A $90 Million Loss Is A Bullet Dodged?

January 21, 2021

Business Bulletin

Many of our readers are aware that a recent hacking incident widely believed to have been perpetrated by Russian state-sponsored hackers against US IT management software company SolarWinds (NYSE:SWI), affected over 18,000 of their customers and had significant national security ramifications for both the United States and Great Britain.

However, it appears that the cyber insurance industry will have dodged a potential financial catastrophe from this event, even though claims are expected to be upwards of $100 million. Reports emerging from industry experts indicate that early observations are that the hackers appear to have used their access to review and collect sensitive data rather than to interrupt the business of affected companies or to destroy their networks through a process known as "bricking" as similar attacks sometimes do. While the data breach has enormous implications for national security and requires affected companies to undertake significant forensic analysis and possibly notification, which are largely covered by cyber insurance and expected to cost insurers over $90 million, those costs are typically very modest compared to those generated by business interruption or network damage claims covered by insurance but which are largely absent here. Another aspect to this attack which was fortunate for insurers is that an unusually high percentage – almost 20% - of affected customers were government agencies, who typically do not buy insurance for risks such as these.

OTHER KEY FINDINGS EMERGING IN THESE REPORTS INCLUDE:

- While 18,000 companies were affected by the backdoor exploit, only about 40 of those companies were actually targeted by the cyber attackers.
- 80% of the identified victims are located in the US, and the remaining 20% are from seven other countries including Canada, Mexico, Belgium, Spain, the United Kingdom, Israel, and the UAE.
- 44% of the initial list of organizations affected by the ongoing espionage campaign were from the information technology arena, the most widely impacted industry in this attack.

Simkiss & Block's Cyber practice group saw an immediate impact on renewals immediately when the breach was announced in December and continues to see questions from underwriters on almost every renewal, inquiring about whether the policyholder or any of its critical business partners used SolarWinds and may have been affected by the incident. Policyholders should be careful and considerate when responding to the underwriting questions to avoid creating a warranty like situation, or the imposition of broad exclusions, both of which dramatically impact the scope of coverage and both of which we are seeing insurers try to implement.

Simkiss & Block's Cyber practice leaders are available to counsel those who need more information about how their coverage might be impacted or how best to respond to underwriters on this fast-developing issue.