OLLIS/AKERS/ARNEY
INSURANCE & BUSINESS ADVISORS
PROTECTING TOMORROW...TODAY.

Cyber Case Study

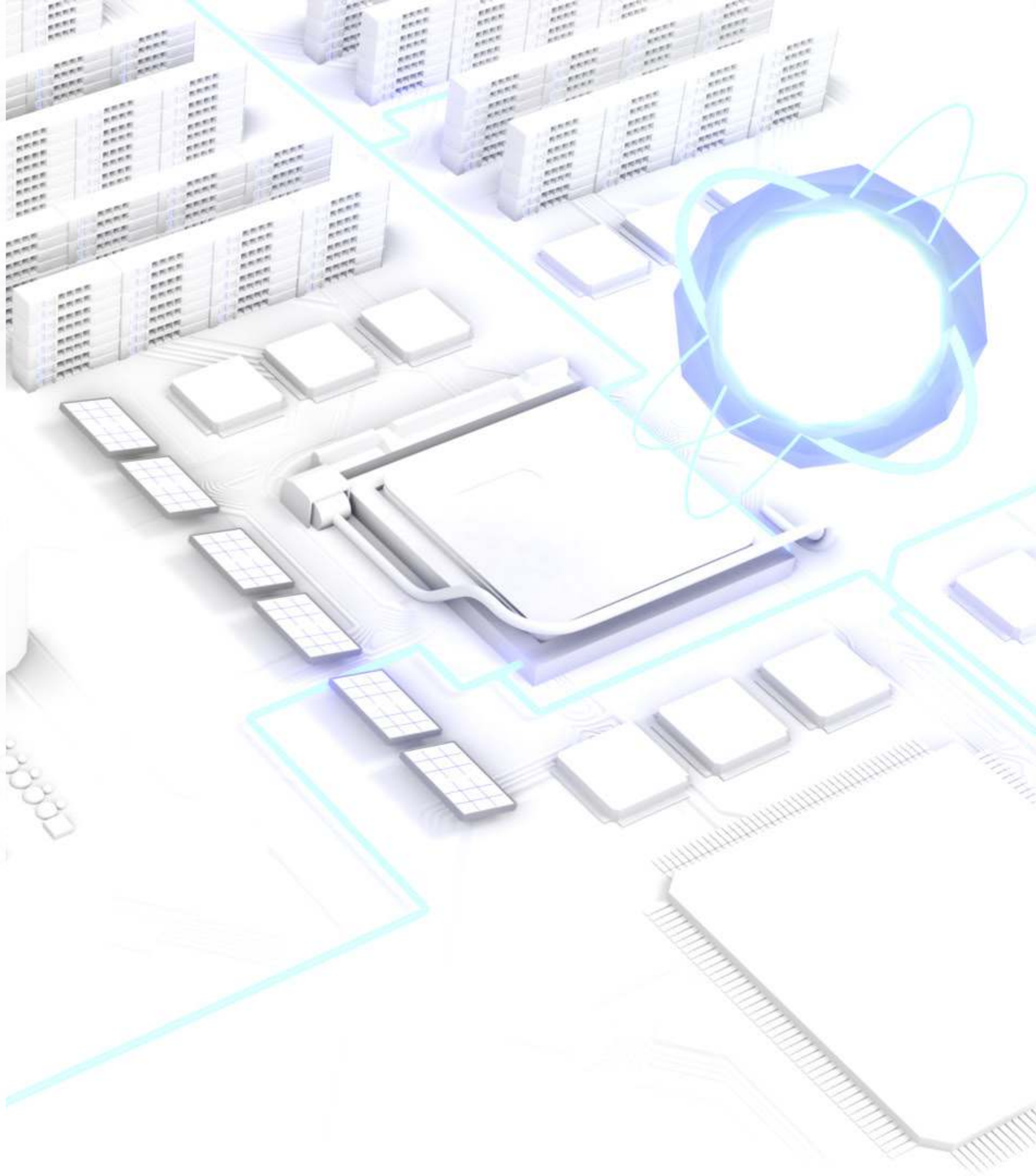
provided by Ollis/Akers/Arney Insurance & Business Advisors

SolarWinds Supply Chain Cyberattack

In the final month of 2020, it was revealed that foreign hackers had orchestrated a supply chain cyberattack throughout the past year in an effort to compromise several federal agencies and private organizations. The cybercriminals first infiltrated the digital infrastructure of SolarWinds—a Texas-based technology company—before using that infrastructure to gain access to sensitive data from a range of government departments and organizations via malware-ridden software updates. The incident ultimately exploited numerous SolarWinds customers and led to millions of dollars in total losses.

