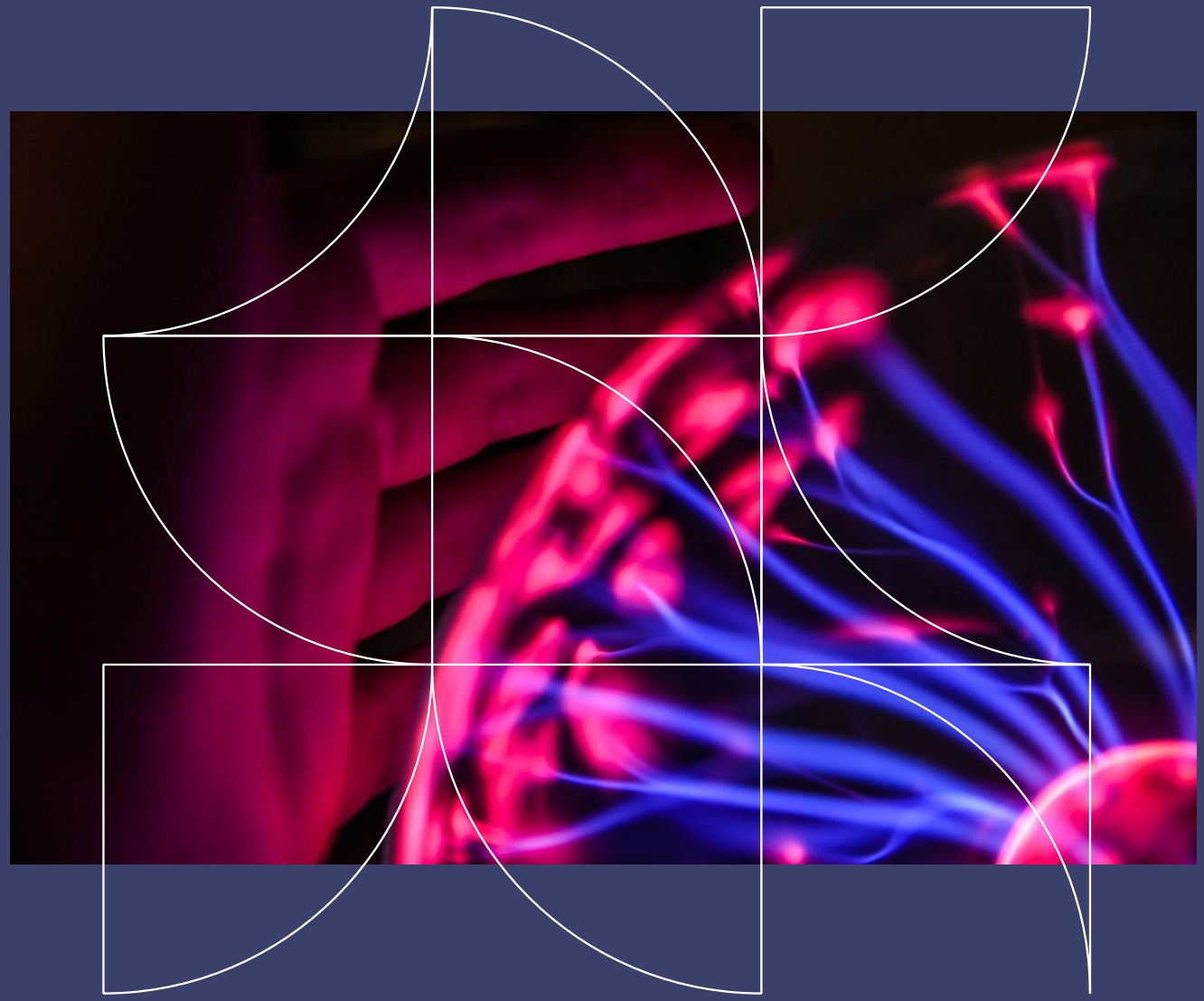
Seyfarth

Responding with Strength
to the SolarWinds Attack



Kate Fazzini, Robert Zukis, Chris Cummiskey, Jerry Bessette and Paul Ferrillo

May 26, 2021

Seyfarth Shaw LLP

Seyfarth

Legal Disclaimer

This presentation has been prepared by Seyfarth Shaw LLP for informational purposes only. The material discussed during this webinar should not be construed as legal advice or a legal opinion on any specific facts or circumstances. The content is intended for general information purposes only, and you are urged to consult a lawyer concerning your own situation and any specific legal questions you may have.

