THE WHITE COLLAR CRIME COMMITTEE NEWSLETTER, SUMER/FALL 2024

Published by the American Bar Association Criminal Justice

Standing in the Breach: Criminally Charging Cybersecurity Officers

By Monica D. Cliatt[1]

As the digital landscape evolves and the role of Chief Information Security Officers (CISOs) continues to expand, so does their potential exposure to criminal liability. Tasked with safeguarding an organization's digital assets, their responsibilities can carry significant legal implications.

Various scenarios, such as not implementing adequate security measures, not promptly reporting data breaches, or providing false information to regulatory bodies have led to government investigations and civil penalties. However, now that the government is turning to criminal prosecutions, considerable evidentiary problems await them.

CISOs Facing Criminal Prosecutions

Recently, federal prosecutors criminally charged two notable CISOs. A jury found Joseph Sullivan, the former CISO of Uber, guilty of obstructing a data breach investigation and of not reporting a crime related to the breach.[2]

SolarWinds and its CISO, Timothy Brown, face pending criminal prosecution for fraud and for internal control failures.[3] The government alleges Brown and SolarWinds misled investors by downplaying cyber risks despite knowing about a breach. SolarWinds claims the government is overstating the case and lacks the competence to regulate companies' cybersecurity.

During oral argument, the government admitted that SolarWinds' client had filed a suspicious activity report that cast doubt on SolarWinds's knowledge of a breach. The client revealed it had informed SolarWinds that it conducted an internal test, a simulated hack.[4]

Potential Evidentiary Problems in Prosecuting CISOs for Cybersecurity Failures

The SolarWinds case highlights the complex evidentiary challenges: proving inadequate security measures and the CISO's intent, knowledge, or negligence.

---

[1] Monica D. Cliatt is Of Counsel with Woods Rogers, PLC, focusing on white-collar defense, False Claims Act litigation, and investigation. Before working for Woods Rogers, Monica was a judicial law clerk in the Western District of Virginia, a First Assistant Federal Public Defender, and an adjunct law professor. As First Assistant, Monica handled many white-collar cases.

[2] U.S. Dep't of Justice Press Release, "Former Chief Security Officer of Uber Convicted of Federal Charges for Covering Up Data Breach Involving Millions of Uber User Records," (Oct. 5, 2022), https://www.justice.gov/usao-ndca/pr/former-chief-security-officer-uber-convicted-federal-charges-covering-data-breach (last visited on June 24, 2024).

[3] U.S. Securities and Exchange Commission Press Release, "SEC Charges Solar Winds and Chief Information Security Officer with Fraud, Internal Control Failures, (Oct. 20, 2023), https://www.sec.gov/news/press-release/2023-227 (last visited on June 24, 2024).

[4] Setting the Record Straight on the SEC and SUNBURST, (Nov. 8, 2023), https://orangematter.solarwinds.com/2023/11/08/setting-the-record-straight-on-the-sec-and-sunburst/ (last visited on June 24, 2024).

1. **Internal policies and industry standards:** The definition of "adequate" cybersecurity varies significantly across industries and has changed over time. A major trial issue will include whether a CISO's actions fell below accepted standards.

   Organizations have their own internal cybersecurity policies and guidelines. Discrepancies between internal policies and external legal requirements could complicate prosecutions. Cyber threats evolve rapidly. What law enforcement and the industry consider adequate security one moment could become obsolete quickly. Establishing a baseline regarding "adequate" security for when the breach occurred will be a complex task.

2. **Technical complexity:** Prosecutors, judges, and juries may struggle to grasp the nuances of highly technical systems and procedures. Cue the expert witnesses.

3. **Intent and knowledge:** Criminal charges usually require proving intent or knowledge. The government will need unambiguous evidence showing a CISO knowingly or intentionally misrepresented an organization's cybersecurity status, or willfully neglected their duties. A reasonable belief that cybersecurity measures were adequate, given the information and resources available, could justify their actions.

4. **Establishing causation:** Multiple factors contribute to cybersecurity incidents, such as relying on third-party vendors to provide cybersecurity. The government will need to delineate the CISO's responsibilities versus the external vendor's responsibilities. Then it must prove the CISOs actions or inactions were the direct cause of a breach.

5. **Documentation and records:** Proving a CISO misrepresented cybersecurity measures will require clear, unambiguous records. Organizations have different policies about retention and destruction of cybersecurity logs and communications, which could result in key evidence going missing and spoliation claims.

6. **Confidentiality and privilege:** Cybersecurity cases often involve sensitive and confidential information. Balancing the need for evidence with the protection of proprietary or classified information can restrict the availability of crucial evidence. Further, attorney-client privilege may shield communications between CISOs and legal counsel.

Will Prosecutors Charge More CISOs?

So far, there have been no high-profile criminal cases involving CISOs beyond Sullivan and Brown. Deputy Attorney General Lisa Monaco said Sullivan's prosecution should not alarm companies and their CISOs.[5] She urged continue cooperation with law enforcement, but indicted

[5] The Record, Jonathan Greig, "DOJ urges CISOs to continue working with law enforcement ahead of Uber security chief's sentencing, https://therecord.media/doj-lisa-monaco-urges-cisos-to-work-with-gov-uber-sentencing, (Apr. 25, 2023) (last visited June 24, 2024)

Brown and SolarWinds a few months later. With the rise in cybersecurity breaches and artificial intelligence, this space is one to watch.