The attack has been dubbed as one of the largest and most sophisticated cyber incidents in U.S. history, motivating many organizations to take a closer look at security risks stemming from their supply chains and software providers. In hindsight, there are various cybersecurity lessons that organizations can learn by reviewing the details of the SolarWinds incident.

Read on for everything your organization needs to know.



The Details

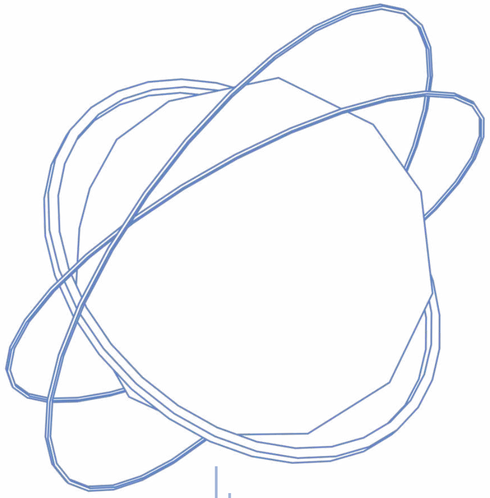
The incident first began in September of 2019, when foreign cybercriminals were able to gain unauthorized access to SolarWinds' digital infrastructure. Although it's unclear exactly how the infrastructure was infiltrated, IT experts have confirmed that the hackers likely leveraged highly advanced digital skills to accomplish this feat. From there, the cybercriminals utilized the final months of 2019 to test whether they could inject a form of malware called Sunburst into SolarWinds' software. During this time, the hackers remained undetected within the company's digital infrastructure.

On Feb. 20, 2020, the cybercriminals officially administered Sunburst into SolarWinds' flagship software product, Orion. Just over one month later, SolarWinds—unaware that the hackers had weaponized its product with malware—began sending out Orion software updates to customers. By installing these updates, impacted customers unknowingly introduced the harmful malware to their own technology. As a result, this malware provided the cybercriminals with a hidden entry point—also known as a digital backdoor—to all affected customers' networks. Although the hackers did not appear to use this backdoor to compromise customers' sensitive data, it certainly gave them the ability to do so.

In total, more than 18,000 SolarWinds customers downloaded the malware and were at risk of potentially having their records exposed during the attack. Because SolarWinds built a reputation as a top U.S. technology company, many of the victimized customers were high-profile organizations and federal agencies. These customers included Microsoft, Intel, Cisco and Deloitte, as well as the Pentagon and the U.S. Departments of Homeland Security, Justice, State, Commerce and Treasury.

Despite the malware incident occurring in early 2020, the hackers' activity went undiscovered for several more months, allowing them continued access to customers' sensitive data. In December of 2020, FireEye—a cybersecurity firm and SolarWinds customer—detected the malware within its network and traced it back to SolarWinds. On Dec. 11, 2020, FireEye informed SolarWinds of the incident. Days later, SolarWinds reported the attack to the U.S. Securities and Exchange Commission (SEC).

Upon investigating the incident, the federal government confirmed that the cybercriminals responsible were likely associated with APT29—which is a Russian hacking group. IT experts then helped SolarWinds and its impacted customers implement a "kill switch" to control the malware and effectively close the digital backdoor that the hackers had created.



The Impact

Because the incident was relatively recent, its overall impact has yet to be seen. As of now, the following consequences resulted from this large-scale attack:

Recovery costs

Both SolarWinds and its impacted customers are expected to incur a combined total of more than $90 million in recovery expenses related to the incident. These costs include investigating the attack, informing all affected parties, removing the malware from every infected network, recovering compromised data and implementing updated cybersecurity protocols to prevent future incidents. Since the attack impacted federal agencies, these costs have the potential to trickle down to U.S. taxpayers as well.

Reputational damages

Considering SolarWinds maintained a trusted and respected reputation prior to the attack, the technology company received significant criticism from customers and the public for its cybersecurity shortcomings after the incident occurred. In particular, SolarWinds was scrutinized for failing to detect the cybercriminals' initial activity within its network and remaining unaware that Orion had been injected with malware until FireEye's eventual discovery months later. Further, while the method hackers used to infiltrate SolarWinds' network is unknown, it was soon discovered that a handful of the company's employees possessed weak passwords leading up to the incident (one employee's password was "solarwinds123")—paving the way for additional security criticism. Amid this scrutiny, SolarWinds' stock price fell by 40% the week following the incident.

