Proskauer

SolarWinds Vendor Supply Chain Attack: A Timely Reason to Review Procedures for Risk Assessments and Vendor Contracts

Proskauer on Privacy Blog on **December 21, 2020**

As reported last week, a state-sponsored hacker may have breached multiple U.S. government networks through a widely-used software product offered by SolarWinds. The compromised product, known as Orion, helps organizations manage their networks, servers, and networked devices. The hacker concealed malware inside a software update that, when installed, allowed the hacker to perform reconnaissance, elevate user privileges, move laterally into other environments and compromise the organization's data.

Orion is not only used by government agencies, but is widely used in both the public and private sectors. According to another blog, victims of the attack include "government, consulting, technology, telecom and extractive entities in North America, Europe, Asia and the Middle East." SolarWinds's recent SEC filings estimate that about 18,000 of its customers may have downloaded the malware-laden software updates for Orion. To learn more information about this attack and evolving cybersecurity threats, please visit the NSA's Cybersecurity Advisories & Technical Guidance. For a list of steps an organization might take to assess the impact of this issue on its specific situation, see this blog post.

Whether or not you are one of the impacted customers, the SolarWinds attack is a reminder of the importance of conducting incident response and risk assessments under privilege whenever possible, the importance of performing due diligence before engaging vendors, and why businesses should implement procedures to minimize information disclosed to or accessed by vendors. The attack is also highlights the care that needs to be taken by both customers and vendors when negotiating data security provisions in technology contracts.

Conducting Privileged Dual-Purpose Risk Assessments

The aftermath of the SolarWinds cybersecurity attack has left organizations scrambling to determine whether their systems have been breached and the scope of any such breach. Unfortunately, the documents created by an organization as it evaluates its security posture are exactly the types of documents that a plaintiff's counsel or regulator would like to get their hands on if there is an investigation or litigation.

To mitigate this concern, risk assessments can be structured in a way to serve both a business purpose (assessing the state of security) as well as a legal purpose (assisting counsel evaluate risks related to the state of security), allowing certain protections to limit discoverability, including privilege, work product, and protections under FRCP 26(b)(4)(D). Assessments that serve both legal and business purposes are known as "dual-purpose" risk assessments.

Under developing case law, there are a number of ways to conduct a dual-purpose risk assessment. While courts will consider the totality of the evidence when deciding whether materials generated during the course of a risk assessment are privileged or discoverable, recent cases have emphasized the following factors.

- Involvement of Counsel: Counsel should be actively – not passively – involved in every step of the assessment, from the initial scoping of the assessment (discussed below), to fact-finding, retaining experts, and drafting any reports. In other words, as recent cases make clear, it is not enough to simply state that the assessment was performed at counsel's direction. Given that courts look at the totality of the circumstances when deciding whether or not to maintain privilege over risk assessment materials, the greater the evidence that counsel was actively involved, the easier it will be to distinguish the assessment and investigation from other ordinary-course-of-business assessments or investigations that would not necessarily involve counsel.
- Scope of the Assessment: The scope of the assessment, and the process by which the scope is defined, should indicate that the assessment is driven by a legal purpose. This means that the scope should be different from those of assessments conducted in the ordinary course of business, and should clearly and expressly convey that the assessment is conducted for a legal purpose. Toward this end, counsel should have at least some direct involvement in defining the scope, and, as discussed above, the greater the involvement, the more evidence to support privilege protection. While the scope will clearly convey a legal purpose, any stated business purpose for the assessment should be, as one court explained, "profoundly interconnected" with the legal purpose.

- Distribution of Materials: While materials generated during the course of dual-purpose risk assessments can be used for certain business purposes without destroying privilege protections, some courts have found that the extent to which these materials are distributed is probative the purposes for which the work product was initially produced. Wide distribution of these materials may suggest they were created further to a business, as opposed to a legal, purpose. As discussed above with respect to scoping the assessment, permissible business uses generally relate to areas where the business and legal purposes interconnect.

In the more extreme cases an organization may want to consider a "Dual Track" approach where separate privileged and non-privileged investigations proceed in parallel. As the SolarWinds cybersecurity attack is likely to trigger organizations to investigate their networks for vulnerabilities and data theft, it is important to consider the downstream consequences should the assessment uncover related (or unrelated) vulnerabilities and/or intrusions. Conducting a risk assessment under privilege may help companies limit the discoverability of what they learn.

Mitigating Risk Using Diligence, Contractual Obligations and Data Minimization

The SolarWinds cybersecurity attack serves as a cautionary tale for all companies and vendors entering into outsourcing software agreements in their business. No one can predict when a malicious cyberattack will occur, especially one with the scale and sophistication of a nation-state attack like this one, but companies and vendors can take steps now to mitigate their risks.

- Diligence: Companies and vendors should conduct thorough diligence (either directly or through a third-party consultant) prior to finalizing material software or IT vendor agreement. Outsourced software solutions provide cost-savings and increased efficiencies, but moving operations off of company systems or introducing third-party software on to company's networks can introduce a fracture point which cyber criminals may target. Companies and vendors should be aware of each other's data security practices, history of cybersecurity incidents, and any security audits conducted. As the SolarWinds cybersecurity attack demonstrates, even sophisticated software companies may face cybersecurity attacks, so after conducting cybersecurity due diligence, companies and vendors must be prepared to respond and cooperate if and when a cybersecurity attack occurs. Additionally, companies and vendors should review and agree on cybersecurity insurance policies as part of the due diligence process.

- Contractual Obligations: With cybersecurity attacks, one of the first things companies and vendors do is review their agreements and determine what steps the parties are required to take and who is responsible for the costs. As such, when negotiating software agreements, companies and vendors should pay careful attention to data breach notification provisions which may require notification of suspected security incidents sooner than as required by law. Such provisions may also require the parties to engage nationally-renowned forensics firms and to promptly respond to the security incidents or breach. Contractually stipulating each parties' notification obligations in the event of a breach may help clarify the parties' responsibilities and timing with respect to notifications to government regulators and the clients of the company.
- Data Minimization: Lastly, the SolarWinds cybersecurity attack demonstrates that even with detailed diligence, vendors may be targeted by a breach. Contractual obligations may limit the costs associated with a breach and downstream legal obligations, but they cannot retrieve company or customer data once it has already fallen into the hands of cyber criminals. The only way to limit the amount of data exposed through cybersecurity attacks is to limit the amount and type of data shared between companies and vendors. This may not always be possible, but the companies and vendors can work together to implement and maintain data minimization procedures which require employees and any other individuals accessing the software solution minimize the amount and type of information provided or generated on such solution.

The SolarWinds cybersecurity attack serves as yet another reminder that organizations must implement technical, physical and administrative safeguards to reduce the risk of suffering a breach, either directly or by a vendor, and to plan ahead in the event that a breach does occur. By assessing organizational risk and taking proactive steps when drafting software agreements, companies and vendors can be better prepared should they become the next target.

Special thanks to associates Stephanie A. Diehl and Kevin P. Milewski for their contributions to this blog post.

View Original

Related Professionals

- **Nolan M. Goldberg**
  Partner

- **Margaret A. Dale**
  Partner
- **Jeffrey D. Neuburger**
  Partner