HINSHAW

Alerts

# Six Information Security Tips to Mitigate the Risk of a SolarWinds-Like Breach

**January 13, 2021**
*Hinshaw Privacy & Cyber Bytes*

The impacts and implications of the recent SolarWinds breach are widespread and on-going. SolarWinds' network-monitoring and management software was used by customers worldwide—including the U.S. military, Fortune 500 companies, government agencies, and educational institutions—to manage their own computer systems. The apparent expert consensus is that Russia used SolarWinds' hacked program to infiltrate roughly 18,000 government and private networks.

Microsoft and FireEye, both victims of the hack, have issued reports detailing the malware specs that hackers added to the SolarWinds' monitoring product updates that were uploaded to customer computers. The Cybersecurity & Infrastructure Security Agency, the New York State Department of Financial Services, and other cyber agencies and regulators have issued advisories requiring immediate action by entities using the affected SolarWinds products or usage by third parties with access to regulated entities' networks and data. There are also increasingly pointed news reports concerning SolarWinds' management and security practices.

Even for organizations not directly impacted, this incident provides incentive to revisit basic security hygiene. In particular, it is important to manage the security risks associated with third-party service providers to ensure that the security of information and information assets is not reduced when: (1) exchanging information with the third party, or (2) introducing their products and services into your environment.

Complacency with respect to third parties is unwise. Organizations can take a few critical steps to improve their security:

1. Confirm that you and your third-party vendors are not implicated by the SolarWinds breach
2. Re-risk assess your data and information system assets and current security posture
3. Revisit your due diligence process for third-party service providers and your procurement of technology
4. Revisit employee security education and training
5. Enhance your protocols for data and information systems access, including authorizations, network segmentation, and backups

## Service Areas

Privacy, Security & Artificial Intelligence

6. Test your security incident response plan, including, in particular, new reporting and notification requirements to regulators and government agencies