Published on *The National Law Review* https://www.natlawreview.com

Corporate Boards Mulling Effects of SEC Cyber Enforcement and CISO Exposure, and Possibly Hacker Complaints to SEC

Article By:

Joseph J. Lazzarotti

According to a New York Times story this weekend, the Security Exchange Commission's lawsuit against SolarWinds is driving discussions in boardrooms and corporate security departments of large organizations about the handling and reporting of cybersecurity breaches. It turns out that such boards and departments may not be the only ones following the SEC's increased focus on cybersecurity and data breaches.

Criminal threat actor group, BlackCat, reportedly posted on its dark web leak site that its latest cyberattack victim failed to comply with the soon to apply SEC four-day rule for reporting data breaches. As reported by databreaches.net, the hackers also filed a report with the SEC. How these developments will shape corporate disclosures, incident response planning, and reporting is unknown.

On the one hand, the New York Times article suggests, the use of boilerplate language by public companies to describe cybersecurity risks may be insufficient where the company is aware of more specific risks. On the other hand, more specific disclosures about potential risks could expose companies to increased attacks (yes, the bad guys do their research). And, there is some question about

whether a primary SEC objective would be served, namely whether the average investor would be able to grasp the impact of more granular reporting on the sheer number of vulnerabilities such organizations face.

Still others worry about a chilling effect. In the SEC's fraud case against SolarWinds, the agency named the company's CISO as well as the company. The NYT reminded readers that personal exposure for CISOs following a major data breach is not new. Whether these developments provide an incentive not to document vulnerabilities raises some concerns.

But there may not be a chilling effect at all. The potential for personal liability might push some CISOs to over disclose or at least diverge from the wishes of other executives to "paint a rosy or maybe rosier-than-aligned-with-reality picture."

Of course, these are the kinds of reactions that might be expected following the SEC's enforcement action – are our disclosures sufficient, we have to be careful about disclosing too much about our vulnerabilities, will the CISO share too much or not enough to avoid personal liability, etc. Reconciling these competing concerns will not be easy, particularly in the absence of clear agency guidance and the facts of a given situation. Further, they are concerns that should not be limited to public companies.

That challenge becomes intensely more complex when criminal threat actors unpredictably join the discussion. For anyone that has been through a significant security incident investigation, there are a myriad of decision points that have to be made along what often is a very short timeline. Each decision, particularly decisions dealing with communication and reporting, and even when well-intended, comes with multiple facets – report to whom, report when,

what must be communicated, it is accurate, it is complete, what if facts change, what will the effects be, etc.

Now knowing that threat actors may be bold enough to report to relevant government agencies may change the calculus of these deliberations.

Facing these issues for the first time when your organization has been compromised and criminal threat actors are demanding millions in ransom while reporting to your primary government regulator(s) is not a good business strategy. No incident response plan will be perfect or prepare the organization for every curveball that will be thrown in a data breach matter, but actively planning for these situations can help. This includes aligning with the organization’s CISO on existing systems vulnerabilities, how best to communicate about them, and addressing potential business and personal exposure in an increasingly complex regulatory environment.

National Law Review, Volumess XIII, Number 324