PHILADELPHIA INSURANCE COMPANIES

A Member of the Tokio Marine Group

CLAIM SCENARIOS

CYBER SECURITY LIABILITY

The average cost of a data breach is $204 per lost record, with more than half of such costs attributable to lost customers and the associated public relations expenses to rebuild an organization's reputation. [1] The below examples illustrate situations in which the costs incurred to remediate a data breach were significant.

Unauthorized Access

An international computer hacking group gained access electronically to the computerized cash registers of a restaurant chain and stole credit card information of 5,000 customers, starting a flood of fraudulent purchases around the world.

Theft of Digital Assets

A regional retailer contracted with a third party service provider. A burglar stole two laptops of the service provider containing the data of over 800,000 clients of the retailer. Under applicable notification laws, the retailer – not the service provider – was required to notify affected individuals. Total expenses incurred for notification and crisis management to customers was nearly $5,000,000.

Privacy Breach

An employee of a rehabilitation center improperly disposed of 4,000 client records in violation of the center's privacy policy. The records contained social security numbers, credit and debit card account numbers, names, addresses, telephone numbers as well as sensitive medical information. The center settled the claim with the state of Massachusetts and agreed to pay fines and penalties imposed by the state as well as extend $890,000 in customer redress funds for credit monitoring on behalf of the victims.

Theft of Digital Assets

A home healthcare organization had backup tapes, laptops and disks containing social security numbers, clinical and demographic information, and in a small number of cases, patient financial data that was stolen. In total, over 365,000 patient records were exposed. The organization settled with the state attorney general, providing patients with free credit monitoring, credit restoration to patients that were victims of identity fraud, and reimbursement to patients for direct losses that resulted from the data breach. The organization was also required to revamp its security policies, implement technical safeguards and conduct random compliance audits.

Human Error

A non-profit community action corporation printed two 1099 forms on one piece of paper. An employee was supposed to separate the forms and send each to its rightful owner. Instead, one person received both copies. The mistake sent tax forms and social security numbers to strangers. Approximately 50% of the landlords who work with the community action corporation received their forms in addition to the private information of the others.

Cyber Extortion Threat

A U.S. based information technology company contracted with an overseas software vendor. The contracted vendor left universal "administrator" defaults installed on the company's server and a "Hacker for Hire" was paid $20,000 to exploit such vulnerability. The hacker advised if the requested payment was not made he would post the records of millions of registered users on a blog available for all to see. The extortion expenses and extortion monies are expected to exceed $2,000,000.

Human Error

An employee of a private high school mistakenly distributed via e-mail the names, social security numbers, birthdates and medical information of students and faculty creating a privacy breach. Overall, 1,250 individuals' information was compromised.

Malicious Code

A juvenile released a computer worm directing infected computers to launch a denial of service attack against a regional computer consulting & application outsourcing firm. The infection caused an 18 hour shutdown of the entity's computer systems. The computer consulting & application outsourcing firm incurred extensive costs and expenses to repair and restore their system as well as business interruption expenses which totaled approximately $875,000.

[1] Ponemon Institute, 4/2009 Global Cost of a Data Breach Study.