SOLARWINDS FOR LAWYERS AND PRIVACY OFFICERS

Mark E. Schreiber
Senior Counsel
Boston
mschreiber@mwe.com
+1 (617) 535-3982

Brian Long
Associate
Dallas
brlong@mwe.com
+1 (214) 295-8085

May 25, 2021

mwe.com

McDermott Will & Emery

AGENDA

- Why Lawyers Need to Know This
- What is SolarStorm?
- History, Kill Chain, and Chronology of SolarStorm
- What Do Lawyers Need to Ask?
- “Reasonable Security” After SolarStorm and CISA Alerts
- Third Party Due Diligence
- What’s Next?

SOLARWINDS DUE DILIGENCE AND CISA GUIDANCE

- Has Company used or installed any of the affected SolarWinds Orion products on its systems from March 2020 - December 2020 (affected versions: 2019.4 HF5, 2020.2 RC1, 2020.2 RC2, 2020.2, 2020.2 HF1) [*see* https://us-cert.cisa.gov/ncas/alerts/aa20-352a]?
- If Company has used or installed the affected versions,
  - was an investigation conducted that followed CISA SolarWinds guidance (or similar guidance) to determine if there was any compromise of systems following the use or installation of the affected versions? [*see* https://us-cert.cisa.gov/ncas/current-activity/2021/03/17/ttp-table-detecting-apt-activity-related-solarwinds-and-active]
  - Following any investigation, were there any indications of compromise (including beaconing) or any signs of potential intrusion, access, or compromise?
  - Has Company performed a risk or impact assessment to determine which CISA category (1 – 3) [https://us-cert.cisa.gov/ncas/alerts/aa20-352a] is applicable?

WHAT DOES “REASONABLE SECURITY” LOOK LIKE?

- National Institute of Standards and Technology (NIST)
- Federal Guidance (e.g. FTC’s 2017 “Stick with Security” series)
- Regulatory Guidance (e.g. GLBA / NYDFS Regulations)
- Guidance from California regulators and/or enforcement actions
  - California Department of Justice (CDOJ) released the California Data Breach Report (Feb. 16, 2016) [CIS Top 20]
    - *“The 20 controls in the Center for Internet Security’s Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization’s environment constitutes a lack of reasonable security.”*

THIRD PARTY DUE DILIGENCE

- Multiple frameworks require assessment and/or monitoring of third parties (e.g. ISO 27001, PCI DSS, NERC CIP)
- Multiple versions of SolarWinds third-party questionnaires used
  - in various stages of maturity and completeness
  - some with delays in responses
  - some with ambiguous or incomplete responses
- Third party questionnaires can incorporate the CISA guidance
  - category framework provides ability to compare third party responses
  - gives a list of mitigations to inquire about

WHAT'S NEXT AND FURTHER DEVELOPMENTS

- Even with SolarStorm the story may not be over
- New Executive Order (May 12, 2021)
- PCI DSS 4.0 (Due Q4 2021)
- More Events and More Due Diligence will be Required

APPENDIX: LINKS AND WEB RESOURCES

- CISA Supply Chain Compromise Page https://www.cisa.gov/supply-chain-compromise
- CISA Alert AA20-352A (includes mitigation categories) https://us-cert.cisa.gov/ncas/alerts/aa20-352a
- CISA Fact Sheet: Russian SVR Activities Related to SolarWinds Compromise https://us-cert.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Russian_SVR_Activities_Related_to_SolarWinds_Compromise_508C.pdf

179670769v1