Legal ramifications

In January of 2021—one month after the details of the incident became public—disgruntled shareholders filed a class-action lawsuit against SolarWinds for its cybersecurity failures during the attack. Several months later, the SEC announced plans to investigate whether SolarWinds' affected customers accurately estimated the impact of the incident within their financial records. As time goes on and additional damages come to light, it's certainly possible that both SolarWinds and its customers could encounter more lawsuits and regulatory fines related to the incident.

Both SolarWinds and its impacted customers are expected to incur a combined total of more than **$90 million** in recovery expenses related to the incident.

SolarWinds' stock price fell by **40%** the week following the incident.

Lessons Learned

There are several cybersecurity takeaways from the SolarWinds attack. Specifically, the incident emphasized these critical lessons:

Supply chain exposures shouldn't be ignored.

Above all, this attack showcased how critical it is for organizations to evaluate and address security concerns within their supply chains, including IT and software providers. Even if an organization follows proper cyber policies and procedures internally, a compromised supplier could still end up threatening its security and digital assets. Supply chain exposures can stem from various avenues—including vendors with access to organizational networks, third parties with inadequate data storage measures and suppliers with poor overall cybersecurity practices.

While it's not possible to totally eliminate supply chain risks, there are several steps organizations can take to help reduce these exposures and prevent costly attacks, such as:

- Incorporating cyber risk management into vendor contracts—This can include requiring vendors to obtain cyber insurance, having them issue timely notifications regarding cyber incidents and establishing clear expectations regarding the destruction of data following the termination of contracts.
- Minimizing access that third parties have to organizational data—Once a vendor or supplier has been selected, it's crucial to work with them to address any existing vulnerabilities and cybersecurity gaps. Moving forward, suppliers' access to sensitive data should be restricted on an as-needed basis.
- Monitoring suppliers' compliance with supply chain risk management procedures—This may entail adopting a "one strike and you're out" policy with suppliers that experience cyber incidents or fail to meet applicable compliance guidelines.

Third parties must prioritize cybersecurity.

As organizations begin to more closely evaluate their supply chain exposures, it's increasingly vital for third-party vendors themselves to adopt effective cybersecurity measures. In particular, suppliers need to recognize that cybercriminals may target them in order to compromise their larger clients and take steps to prevent such incidents from occurring. After all, failing to do so could not only result in cybersecurity vulnerabilities, but also contribute to reduced client trust and lost business. By upholding proper digital practices, third-party vendors can show their clients that they take security seriously, boost their overall reliability and—in some cases—secure additional contracts.

Access controls can offer a strong defense.

Although it's unknown whether SolarWinds' access control protocols or password blunders contributed to the incident, IT experts attest that bolstering these cybersecurity elements can play a major role in defending against hackers and subsequent attacks. Valuable access control and password tactics include the following:

- Instructing employees to develop complicated and unique passwords for their accounts in addition to changing these passwords on a routine schedule
- Implementing multifactor authentication measures that require employees to verify their identities in several ways (e.g., entering a password and answering a security question)
- Limiting employees' digital access solely to the technology, networks and data they need to perform their job responsibilities
- Segmenting different workplace networks to prevent all networks from being compromised if a single employee's credentials are exploited

Lessons Learned (cont.)

Effective security and threat detection software is critical.

This incident emphasizes the importance of having appropriate security and threat detection software in place. This software can be used to better identify suspicious digital activity and reduce dwell time—which refers to how long it takes to detect cybercriminals' presence after their initial network infiltration. Although this software may seem like an expensive investment, it's well worth it to help continuously monitor security threats, catch perpetrators before it's too late and minimize the impacts of potentially devastating cyber incidents. Necessary software to consider includes network monitoring systems, antivirus programs, endpoint detection products and patch management tools. Also, it's valuable to conduct routine penetration testing to determine whether this software possesses any security gaps or ongoing vulnerabilities. If such testing reveals any problems, these issues should be addressed immediately.

Proper coverage can provide much-needed protection.

Finally, the SolarWinds incident made it clear that no organization—not even a major technology company—is immune to cyber-related losses. That's why it's crucial to ensure adequate protection against potential cyber incidents by securing proper coverage. Make sure your organization works with a trusted insurance professional when navigating these coverage decisions.

For more risk management guidance and insurance solutions, contact us today.