NAMICO
NAMIC INSURANCE COMPANY, INC.

INSURANCE COMPANY CYBER LIABILITY

Cyber Threats To Your Business

Cyber Crime Claim Scenario

The accounting department discovered a series of unusual wire transfer requests during a quarterly audit. After further investigation, it was determined the e-mail accounts of several executives had been compromised, and, as a result, several wire transfer requests had been sent to the accounting department by hackers using "spoof" email accounts. Over $600,000 in funds had been transferred to unknown bank accounts in four countries. Some of the funds stolen in the fraudulent wire transfer were reimbursed by the bank. Cyber crime liability insurance covered the amount not reimbursed by the bank.

PCI DSS Liability Claim Scenario

The credit card data of over 2,000 policyholders was exposed when it was discovered a company's system had been compromised. An investigation determined that customers' credit card data had been 'skimmed' off the compromised system by criminals to be sold on the black market, and the company failed to maintain the required data security controls under the Payment Card Industry Data Security Standard. The acquiring bank imposed fines and assessments in the amount of $380,000 against the company for failing to comply with the Payment Card Industry Data Security Standard. The fines and assessment were covered under the cyber liability insurance policy.

Privacy and Security Liability Claim Scenario

The Communications Act of 1934 was enacted to regulate and protect the collection of personally identifiable information. Two amendments to this law, the Telephone Consumer Protection Act of 1991 (TCPA) and the Junk Fax Prevention Act of 2005 (JFPA) were later passed to update this legislation for new and emerging technologies including limiting the use of automatic dialing systems, artificial or prerecorded voice messages, and unsolicited advertisements. The insured used software to fax authorizations. After an incorrect phone number was entered into the system, an individual with no prior relationship to the insured began receiving calls from the system. Despite the individual's requests for the calls to stop, he received 31 phone calls per day (1,200 per year) over the course of a four-year period and filed a suit against the network alleging violation of the TCPA. The case ultimately settled in favor of the individual for $1,190,000 with defense fees in excess of $200,000. The settlement and defense fees were covered by the cyber liability insurance policy.

Breach Event Costs Claim Scenario

A company received notice from IT security that the PII of 88 policyholders was found on the "Dark Web", which is used for illegal activity by criminals. Shortly after, the Insured received an anonymous email from a hacker calling himself "The Dark Overlord" claiming to be in possession of all the company's information and records. IT forensic consultants determined the PII was accessed by a hacker gaining access to an employee username and password. Breach Coach Counsel determined there was a high probability that all records were in fact obtained by "The Dark Overlord", requiring notification and credit monitoring to every policyholder, which totaled 544,000 individuals. A Public Relations Firm assisted the company in developing a crisis management plan to mitigate reputational harm resulting from the incident. The cyber liability insurance policy covered the IT expenses, Breach Coach Counsel, PR expenses, notification, and credit monitoring expenses, which totaled over $1,050,000.

Privacy Regulatory Defense and Penalties Claim Scenario

The laptop belonging to a claims employee of a company was stolen. The laptop, containing the electronic protected information of approximately 296,000 policyholders and claimants, was not encrypted. Names, dates of birth, addresses, social security numbers, diagnoses, and laboratory results were included in the protected information. Given the nature of the information stored and the fact that the laptop was not encrypted, the incident was determined to be a reportable breach under HIPAA and reported to the Department of Health and Human Services (DHHS) and the Office for Civil Rights (OCR). After an investigation, the OCR concluded the security policy did not comply with the HIPAA Secu-rity Rule as it was limited in scope, incomplete, and insufficient to address potential risks and vulnerabilities to the confidentiality, integrity, and availability of information held by the company. The OCR imposed civil fines and penalties. Counsel was ultimately successful in helping the insured achieve a settlement with the OCR, which reduced the fines and penalties and included a corrective action plan. The cyber liability insurance policy covered the legal expenses incurred in responding to the OCR's investigation and the OCR settlement, which totaled $1,600,000.

TPCA Claim Scenario

As part of its new mobile marketing campaign, text messages were sent to customers encouraging them to opt-in to its mobile offers. The texts were sent by using an "automatic telephone dialing system", which stored or produced telephone numbers using a random number generator. Several recipients filed a class action complaint alleging the text messages were unsolicited, unauthorized, an invasion of privacy, and illegal under the Telephone Consumer Protection Act ("TCPA"). The cyber liability insurance policy covered the defense costs incurred to defend the TCPA complaint, which totaled more than $25,000.

GET IN TOUCH:

3601 Vincennes Road, Indianapolis IN 46268 | 800.336.2642 | namicinsurance.com