Client alert: SolarWinds cyber incident

Business impact and organizational considerations

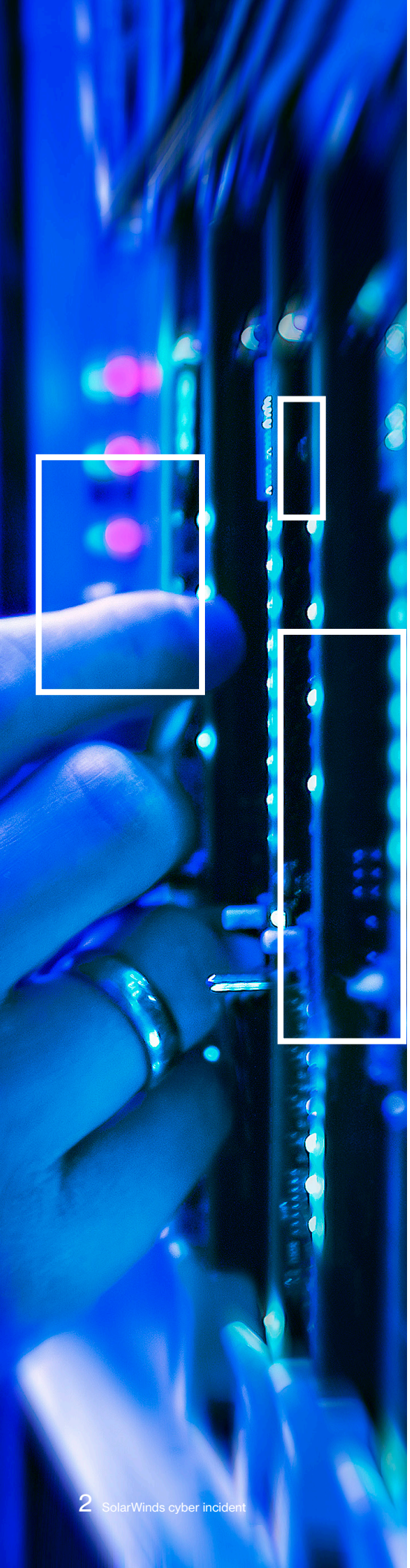
The SolarWinds cyber incident continues to cause significant global business and geopolitical consequences. Recent developments have confirmed that this was an unprecedented supply chain software attack with broad, systemic ramifications. The impact of this attack on organizations is still unfolding however the following alert outlines some key considerations in identifying and mitigating known risks. Organizations should closely monitor developments and ensure that technical controls and ongoing security recommendations are implemented.

Background

This incident was first publicized by FireEye who reported that they had been the victim of a highly sophisticated cyberattack in which attackers accessed internal systems but not client data. Please refer to our previous client alert for more background, as well as FireEye's released guidance and countermeasures for organizations impacted by this incident.

A subsequent investigation found the FireEye intrusion was caused by malicious code from SolarWinds Orion software, a network monitoring and management platform. The attackers gained access to SolarWinds network as early as September 2019, with the malware being distributed in software updates between March and June 2020. Approximately 18,000 organizations, both private and governmental, installed the SolarWinds Orion updates during this period. Once this malware was installed, a second malware could be activated to set up a backdoor allowing the hackers to observe activities within these networks. It has been reported that approximately 250 organizations had the second malware activated in their networks, with many U.S. government agencies and large technology companies targeted. Microsoft has stated that their source code was accessed (but not altered) and it has been reported that the hackers gained access to a number of technology companies including Intel, VMware and Belkin, among others.

The targeted nature of the attacks indicate that the hackers were aiming to infiltrate key technology 'supply chains' to gain maximum access to networks. The U.S. intelligence community has attributed responsibility to Russian state sponsored actors. Notably, A U.S.-CERT government alert indicated there is evidence that SolarWinds was not the only attack vector used. It is possible that additional widely used applications were also compromised, meaning that the scope of the attack and number of affected organizations could still broaden significantly.



Organizational considerations

Countermeasures and risk mitigation

The scope and breadth of the SolarWinds cyber incident is still unfolding but this is an unprecedented systemic attack that will have long term ramifications. SolarWinds has released detailed guidance and countermeasures to remediate the discovered vulnerabilities arising from this attack. We recommend immediately patching and updating relevant systems, while concurrently monitoring the ongoing situation closely. It is likely that as more information becomes available additional updating and countermeasures will become necessary. Additionally, cyber criminals will inevitably seek to exploit discovered vulnerabilities and create new methods of attack adapted from the SolarWinds malware to target organizations.

Managing the technology supply chain

The SolarWinds cyber incident was perhaps the largest ever software supply chain cyberattack. Rather than targeting a specific organization, the hackers infiltrated a third party that would allow the malware to be installed on target organizations' networks, greatly increasing the scale of the attack. This method of attack highlights the critical importance for organizations in effectively assessing and managing vendor relationships. Almost all organizations utilize third-party technology providers and they are increasingly the method in which hackers gain access to an organization's sensitive data and systems. Awareness and documentation of which third-party providers are utilized, controlling vendor access to critical devices, if practical, and ongoing risk assessment and cost benefit analysis of using vendor systems all play an important part in managing this core risk. It is also important for an organization to review their potential contractual rights to inspect vendor systems and notification obligations by the vendor for cyber incidents affecting their networks.

Insurance markets are reacting and may limit coverage

The widespread impact of the SolarWinds hack and the significant potential financial consequences to organizations affected has caused insurance carriers to analyze their exposures and seek to minimize potential losses. Carriers are increasingly seeking clarification from insureds on whether SolarWinds Orion software was used and some are seeking to limit exposure or exclude coverage entirely if remediation updates are not installed. In an already hardening insurance market caused by a dramatic increase in ransomware attacks, this incident is likely to be impactful in changing terms and availability of cyber coverage for some organizations. It is important for organizations to be aware of their potential exposure to this incident and be prepared for detailed additional enquiries from carriers on technical measures they are taking to manage vendor and broader cyber risks.

Other insurance considerations

Cyberinsurance policyholders, especially those who utilize the Orion platform and/or have been notified of a SolarWinds event-related compromise at a third-party vendor should strongly consider reporting this matter to their insurer(s). Given the breadth of the attack and sheer number of potentially affected organizations, including government agencies, even those cyberinsurance policyholders without a definitively known compromise in-house or at a vendor, should discuss with their broker whether a notice to the insurer(s) of a potential compromise is prudent under the circumstances.

About the FINEX Cyber Risk Solutions team

The FINEX Cyber Risk Solutions team is a global team of consultants offering tailored services that support insurance goals, align cyber risk management with business objectives and deliver cost effective Cyber Risk Resilience. The CRS team can design solutions to meet client needs in Cyber Risk Assessment and Quantification, Incident Response and Business Continuity Planning, Operational Risk Analysis, Governance and Policy development and many other cyber risk areas.

Why Willis Towers Watson

More than half of all cyber incidents begin with employees, so it's a people problem. And the average breach costs $4 million, so it's a capital problem, too. No one decodes this complexity better than Willis Towers Watson. As a global leader in human capital solutions, risk advisory and broking, we are well prepared to assess your cyber vulnerabilities, protect you through best-in-class solutions and radically improve your ability to successfully recover from future attacks.

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 45,000 employees serving more than 140 countries and markets. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas – the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

Contact

Dominic Keller
Global Team Leader, FINEX Cyber Risk Solutions Team
dominic.keller@willistowerswatson.com

willistowerswatson.com/social-media

willistowerswatson.com

Willis Towers Watson