

CyberSubroSM

As cyber risks have taken the world by storm, a tremendous amount of attention has been given to the proper methods for responding to inevitable data breaches and cyber-related losses. However, at Cozen O'Connor we recognize that cleaning up the mess is only part of the job, so we do not stop there. Our CyberSubroSM task force goes "beyond the breach" by investigating the cause of the cyber-related loss and pursuing responsible third parties for directly causing the loss or allowing it to happen on their watch. Potential targets can include a wide variety of entities including website or maintenance security vendors, network security designers, software/hardware manufacturers, data backup/cloud computing companies, as well as the hacked entity itself (including governmental entities).

The principles of property subrogation including early investigation, evidence preservation, expert analysis, and evaluation of industry standard breaches similarly apply to our CyberSubroSM investigations. After a cyber-related loss, we work with insurers and their insureds to evaluate how the breach occurred and what evidence — be it corrupt hard drives, forensic screen images, or anything in between — needs to be preserved. We assist in retaining the appropriate forensic expert to further evaluate how the breach occurred and identify the entities who caused, could have prevented or limited the consequences of, the security breach. This includes identifying and understanding any applicable standards in the software industry, such as PABP (Payment Application Best Practices) in the point of sale industry or determining if a reasonable level of security was provided, including encryption, passwords, firewalls, system upgrades, and intrusion detection/protection systems. Our litigation-experienced subrogation attorneys also understand the impact contractual limitations can have on CyberSubroSM recoveries and have navigated around these limitations.

Our recoveries in CyberSubroSM are not limited to carriers providing cyber-risk insurance policies. Property insurers also have instances of providing property coverage for cyber-related losses including replacement of computer and network equipment after a breach. We have handled recoveries against network security vendors for failing to adequately protect the insured's system that resulted in the breach (and subsequent property damage from the breach). Additionally, we have handled recoveries against the insured's vendors who installed programs on the insured's network that provided a portal for the hacker's access to the insured's network and private information.



David D. Brisco

Vice Chair, Subrogation & Recovery, West Region

dbrisco@cozen.com
Phone (619) 685-1704
Fax (619) 234-7831