Cybersecurity at MIT Sloan

Cybersecurity at MIT Sloan The SolarWinds Attack: A Cybersecurity Game-Changer?

Cybersecurity at MIT Sloan brings thought leaders from industry, academia, and government together with MIT faculty, researchers, and students to address strategy, management, governance, and organization of cybersecurity of critical infrastructure using an interdisciplinary approach.

> *"Most existing cybersecurity approaches and solutions failed us during this incident. SolarWinds has shown us that we may need to be doing things fundamentally differently."*

The SolarWinds Attack – What Happened?

It is known is that the build process of SolarWinds was compromised and a backdoor was embedded in the code of the Orion network management product, which is used around the globe. The compromised software was downloaded by roughly 18,000 organizations including leading businesses and government organizations.

The malware was not detected for almost a year until December 2020, when a request to add a user device triggered an alert at FireEye, a leading cyber-security company. The backdoor allowed threat actors to penetrate hundreds of systems and use sophisticated lateral steps to escalate the attack and avoid detection.

Since the SolarWinds incident, other similar attack vectors have since been detected. While the magnitude, impact, and root-cause are not fully known, it's clear that most existing cyber-security approaches and solutions proved inadequate for addressing the SolarWinds attack and similar incidents.

Aftermath – Advancing Toward a New Cybersecurity Paradigm

Research efforts are focused on new systematic, data-driven scalable approaches to quantifying and prioritizing cyber-risk. There is a need for better methods for assessing and managing the cyber risk of supply chains beyond questionnaires and outside-in scores. New scenario-based models will lead to more effective cyber-risk management. Zero-trust approaches need to be enhanced to be more effective in addressing emerging cyber threats

Cross-organization cyber accountability and shared-responsibility models must be redefined and re-assessed. Better overall cyber-risk transparency, effective alignment of economic benefits with cybersecurity needs, and improved data-sharing approaches for supply chain ecosystems, are urgently needed. This can be supported with more effective public-private cybersecurity partnerships – at national and global levels.

SolarWinds as a Game-Changer

Similar attacks can be performed by less sophisticated and less resourceful threat actors with devastating consequences. The incident highlights a breakdown of liability and accountability boundaries across organizations. In the aftermath of SolarWinds there have been multiple cases of finger-pointing across organizations related to the incidents root-causes and escalations. The incident caused a significant erosion of trust and confidence, specifically around data integrity and system cybersecurity management.P

IMPACT: The scope, impact, and sophistication of this cyber-attack were unprecedented, and most existing protection and detection mechanisms proved ineffective. New approaches are required for assessing and monitoring cyber-risk in supply chains in an effective and scalable manner. Related attacks may involve modification and corruption of data, beyond data exfiltration.

Cybersecurity at MIT Sloan welcomes funding from sponsors for general support of the consortium research, and from organizations interested in specific research topics. All members and sponsors receive invitations to consortium events and activities, and access to consortium research, websites, and newsletter. For more information visit cams.mit.edu or contact:

Dr. Stuart Madnick • Professor and Director • smadnick@mit.edu
Dr. Michael Siegel • Director • msiegel@mit.edu
Dr. Keri Pearlson • Executive Director • kerip@mit.edu