Six Questions for Boards to Ask after SolarWinds

Updated 15 March 2021

If it hadn't come to light on December 13, 2020 – the day before the Electoral College met and when daily reported COVID-19 cases in the US reached an all-time high of 243,000 – the SolarWinds attack would have received more sustained media attention. But the hack, which Microsoft's President Brad Smith has described as "the largest and most sophisticated attack the world has ever seen,"[1] *has* received sustained attention in corporate board rooms. While it appears that about 100 companies were infiltrated, more than 18,000 companies uploaded a compromised update to SolarWinds' Orion software. Three months later, companies are still assessing their potential exposure.

In addition to digging into the impact of the SolarWinds hack on the company itself, companies have an opportunity to use the attack as a catalyst to take a fresh look at their approach to cybersecurity. Here are six questions boards may want to ask:

1. What are we doing to prepare for state-sponsored hacks? Russia's role in the SolarWinds attack made clear that companies of any size can be targeted by state-sponsored hackers, especially companies in the software supply chain. Directors should be sure management explains what they are doing to: inventory the firm's software assets; enhance due diligence for the software supply chain; strengthen their threat-hunting programs, especially those detecting lateral movement and anomalous behavior by privileged accounts; and simulate state-sponsored attacks.

2. Are we ready for advanced ransomware attacks? Ransomware attacks used to be relatively straightforward: a hacker would block access to a company's data unless the company paid for an encryption key. With companies now routinely backing up their data, ransomware attacks have become more sophisticated and dangerous– not just blocking access to data, but threatening to make sensitive data

public, or manipulating your data in ways that can lead to enormous harm – even death if they take control of systems affecting health and safety. Many of the steps to guard against state-sponsored attacks apply equally to ransomware. In addition, directors can ask whether the company has adequate cyber insurance, how the company would handle ransomware negotiations, and how it will assure compliance with US Treasury guidelines that prevent payments to certain bad actors.

3. What are our sector-specific vulnerabilities? Each industry faces its own challenges, but two areas are worth particular focus. Manufacturing operations can be overlooked when it comes to cybersecurity. The security features of manufacturing software may be specialized, outdated, or not connected to the company's broader program. Another area of risk is the environment used for developing software and digital-based IP. In the pursuit of speed and flexibility, companies have often created work environments to give those involved in the creation of digital IP easy access to each other's work. This can be a major security risk. Ask management about its cost-benefit analysis in this area: does it make sense to reduce clearance levels for developers and increase security measures, even if it may incrementally slow down collaboration?

4. Do we have the right internal processes – and working relationships – to address evolving cyber risk? Management needs to build a strong team and a have plan before a crisis hits. Tabletop exercises are helpful. But it's useful to learn how finance, legal, technology, and other functions actually work together to address risk. Is it just at times of actual and simulated crisis, and through formal mechanisms such as quarterly risk assessments or internal information security committee meetings? Or is there a closer relationship, as typically exists between the finance and legal functions who work hand-in-glove on a range of matters on a daily basis? And does the company have a clear matrix that outlines who does what – and what our reporting process is – for each category of attack?

5. More broadly, do we have a "cyber strategy" that is keeping pace with our business strategy, competition, regulation, stakeholder expectations, and threats? Just as it's advisable for companies to have an explicit workforce strategy to support their business plans, [2] it's increasingly important for companies to have an overall strategy and policies that cover (1) cybersecurity (protection of your systems from unauthorized access), (2) data security (protection of personal and other sensitive data within those systems), and (3) privacy (prevention of misuse of personal data by both authorized and unauthorized users). Make sure you're running your business, and going to market with new products and services, with all the cost-justified protections you need.

6. What more can the board do, and what can management do to support the board? Today, 20.9% of corporate directors in the S&P 500 cite technology expertise in their biographical profile. [3] And when data is a paramount business priority, some companies such as General Motors have established a committee to

> focus on cyber risk. But there is a widespread need for broader board education and deeper engagement on cyber issues. A recent survey of C-suite executives found that, while just under half of the respondents thought their boards had good or excellent expertise in technology, only 12% found that the board understood their firm's cyber threats (and 11% understood crisis management) very well. Notably, 48% want their boards to be more assertive in challenging crisis management plans, and 37% in challenging risk management programs. [4]

This means that management – with outside resources, if needed – should ensure that the board is relatively fluent in cyber; and just as directors need to speak "tech," it is critical that technology executives be able to speak in terms that resonate with a board. Directors and management also need to have a shared understanding of the board's role in a cyber crisis. Often, the board's best role is to stay closely informed, but to leave management of the crisis *to management*.

It's not a question of whether your company will be subject to a cyberattack, but when, how, and by whom. Even the most sophisticated companies can't answer those three questions with 100% assurance. But by asking the questions posed in this article, boards can help make sure that their companies are prepared for the inevitable.

This post draws upon the expertise generously provided to The Conference Board by Latham & Watkins and Stroz Friedberg, an Aon Company.

---

[1] "SolarWinds Hack Was 'Largest and Most Sophisticated Attack' Ever: Microsoft President," Reuters, February 14, 2021.

[2] Paul Washington, Rebecca L Ray, PhD, Solange Charas, PhD, Amy Liu Abel, PhD, *Brave New World: Creating Long-Term Value through Human Capital Management and Disclosure* , The Conference Board, December 2020.

[3] Matteo Tonello, *Corporate Board Practices in the Russell 3000 and S&P 500: 2020 Edition*, The Conference Board, October 2020.

[4] *Board Effectiveness: A Survey of the C-suite*, PWC and The Conference Board, December 2020.

AUTHORS

Paul Washington
President and CEO
Society for Corporate Governance