cybersecurity breaches that are not covered by Section 314(b).

Outlook for Future Changes to the Cybersecurity Regulation and Enforcement

The DFS has been the most active state government functional regulator focused on cybersecurity regulation, and the issuance of the SolarWinds Report is one of the many examples of the DFS continuing its efforts.

After adopting the Cybersecurity Regulation in 2017, and releasing several alerts informing its regulated companies of cyber threats and providing reminders of obligations under the Cybersecurity Regulation, in July 2020, the DFS commenced its first enforcement action under the Cybersecurity Regulation against the second largest title insurance provider in the United States. Last February, the DFS released the United States' first "Cyber Insurance Risk Framework"[11] and alerted DFS-regulated entities of the growing cyber campaign to steal NPI.

With respect to management of supply chain risks, DFS-regulated companies should expect future changes to the Cybersecurity Regulation and related guidance that stresses the importance of:

- Effective third-party risk management and identifying critical vendors that have access to sensitive information and NPI;
- Enhanced information sharing amongst regulated entities regarding cybersecurity breaches;
- Adequate patch management systems, with validation processes, deployment, and priorities, as well as mandated patching and testing of patch management systems on a routine basis; and
- Mandated testing of incident response plans that include cybersecurity fundamentals and "table top" exercises.

Additional Considerations for DFS-Regulated Banks

The DFS may look to federal regulations and guidance for developing additional requirements related to incident response plans. DFS-regulated banks and other insured depository institutions are also subject to the regulation and supervision of the federal banking agencies, and in December 2020 the federal banking agencies proposed a computer-security incident notification rule that would require banking organizations to notify their primary regulators upon the occurrence of certain computer-security incidents as soon as possible and no later than 36 hours after the banking organization believes in good faith that the incident occurred.[12]

Under the proposed rule, bank service providers also would be required to notify the banking organizations for which they provide services of computer-security incidents that the service provider believes in good faith could disrupt, degrade or impair services provided for four or more hours. The heightened focus of supervisory agencies on real-time information sharing of cybersecurity incidents that may be disruptive and harmful to supervised institutions and the industry likely will require certain institutions to enhance their monitoring, testing, and reporting controls and processes over time.

In addition, although it appears that the proposed rule would have a collaborative purpose and is not intended to be used as a means of identifying and scrutinizing supervised institutions perceived to have insufficient cybersecurity risk management controls, institutions must nonetheless be prepared to manage any supervisory or examination scrutiny that may arise from the satisfaction of their current and future obligations to share information with their regulators and other institutions regarding known or suspected cybersecurity incidents (if, for example, a cybersecurity incident exposes a vulnerability or insufficient control that results in greater supervisory or examination scrutiny and/or enforcement action).

Conclusion

All in all, the SolarWinds Attack provided the DFS with a real-time opportunity to assess the cybersecurity preparedness of its regulated entities, and identify areas of improvement for its regulated entities in managing risks from third-party service providers as well as areas of improvement for cybersecurity regulation. The SolarWinds Report provides some insight into the DFS's expectations of DFS-regulated entities, as well as plans for the future of the Cybersecurity Regulation and related guidance.

Notes

1. *See gen*. "The US is readying sanctions against Russia over the SolarWinds cyberattack," *available at https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12,* and SEC Form 8-K, Solarwinds Corporation, *available at https://www.sec.gov/ix?doc=/Archives/edgar/data/1739942/000162828020017451/swi-20201214.htm*.
2. Business Insider, December 20, 2020, "Former US cybersecurity chief Chris Krebs says officials are still tracking 'scope' of the SolarWinds hack."
3. SolarWinds unknowingly sent out software updates to its customers that included the hacked code that allowed the hackers to have access to customer's information technology and install malware that helped them to spy on SolarWinds' customers, including private companies and government entities, and thereby exposing up to 18,000 of its customers to the cyberattack. *See*, Press Release - April 27, 2021: DFS Issues Report On the SolarWinds Supply Chain Attack | Department of Financial Services, *available at https://dfs.ny.gov/reports_and_publications/press_releases/pr202104271.*
4. *See* the Supply Chain Compromise Alert, *available at https://www.dfs.ny.gov/industry_guidance/industry_letters/il20201218_supply_chain_compromise_alert*. The DFS advised its regulated entities to respond immediately to assess the risk to their systems and consumers, and take steps necessary to address vulnerabilities and customer impact. The alert included several resources for completing such tasks.
5. In 2017, the DFS adopted the Cybersecurity Regulation, 23 NYCRR Part 500, which requires all DFS-regulated financial services entities to implement a risk-based cybersecurity program and to report any unauthorized access (or attempts) to their information systems. The DFS was the first in the United States to adopt such a regulation, and in 2019 the DFS became the first financial regulator in the nation to establish a division dedicated to cybersecurity.
6. *See* SolarWinds Report. It is estimated by the DFS that approximately nine federal agencies and approximately 100 companies were compromised.
7. *https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/*.
8. The DFS defined "patching cadence" in the SolarWinds Report to refer to how often an organization reviews systems, networks, and applications for updates that remediate security vulnerabilities
9. *See* SolarWinds Report.
10. *Id*. Following the removal of the Sunburst malware, on December 24, 2020, SolarWinds became aware of another vulnerability, referred to as "Supernova" that was found in the same versions of Orion that had the Sunburst malware as well as other versions of Orion that had been distributed to customers. SolarWinds released additional patches that addressed Supernova, and informed its customers that the patches released on December 14 and 15 also eliminated the vulnerability in the versions of Orion that held the Sunburst malware. SolarWinds released additional patches to address both Sunburst and Supernova on January 25, 2021. The Sunburst and Supernova vulnerabilities in the Orion software allowed the hackers to gain access to the exposed institutions' internal network and nonpublic information, however, as of the date of the SolarWinds Report, no reports or indications that hackers exploited the vulnerabilities resulting from the Sunburst or Supernova in any financial services organization.
11. *https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02*.
12. *See* "Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers," 86 Fed. Reg. 2,299 (Jan. 12, 2021).