We get it. bit-x-bit

The Frick Building
437 Grant Street, Suite 1250
Pittsburgh, Pennsylvania 15219
Tel: 412-325-4033
www.bit-x-bit.com

Lessons Learned from the SolarWinds Hack: What Went Wrong & How Can Lawyers Help Mitigate the Risk of Cyberattacks

Authors: Carina Mendola, University of Pittsburgh School of Law (JD expected 2022), BA, MBA, MSIT;
Brett Creasy, President and Director of Digital Forensics, bit-x-bit, LLC, CISSP, GCFA, CCE

The recent SolarWinds hack has been described as "a turning point in the digital world." [1] Security professionals knew about the cracks in the digital supply chain, but this attack revealed those cracks to the global community. As with all successful attacks, there are lessons that lawyers as well as IT professionals can take away from this event.

The Attack

SolarWinds is a software company that produces a variety of system management tools. Orion, a Network Management System (NMS), is SolarWinds' most popular product. In December 2020, we learned that SolarWinds Orion supply-chain and nearly 18,000 customers were susceptible to a series of malware, later identified as Sunburst, Teardrop, and Sunspot. [2]

The SolarWinds hack is considered a supply chain attack, a type of cyber-attack that uses third-party vendor software to infiltrate subsequent users of the software. Bad actors exploit vulnerabilities in the software, often during development, to inject malware that will propagate when triggered by some event, like installing the software. Supply chain attacks are not new. Some of the most well-known cyber-attacks are supply chain attacks, including Target, OPM, NotPetya, and Stuxnet.

The Target breach, which occurred in 2013, resulted from a compromised third-party HVAC firm, which likely allowed the attackers access through a Target vendor portal. [3] Once they infiltrated Target's system, the attackers set their sights on Target's point-of-sale (POS) system. Over 40 million credit and debit card records and 70 million personal information records were stolen. It is estimated that Target spent over $300 million to secure its systems and in breach-related legal settlements. [4].

After that breach, case studies were performed, and "lessons learned" were published, yet supply chains were often left vulnerable. Cost and time often kept c-suites from implementing the "lessons learned" from Target, much to the chagrin of CISOs and certainly the legal departments supporting those functions. Much of the rhetoric about the cause of the Target attack blamed Target's lack of compliance with the Payment Security Card Data Security Standard (PCI DSS), which is an information security standard mandated by the credit card brands. Thus, recommended remedial courses of action focused largely on securing payment systems. Such recommendations included increased encryption, use of chip and pin credit cards, application whitelisting, network segmentation, increased security awareness training, and many other security controls. [3][5]

As the finger was pointed toward PCI compliance failure, applying security controls to the rest of the supply chain was less of a priority. PCI compliance became the focus when, in reality, the vulnerabilities underlying the Target breach would prove to be far more detrimental when applied more broadly than only to POS systems.

Enter the SolarWinds attack. What makes the SolarWinds hack so remarkable is that SolarWinds itself was the vector of compromise for its customers. Unlike the Target breach, where the malware came from a supplier into the organization, SolarWinds itself is the propagating supplier. Rather than sending the malware to one target organization, it was sent to over 18,000.

A network management system ("NMS"), like Orion, is highly integrated into the system on which it operates, meaning that it can communicate with many devices to monitor and respond to security events. Because a NMS has administrative privileges, meaning it can automatically make changes to a system, a NMS can be a prime target for hackers. [6] "If present and activated [the malware] could allow an attacker to compromise the server on which the SolarWinds Orion product is run." [7] Due to the attack's sophistication, using cyber tools never before seen, it is widely believed that a nation-state conducted the attack, likely Russia. [7][8]

Practical Tips: How Attorneys Can Help Improve Security

Prior supply chain attacks should have prepared us for this. So, what can be done now, and can lawyers actually help?

Robust, secure coding practices may have allowed for the malware to be detected more quickly by SolarWinds. Code reviews on the critical parts of the system may have revealed the presence of the malware. For SolarWinds customers, it is now crucial to implement any patches released by SolarWinds to help rid the software of the malware. However, patching only prevents future damage. It does not retroactively fix malware that has already permeated the system. In many cases, a SolarWinds Orion server, or perhaps entire systems, may need to be rebuilt to remove as much of the attacker's foothold as possible [9]. SolarWinds published guidance [here] on how to determine if such lengths are necessary.

