CLAIM SCENARIO

BREACH OF CONTRACT / NEGLIGENCE LAWSUIT

Software Development Company

The following claims scenario is meant to illustrate a potential scenario you might encounter. It may not necessarily represent details of a specific claim.

SITUATION

A niche financial software company was hired to develop a customized inventory management system for a regional autoparts retail chain. The retailer alleged that the software system was delayed several weeks after the due date. Further, they claimed users encountered system glitches that hindered the use of the inventory management system. The software company countered that the client frequently changed the requirements of the project and intentionally withheld important information that, had it been known, could have prevented the system errors.

The autoparts chain sued the software company for breach of contract and negligence.

POTENTIAL IMPACT

INCIDENT RESPONSE	
Legal expenses	$ 44,350
Settlement costs	$ 276,000
REPUTATION MANAGEMENT COSTS Public relations fees to minimize reputational impact	$ 22,000
TOTAL	**$ 342,350**

RESOLUTION

The insurance company worked with client counsel to quickly settle the case for $276,000 allowing the software company to get back to business while not admitting any wrongdoing. The carrier covered the full cost of the settlement, media expenses, and legal fees.

CLAIM SCENARIO

CYBER BREACH

Data Storage Provider

The following claims scenario is meant to illustrate a potential scenario you might encounter. It may not necessarily represent details of a specific claim.

SITUATION

A data storage provider specializing in supporting e-commerce businesses experienced a cyber breach. Critical customer data was compromised.

The hacker group behind the attack demanded a ransom payment of $1.3M in Bitcoin, deliverable in 48 hours, to restore the data as well as prevent them from publicly releasing sensitive client information.

In addition to their damaged systems, the storage provider was faced with a large ransom payment, work stoppage, angry clients threatening to sue, and fines from regulatory bodies.

The company called their insurance company's cyber response team, who assigned a "breach coach," which is covered as part of the storage provider's Cyber/Technology E&O policy.

The breach coach worked on several fronts to minimize the damage and get the business back up and running.

POTENTIAL IMPACT

INCIDENT RESPONSE	
Forensic investigation costs to isolate vulnerability, analyze damage, ensure containment and calculate loss	**$ 41,000**
Notification costs	**$ 2,500**
Public relations fees to minimize reputational impact	**$ 19,000**
DATA RECOVERY Costs associated with intiating backups	**$ 7,500**
LEGAL FEES	
Legal expenses arising from regulatory investigation due to mismanagement of private information	**$ 33,500**
Legal expenses and settlement costs for claims	**$ 64,100**
REGULATORY Settlement fine	**$ 49,900**
Ransom payment	**$ 425,000**
TOTAL	**$ 642,500**

RESOLUTION

The breach coach assigned a forensic team to help restore systems. Simultaneously, they worked with the storage provider's counsel to settle any legal disputes with affected clients as well as work with state regulators to negotiate lower potential fines. The breach coach also secured a public relations agency to minimize the reputational damage to the company. At the same time, a claim was started to help with the legal and consulting fees, potential fines, and media costs.

Several clients expressed concern about their customer data being exposed despite the fact that backups were effective in restoring systems. The data storage provider and insurance company decided to pay the ransom. The breach coach initiated negotiations with the hackers, reducing the ransom payment to $425,000.

The insurance company then paid the ransom via their Bitcoin account. The proactive response and fast turnaround allowed the data storage provider to quickly resume operations.