PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

The SolarWinds Digital Breach and Why It Matters

By Thomas J. DeMayo, Principal, David Plunter, Supervisor and Robert Frank, Supervisor

Over the past few weeks, two company names have dominated the news, SolarWinds and FireEye. If you work in IT or as a security professional, these companies are considered to be household names; however, for the vast majority of senior management teams and boards of directors, this is most likely the first time they are hearing about them.

What Happened?

SolarWinds is a very popular software vendor that creates a suite of applications that many corporations utilize to manage and monitor their systems and networks. They simplify the life of IT departments by affording them central control and visibility across their fleet of systems and devices. In the context of the services they provide, they become linked into the supply chain of the businesses that implement their software. Given the nature of the services provided, they operate at a very privileged level.

FireEye is recognized as one of the leading global cybersecurity firms that help organizations understand and manage their cyber risk. FireEye, like countless other companies, utilizes SolarWinds. It was in the first week of December when FireEye identified that the very software they depended on to manage and monitor their internal network was being used against them and, ultimately, they had been breached.

It was determined that an incredibly sophisticated nation state cyber group had compromised SolarWinds as a company and managed to inject malicious code into their products without raising any alarms. The newly-introduced malicious code was than deployed to the SolarWinds customer base as a legitimate software update. Once the update was installed, the nation state cyber group was able to gain a foothold into a multitude of a company's customer networks. In the case of FireEye, the attackers stole the various customized hacking tools used by FireEye when they perform penetration tests for their customers.

Fortunately, FireEye was able to detect and identify the attack through a robust process of monitoring and threat hunting in their internal network. It was noted by SolarWinds that approximately 18,000 businesses had been impacted by this breach. A short list of compromised customers includes the U.S. Treasury, U.S. Postal Service, U.S. Air Force, U.S. Department of Defense, Lockheed Martin, Microsoft, Visa, Ernst & Young, AT&T, Dow Chemical, and the Federal Reserve Bank.

Why Does It Matter?

As a business, you will inevitably work with other entities and ultimately depend on them to provide certain services or products. Part of that relationship becomes built on trust, and the business you partnered with becomes a link in the supply chain that helps power your business. In that trust lies the issue. In the words of President Reagan, "Trust but verify."
The SolarWinds breach brought to light a digital risk that has always existed, but has never been so well taken advantage of – until now. The breach brought to light the enormity of supply chain risk; the market place of products and services that companies rely on to drive their success.

In an increasingly digital and interconnected world, one that is rapidly moving toward cloud first and mobility models, the supply chain risk is going to jump exponentially. While SolarWinds is deemed the first, it most certainly won't be the last.

What Can We Do?

The big question that is now on everyone's mind is how do we defend or stop it from happening again. A consistent phrase that is used by the cybersecurity community is that it is ***not a matter of IF, but WHEN***, an incident will occur. The SolarWinds breach demonstrates that some of the most sophisticated and well-protected businesses on the globe are vulnerable and will remain vulnerable. No one is immune.

While it is easy to cast stones at FireEye or some of the other prominent names impacted by this breach, and question "how could they let that happen" that particular view is unrealistic and will continue to disappoint any person that holds it going forward. Yes, FireEye was breached, but they have also become the model in demonstrating to the world just how important being prepared for a breach is. Thankfully, FireEye detected the breach, which was no small feat given the level of sophistication of the attack. The key takeaway is that they detected and responded in a timely, professional, and honest manner.

To this day, effective monitoring of a network to identify intrusions is one of the most complex and often expensive line items in a company's cybersecurity budget. Not only does it require specialized tools and skillsets, but it is the most critical in detecting and stopping a breach and ensuring appropriate visibility into the chain of events after the attack. Without effective monitoring, your business is ultimately running blind.

The SolarWinds attack should serve as a reminder or wakeup call that cybersecurity is a key business issue and needs to be understood and addressed by those who are responsible for governance. There will never be a single silver bullet that will solve the cybersecurity problem. Cyber risk requires a holistic strategy across the people, processes, and technologies that drive your business to effectively manage it. It requires a risk-based approach that supports the mission and strategies of the business. It requires a plan not only to manage the cyber risk, but also a plan to respond when an incident occurs. In addition, a clear understanding of your supply chain risk is key.

While SolarWinds is an extreme example, there are plenty of service providers and suppliers that currently support your business that can be risk-assessed and validated to ensure they have the appropriate controls and they themselves have a reasonable security program.

The following are key steps you can do now:

- Confirm with your IT Department whether a SolarWInds product deployed in the environment.
- If it exists and is listed as an impacted product, ensure that the necessary patches have been installed. A full listing of impacted products can be found here.
- If you utilize a security monitoring service, verify that they are aware of and are utilizing the Indicators of Compromise provided by FireEye to identify usage of their stolen tools. The IOCs can be found here.

The following are longer term considerations:

- Create or re-evaluate your existing third party risk management program. Ensure all vendors have been assigned an appropriate risk rating.
- Confirm your existing information security and data risk management process is comprehensive and well-informed by utilizing qualified individuals. The risk assessments should be supplemented with external qualified and unbiased viewpoints.
- Begin to embrace a "Zero Trust Model," i.e., allowing users to connect from anywhere as long as you validate the user, the device, and limit access.
- Evaluate your incident response plan and schedule table top exercises with the team to ensure roles and responsibilities are well understood.
- If you have security and monitoring tools in place, engage a third party to test the effectiveness of those tools in preventing and/or detecting the attacks.

Contact Us

Sometimes the most important step you take to help secure your cyber infrastructure is the first step. If you need assistance in evaluating your third party risk management or guidance in any of these areas discussed in this article, we are always here to help. At PKF O'Connor Davies, we have the resources to help you navigate your path forward across all facets of your business. We encourage you to contact us **today** so you can continue down that path of success.

Thomas J. DeMayo, Principal, Cyber Risk Management
CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE
212.867.8000 or 646.449.6353 (direct)
tdemayo@pkfod.com

About PKF O'Connor Davies

PKF O’Connor Davies, LLP is a full-service certified public accounting and advisory firm with a long history of serving clients both domestically and internationally. With roots tracing to 1891, sixteen offices in New York, New Jersey, Connecticut, Florida, Maryland and Rhode Island, and more than 900 professionals, the Firm provides a complete range of accounting, auditing, tax and management advisory services. PKF O’Connor Davies is ranked 27th on *Accounting Today’*s 2020 “Top 100 Firms” list. It is also ranked among the top 20 best accounting employers to work for in North America by *Vault*.

PKF O’Connor Davies is the lead North American representative in PKF International, a global network of legally independent accounting and advisory firms located in over 400 locations, in 150 countries around the world.

Our Firm provides the information in this e-newsletter for general guidance only, and it does not constitute the provision of legal advice, tax advice, accounting services, or professional consulting of any kind.