

Corporate Cybersecurity Realism:

Managing Trade Secrets in a World Where Breaches Occur

By

John Villasenor

ABSTRACT

Cybersecurity intrusions aimed at extracting trade secrets are an unfortunate feature of the 21st century business landscape. In response, many companies have made cybersecurity a top priority, and their networks and systems have become much more secure as a result.

However, while improving security is a critical goal, it should not be the only goal. Companies also need to give attention to what might be called corporate cybersecurity elephant in the room: How does the inevitability that their networks will sometimes be compromised impact best practices for handling trade secrets *despite* those breaches? This paper aims to provide some answers to that question.

As discussed herein, companies should 1) “segment” not only their networks but also the trade secret information on those networks, thereby limiting the impact of any single cybersecurity breach, 2) avoid overreliance on NDAs, since over-disclosure can lead to increased exposure to cyber-enabled trade secret theft, 3) act more quickly on patentable inventions in light of recent changes to U.S. patent law that can increase the incentives driving trade secret theft, 4) ensure that cybersecurity considerations are be part of patent/trade secret decisions, and 5) be aware of—and, as appropriate, take advantage of—new changes to U.S. patent law the increase the potential benefits of early commercial use of trade secrets.