



CYBER RISK CLAIM EXAMPLES

Are Your Clients Protected?

Businesses are at risk for computer attacks and network security liability claims. The same consequences of harmful cyber attacks that happened to these businesses, could happen to any modern business.

The “computer attack” was discovered by the insured while monitoring traffic on their network/firewall. Excessive traffic caused them to further investigate and during that investigation, they discovered that user accounts had been created on their servers and that files on one or more computers on their network were being actively deleted as they watched. The insured disconnected all of their systems from the internet at that time and corrected their systems. Costs associated with the claim: to recover data as well as the cost of hardware and software to correct the network.

Total Loss: \$80,264

An insured was a victim of a ransomware virus that propagated through the Insured’s network, infecting multiple PCs and servers. The insured engaged a local IT firm to assist with his systems restoration. The scope of the infection revealed it was less to replace computers and the server instead of deleting systems, reformatting the drives and rebuilding them from scratch or reimaging.

Total Loss: \$16,006

A transportation contractor was hacked by a former employee, whose passwords had not been changed upon termination. The insured’s computer system began to act erratically, crucial software programs were unavailable and large amounts of data appeared to have been deleted. An outside IT firm was hired to recover electronic data and input other records only available in paper form. In addition, the IT firm reinstalled software, re-configured the insured’s servers and repaired other damage to the insured’s computer system. The insured also had to replace various pieces of cargo tracking software that had been damaged or destroyed. Separately, the insured suffered business income losses over the course of several days while systems issues were being addressed. The insured also hired a public relations firm to help it communicate with its customers about the incident.

Total Loss: \$33,850

A retail business suffered a virus infection that corrupted data and caused the insured’s computer system to stop functioning properly, resulting in lost income. The insured hired an IT firm to remove the virus and reinstall software.

Total Loss: \$22,000



CLAIM EXAMPLES

The customers of an insured equipment dealer began to receive strange email messages that appeared to have come from the firm. The firm's owner called an outside IT consultant who investigated and confirmed the insured's computer had been infected with a virus. The virus was removed by the IT vendor. Several weeks later, the dealer received a certified letter from a local lawyer alleging that a former customer of the equipment dealer had been infected by a virus received in an email message sent by the dealer. According to the letter, the former customer had suffered a variety of different kinds of harm related to the virus and had incurred significant cost to have the virus removed.

Total Loss: \$48,200

The insured, an assisted living facility for the elderly, was notified that their servers were sending spam messages. A technician was dispatched and discovered a large amount of uploaded bandwidth being used by the server that controlled the phone systems. Since they were unable to discover how the server was being remotely accessed, they closed it to protect their information. The technician was able to restore the phone systems, however, due to extensive and ongoing issues, the insured decided to install a new phone system.

Total Loss: \$40,575; (Data Restoration for \$11,412, System Restoration for \$5,182, and Data Recreation for \$23,981)

The insured discovered he had a computer breach/attack. Someone infiltrated his system and gained access to his Merchant ID to use his identity and make fraudulent purchases on a regular basis. The insured tried to fix the problem on his own by wiping out the system, replacing the router and Point-of-Sales system. His attempts to fix the problem did not help. The issue remained. The insured then had to engage a third party vendor to replace the Point-of-Sales system which stopped the hacking and the fraudulent purchases.

Total Loss: \$23,894



Protecting your piece of the world

MMG Insurance Company | 44 Maysville Street | Presque Isle ME | 1-800-343-0533 www.mmgin.com