PRIVATE DIRECTORS ASSOCIATION®
Creating Value Through Board Excellence

December 22, 2020

PDA Cyber Security Newsflash

Do Not Let the SolarWinds Hack Derail Your Business

Executive Summary

There has been a significant cyber hacking incident that has impacted dozens of private, public, and governmental organizations around the world. Multiple investigations into these technology breaches are in progress and are likely to remain ongoing for some time. This briefing is intended to educate you on what is known at this time and prepare you for any incident response or cyber security governance discussions on the topic in your board meetings.

For Board Consideration

- Understanding leadership's approach and capability to cyber security incident response is best practice for Boards of Directors. If not impacted by this event, Boards should consider an incident exercise to test their capabilities.
- Cyber criminals generally seek to steal the crown jewels of the company, understanding how well protected the crown jewels of your company are from sophisticated cyber-attacks is always prudent. Using professional "white hat" hackers to test the environment should be done frequently and reported to the Board.
- Boards should evaluate their current cyber-risk and risk tolerance expectations and compare their expectations to the plan and investment that management has made in defending and detecting similar sophisticated attacks.
- Outside security expertise brings a more objective perspective; Boards should consider an outside expert for a tailored cyber security briefing.

Fundamentals of the Attack

SolarWinds is a US-based IT infrastructure and network management company with over 300,000 global customers. The system is generally used by organizations to monitor and manage their IT data networks across industries from oil and gas, to retail, manufacturing, finance, technology, critical infrastructure, government services, and national security. The hackers, who are being described as sophisticated nation-state attackers, infiltrated the SolarWinds "Orion" platform and secretly coded a backdoor for themselves into the next version of the software.

As organizations downloaded their regular software update, it came with the hacker's coded backdoor, giving the hackers direct access to what could be more than 200 organizations, as of today. It is believed at this point that there could be as many as 33,000 organizations who downloaded this backdoor and could potentially be impacted.

The SolarWinds IT platform consolidates access to many systems within the company's network, this consolidation is accomplished by allowing the Orion platform to have full access to the systems it manages, which means that anyone who gains access to the platform, essentially has the keys to the kingdom.

PRIVATE DIRECTORS ASSOCIATION®
Creating Value Through Board Excellence

This appears to be what happened in the case of organizations like FireEye, the US Treasury, the NSA, and even Microsoft. There may be other systems that have been compromised as well and are yet to be announced.

Key Considerations

- It is not likely over just yet, many potential scenarios are going forward given the attackers could have been inside affected IT systems for 8 months or longer!
- IT teams need to determine the full extent of what occurred to date and stay vigilant for updates as they are released; it is currently unclear to what extent each company may have been penetrated.
- The attack was unlikely preventable for the victims, but organizations should ensure they have the advanced detection tools/capabilities to detect the action after the hackers were inside.
- Affected organizations should not treat this as business as usual, given the head start the attackers have had, and the depth of their penetration. Leadership should establish an effort with sufficient cyber security expertise to ensure network and business system integrity.

PDA's Cyber Security Initiative can assist with providing subject matter expert briefings for Boards who are PDA members! Contact PDA at admin@privatedirectorsassociation.org.

Private Directors Association® Cyber Security Initiative
The Private Directors Association® has made Cyber Security a board governance information priority and continues to expand its efforts in this area. Through webinars, white papers, and other educational resources, PDA is providing the highest level of insights and guidance for private company owners and board members

Private Directors Association® Mission
Our mission is creating, sustaining, and enhancing Private Company value through the active use of diverse Boards of Directors and Advisory Boards. We advocate for excellent practices in board formation and governance. We provide a national network where executives and professionals interested in board service can find and meet with those interested in securing exceptional board members. We provide a welcoming and responsive culture that distinguishes us.

Disclaimer
The Private Directors Association® provides this information as a value to its members and it should be considered general information and not professional or legal advice. The reader should not rely on any information in this document in making business decisions and should seek professional advice. Laws and rules can vary by jurisdiction and members should consult with experts in evaluating their unique situation.