BRACEWELL

INSIGHTS

Cybersecurity and Infrastructure with Phil Bezanson and Seth DuCharme

September 28, 2021

*By: **Daniel J. Pope** and **Seth D. DuCharme***

On this episode of Environmental Law Monitor, host ***Daniel Pope*** is joined by guests Phil Bezanson and ***Seth DuCharme*** look at cyber attacks and cyber security.

Seth is a Bracewell partner and and draws on his experiences serving as the principal associate deputy attorney general of the United States and the acting US attorney for the Eastern District of New York to advise companies and individuals on a range of matters, including cyber security and breach response

Phil is the managing partner of Bracewell's Seattle office and co-host of Bracewell Sidebar. Phil regularly conducts internal investigations and defends corporations and executives facing allegations of fraud, product defect, antitrust violations, environmental crimes, bribery, insider trading, tax offenses and other allegations of business-related misconduct or regulatory violations.

What can you do on the front end to anticipate or prepare for certain kinds of disasters?
One of the things that has historically been common in most industrial segments of the business world is having things like incident simulation and tabletop exercises to plan for what happens if there's an oil spill or a similar incident. It's figuring out who's on the team, who needs to be communicating with whom, who are the real decision makers, and how do we anticipate for different things to go wrong.

The same concepts apply to a cyber attack. A virus has been detected on a server that deals with HR matters. What does that entail? What needs to be locked down? If we lock down this server, what are the ripple effects of other components of the company that may not function? After all, there's some component of the security server that's tied in with the HR server where the biometric information lives. Going through that kind of thing and just getting in your reps is like any other exercise or practice for competition or practice for an oral argument.

Who are the full range of stakeholders in investigations?
In the cyber security/government investigations world, the SEC puts out a very broad request for information. For instance, they are seeking information about the customers' interactions with SolarWinds, among other things, in response to the SolarWinds breach in December 2020, and that's a meaningful commercial consideration for SolarWinds. Now the SEC has reached out to thousands of other entities and asked about what kind of communications they had with SolarWinds around the time of the breach.

If you think about any organization that is subject to a cyber attack, typically the list of questions a business should consider include:

- Who in government can maybe help us with defeating or defending against the attack?
- Who in government are we legally required to notify, and when?
- Who else within the company are we legally required to notify, and when?
- Who are our commercial partners?
- Who are our customers?
- Who are the people whom we rely on for our business to make money?
- When do we reach out to them?
- How do we reach out to them?
- Do we do it the wait-and-see until we solve the problem?
- Do you do it right away and reach out with incomplete information?

These are all very different approaches depending on the circumstances, but some things merit a great deal of anticipation and discussion beforehand.

How do you respond to different types of attacks in ways that protect your company's operations, its data or other critical information?
One of the things that is super important right now for how people think about this and how they think about it going forward because we've moved past the period of time where the victim of a cyber attack can truly, fully and completely be an unaware victim and garner knee jerk sympathy. The world is much more sophisticated in assessing.

For any questions about cyber-attacks, please contact ***Daniel Pope***, ***Phil Bezanson*** or ***Seth DuCharme***.

The opinions expressed in this podcast are those of the speakers and do not necessarily reflect the viewpoint of their institutions or clients.