Cyber Liability Trends 2022

The past couple years have seen significant changes in the cyber liability landscape. While the regulatory landscape is always changing, COVID-19 altered the way many employees perform job functions. With the rise of a remote workforce, companies changed the way in which they operate. Not surprisingly, the move toward a remote work environment exposed companies to additional liability and risk from nefarious actors.

Last year saw a significant increase in cyber events, particularly ransomware and wire transfer fraud. Nefarious actors are aware home offices and personal devices are generally less secure than business environments, and they have deployed new attack strategies to cause greater disruptions and increase potential payouts. Wire transfer fraud schemes have become more sophisticated, attacks on large scale software providers like SolarWind have occurred, and ransomware attacks have become more prevalent and costly. Furthermore, ransomware attacks have expanded in scope, with some now targeting compromised companies along with the compromised companies' customers and business partners.

The insurance industry has noticed the significant uptick in cyber events along with an increase in related expenses. It is now common for the costs related to cyber events to reach six or seven figures, as expenses can include business interruption costs, attorney fees and those of experts brought in to handle the cyber event, fines and other civil penalties, and ransom payments. Moreover, common "war" exclusions have recently been interpreted to apply only to traditional forms of warfare, not cyberwarfare. Even if a "war" or "hostile act" exclusion is updated to include cyberwarfare, it can be difficult to determine the locations and affiliations of the nefarious actors in a cyber event, thus impossible to definitively prove whether a cyber event is excluded from coverage.

Accordingly, insurers have sought to balance the risks in their respective portfolios as cyber events and related expenses rise. Many insurers have significantly raised premiums associated with cyber insurance, increased deductibles and self-insured retention rates, lowered limits, altered coverages, and in more drastic situations, refused to issue coverage within a specific industry or geographic area. Insurers are also placing additional requirements on insureds to qualify for coverage. The requirements are not just limited to technical requirements, like the implementation of zero-trust solutions, but also include other requirements, like mandatory and regular employee cybersecurity awareness training.

Fortunately, there are some basic and effective steps a company can take to mitigate its cyber risk:

1) Address network security vulnerabilities, such as by disabling unused remote access tools and patching out-of-date software.
2) Implement zero trust solutions, such as multi-factor authentication.
3) Implement email security measures, such as email tagging.
4) Implement regular cybersecurity awareness training for employees.
5) Routinely test the integrity of data backups.
6) Implement payment processes with required two-party approval.

7) Draft, test, and implement cyber event response plans.
8) Implement vendor management systems that contractually obligate vendors to notify, cooperate, and assist in the event of a cyber security incident.

Disclaimer: *This material is provided for informational purposes only. It is not intended to constitute legal advice, nor does it create a client-lawyer relationship between Galloway and any recipient. Recipients should consult with counsel before taking any actions based on the information contained within this material. This material may be considered attorney advertising in some jurisdictions.*

Doris Bobadilla, Esq.
Offices: Mandeville, LA; New Orleans, LA; Gulfport, MS, Ft. Lauderdale, FL
dbobadilla@gallowaylawfirm.com | 985-674-6680

Mark Lehman, Esq.
Office: Tampa, FL
mlehman@gallowaylawfirm.com | 813-977-1200