Cyberattacks on service providers pose a unique threat to firms

by Alicja Grzadkowska 25 Feb 2020

What do healthcare diagnostics company LabCorp, the State of Texas and 141 airline companies have in common? In 2019, they were all victims of cyberattacks that originated with a third-party service provider. In the case of Texas, hackers broke into information technology software managed by an outsourced company and used by many municipalities across the state and demanded $2.5 million to unlock the files.

Ransomware attacks originating with an IT vendor or managed service provider (MSP) are increasingly a source of concern, particularly for small and medium-sized businesses (SMBs).

“Managed service providers, software as a service (SaaS) companies, application service providers (ASPs) and anyone aggregating a large volume of client companies pose a unique cyber risk,” said Michael Palotay, chief underwriting officer for Tokio Marine HCC’s Cyber & Professional Lines Group. “If they are compromised with malware, they can quickly spread it to a large number of other entities.

”He added that Tokio Marine HCC has seen cyber insurance policyholders across industry classes experience ransomware attacks via trusted connections with their third-party service providers.
“We’ve also insured software as a service providers who have been infected and then spread the malware to their clients, and we’ve paid multiple ransoms for their clients to get their data unlocked,” explained Palotay. “It is another potential nexus for aggregation risk.

”The degree of disruption that ransomware incidents can cause is significant for SMBs. Oftentimes, even companies’ back-ups can be compromised by an infection, and it can take days, if not weeks, for a business to get back up and running. “If you’re a small business struggling to survive and you have a multi-day outage where you’re unable to service your customers, the cyberattack could become the extinction event for your business,” remarked Palotay.

Cyber insurance can help businesses get back on their feet following a cyber event. It does not, however, completely mitigate the impact of a cyberattack because there’s only so much that can be done in the event the insured gets infected.“We can prepare our policyholders, we can pay for experts, we can pay the ransom, but we can’t wave a magic wand and get them up and running instantaneously,” cautioned Palotay. “The impact of the attack may be across multiple systems, and in the event a third-party system is involved, it could be weeks before our insureds are back to business as usual.

”As a result, Tokio Marine HCC’s cyber team is encouraging insureds to implement proven preventative methods and procedures. Palotay recommends SMBs focus on having segregated data back-ups in place, such as cloud-based solutions that are separate from networks and won’t be encrypted if a network is hit with a virus. Other types of endpoint protection measures are also important, such as next generation antivirus tools that are more sophisticated than their predecessors, including those offered by CrowdStrike and Carbon Black.

“In addition, businesses of all sizes should have two-factor authentication activated for all of their connected applications, including G Suite and Microsoft Office 365,” added Palotay.

https://www.insurancebusinessmag.com/us/news/cyber/cyberattacks-on-service-providers-pose-a-unique-threat-to-firms-214831.aspx?fbclid=IwAR2JODVhmWuLPvbBx0hlkCkZRiIxQ5X46eQrAkOyqEewz4UPc5jVbxvZWO8