Rebuilding a system means losing all new information from the point at which the system was compromised. Since it is reported that the SolarWinds attack initiated around March 2020, a difficult decision must be made regarding whether to lose all new information since March or risk the possibility that the system remains compromised. That also assumes that backups used to rebuild the impacted environment are still available from before March. In-house counsel in these scenarios should consult with their Information Technology team about any impacts to the confidentiality of client information, records retention and disposal schedules, and potential legal hold implications.

There is also the cost of stolen sensitive or confidential information. For example, the Administrative Office of the U.S. Courts reported that its Case Management/Electronic Case Files system (CM/ECF) was compromised, endangering the confidentiality of sealed court documents. [10][11] The release of such information could be catastrophic to the Office of the U.S. Courts integrity, which represents just one of SolarWind's customers, including government agencies, like the DoD, and over the 425 of the U.S. Fortune 500. [6] While some portion of associated costs could be offset by cybersecurity insurance, counsel should consider supply chain vulnerabilities in an organization's risk analysis when negotiating cyber insurance coverage.

Organizations need to ask, "what happens when the solutions keeping you secure fail?" Here are a few precautions for preventing supply-chain attacks in the future:

- Reevaluate your vendor selection process. Consider who decides to select a vendor, what criteria are used for choosing a particular vendor, and whether vendor security is considered. Make sure a

formal review process is in place. Perform independent risk analysis of the vendor's security posture. Counsel should be proactive in this process by advising to select vendors who are compliant with industry and government security regulations. Start early in the RFP process to procure security commitments from vendors while you have the most leverage to negotiate.

- Counsel should ensure that the proper security requirements are included in vendor contracts. Review existing contracts and renegotiate if feasible. These attacks have also proven that only contractually mandating a vendor to take the proper precautions is not enough; you must VALIDATE their security posture through independent reviews or audits. Counsel should include requirements for audit rights in vendor contracts and include breach notice provisions.
- Counsel should advise their clients to request to be removed from customer lists, including on vendor websites. This will make it more difficult for threat actors to determine whom an organization uses as a vendor. [12]
- Diversify IT toolsets rather than having all-in-one solutions. [13] Access to an all-in-one solution, like SolarWinds, means threat actors only need one entry point to gain a foothold over an entire system. It is important to remember that additional tools must be appropriately managed.
- Temper user demand for faster, more integrated technology. Users frequently demand easier access to more data with more functionality. Such solutions add complexity to already complex systems, making the systems more difficult to secure. [9] Counsel should partner with IT to analyze the risks associated with these tools, and can promote organization-wide cyber security training on the adverse impact employee expectations may have on organizational data security.
- Identify and review all user-related applications to ensure they do not have excessive user privileges, meaning the application has more access and control to an environment than it should. Applications with administrative access can automatically act on behalf of a user, system, or application - precisely how the SolarWinds attack was executed. If necessary, upgrade solutions or select new ones with capabilities that allow you to implement least privilege practices. Counsel should advocate for and participate in regular excess privilege reviews.
- Be sure the organization has policies and resources in place to ensure that it can respond to data breaches quickly. While more of a reactive measure, counsel should ensure that they have access to legal expertise regarding breach-notification, privacy laws, and incident response firms.

[1] https://www.wsj.com/articles/solarwinds-hack-forces-reckoning-with-supply-chain-security-11610620200

[2] https://www.foxbusiness.com/technology/cybersecurity-firm-third-malware-strain-solarwinds-hack

[3] https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412

[4] https://www.thesslstore.com/blog/2013-target-data-breach-settled/

[5] https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/

[6] https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/

[7] https://www.solarwinds.com/securityadvisory/faq

[8] https://www.foxbusiness.com/technology/cybersecurity-firm-third-malware-strain-solarwinds-hack

[9] https://www.lawfareblog.com/reflections-solarwinds-breach

[10] https://www.uscourts.gov/news/2021/01/06/judiciary-addresses-cybersecurity-breach-extra-safeguards-protect-sensitive-court

[11] https://krebsonsecurity.com/2021/01/sealed-u-s-court-records-exposed-in-solarwinds-breach/

[12] https://www.zdnet.com/article/the-solarwinds-and-us-government-breach-is-not-a-marketing-opportunity/

[13] https://techcrunch.com/2020/12/21/after-the-fireeye-and-solarwinds-breaches-whats-your-failsafe/

For Cybersecurity, eDiscovery, Digital Forensics, or Information Governance needs, visit us at: www.bit-x-bit.com.