Presenters

Paul Ferrillo
Seyfarth Partner, Privacy & Cybersecurity

Jerry Bessette
Senior VP, Booz Allen's Cyber Incident Response Program

Chris Cummiskey
CEO, Cummiskey Strategic Solutions, LLC

Kate Fazzini
CEO, Flore Albo LLC

Bob Zukis
CEO, Digital Directors Network

Agenda

Responding with Strength to the SolarWinds Attack

1 | What do we know publicly about the SolarWinds attack?

2 | The Government Response to the SolarWinds attack?

3 | Was this a board failure, an IT failure, or both?
The Systemic nature of cybersecurity.

4 | Lessons Learned

5 | What is the answer? Rule-making? Compliance?
Frameworks? or “All of the above”?

6 | Questions

Cyber Security Risk
is at an All-Time High

Startling stat from 2019: *Organizations and security leaders say, now matter how much. A money and effort they are putting into cybersecurity products and tech, they don't feel safe.*

91% *of organizations believe they are at risk for significant cyberattack*
-ESG/ISSA 2019 Report

95% *of CIOs expects cybersecurity threats to get worse*
-2019 CIO Agenda

77% *of security leaders anticipate a critical infrastructure breach which could have hazardous repercussions*
-Black Hat 2019 report

Responding with Strength to the SolarWinds Attack

- What happened?
- How? By zero-day? OR was this vulnerability already known?
- Who was breached?
- Why SolarWinds? What did they do right? What did they do wrong?
- Where are the software problems?
  – what do you know about your software vendor?
  – what work did you do to vet its software updates?
  – do you always click on the “Install Button?”

The Role of the Government

- The Players
  - CISA
  - DHS
  - The NSA
  - The FBI

- The White House Response
  - The New Biden Administration Executive Order on Cybersecurity

Clearly, boards must take seriously their responsibility to ensure that management has implemented effective risk management protocols. Boards of directors are already responsible for overseeing the management of all types of risk, including credit risk, liquidity risk, and operational risk — and there can be little doubt that cyber-risk also must be considered as part of board's overall risk oversight. The recent announcement that a prominent proxy advisory firm is urging the ouster of most of the Target Corporation directors because of the perceived "failure…to ensure appropriate management of [the] risks" as to Target's December 2013 cyber-attack is another driver that should put directors on notice to proactively address the risks associated with cyber-attacks.

Luis Aguilar, former Commissioner of the Securities and Exchange Commission 2014

The Securities and Exchange Commission on Cyber Risk

The 2018 SEC Commissioners' Guidance on Cybersecurity, Release No. 33-10459 does not say whether public company board should have a cybersecurity expert member. It does say that a company must disclose the extent of the board's role in overseeing the company's risk.

"To the extent cybersecurity risks are material to a company's business, we believe this discussion should include the nature of the board's role in overseeing the management of that risk," the SEC said in the guidance. "In addition, **we believe disclosures regarding a company's cybersecurity risk management program and how the board of directors engages with management on cybersecurity issues allow investors to assess how a board of directors is discharging its risk oversight responsibility in this increasingly important area."**

SolarWinds Again Raises the Ugly Head of Cyber and Systemic Risk

- The Role of the Board Generally When it comes to Cyber Risk
- Enterprise Risk Management
- Cyber Risk
- Systemic Risk
- What's the difference between the three risks?
- Why Don't Boards 'get' Cyber Risk and its intersection with Systemic Risk?

Lesson Learned from the SolarWinds attack

- Board Education on Cyber and Systemic Risk
- The Importance of vendor/supply chain risk management
- Software supply chain risk management
- What's in your "threat detection" wallet? Can AI or Machine Learning Solutions Help Find the Needle in the Haystack?
- Can Zero Trust Help?
- Information Sharing is Caring
- The value of employee training – don't click on the link!
- Cyber Security Best Practices – the NIST Cybersecurity Framework

solarwinds

Lesson Learned from the SolarWinds attack

- After SolarWinds, what is the right answer? How do we change the cybersecurity paradigm in a positive direction?
- Compliance Efforts? Do they matter? Do they make you safe?
- Executive Rule-Making? Congressional Law Making
- Frameworks?

solarwinds

Thank you

For more information please contact us.

Paul Ferrillo: pferrillo@seyfarth.com
Jerry Bessette: Bessette_Jerry@bah.com
Chris Cummiskey: Chris@cummiskeyllc.com
Kate Fazzini: kfazzini@florealbo.com
Bob Zukis: bob@digitaldirectors.network