Cyber Risks and their Impact

Businesses of all sizes are vulnerable to cyber losses from some form of information technology failure, whether by malfunction, human error or breach – often with catastrophic results. An unauthorized intrusion could rob your business of assets, damage its reputation and prevent it from operating. And while attacks on large corporations gain most media coverage of cyber risk, small and medium-sized businesses are more vulnerable, with fewer resources to prevent and recover from security failures.

Because traditional property, personal and general liability policies don't cover many of the losses caused by cyber exposures, insurance companies have developed new products to address businesses' increased risks. As an independent advisor, Alera Group can design an insurance program that best serves your business needs. Program options include:

FIRST-PARTY COVERAGES

Loss of Digital Assets
Reimbursement for loss resulting from damage to or corruption of your electronic data and computer programs.

Cyber Business Interruption and Extra Expense
Income reimbursement during the period of restoration of your computer system or website.

Security Event Costs
Reimbursement for cost of customer notification, regulatory fines and penalties, and public relations expenses.

Cyber Extortion Threat
Reimbursement for extortion expenses resulting directly from a credible threat to your computer system.

Cyber Terrorism
Reimbursement for income loss, interruption and special expenses directly as a result of an interruption or failure of your computer system caused by an act of terrorism.

Cyber Crime
Protection from e-theft exposures such as:

- **Funds Transfer Fraud:** wrongful transfer of funds by a third party from your account at a financial institution.
- **Computer Fraud:** use of a computer to fraudulently transfer your property from inside an insured premises or bank to a person or place outside the insured or bank's premises.
- **Social Engineering Fraud:** use of human interaction to influence someone into acting inappropriately, often by breaking normal security procedures.

THIRD-PARTY COVERAGES

Data Breach
Includes claims arising from unauthorized access to or dissemination of private information, including credit card numbers.

Network Security/Privacy Liability
Legal Liability for a security breach or privacy breach resulting from alleged violations of HIPAA and other privacy protection laws or regulations (state, federal or foreign).

Employee Privacy Liability
Legal liability for a security breach or privacy breach of employees' personally identifiable information or protected health information.

Electronic Media Liability
Claims arising from the following on your internet or intranet site:

- Defamation, libel or slander.
- Invasion of an individual's right of privacy.
- Plagiarism or misappropriation of ideas under an implied contract.
- Infringement of any copyright, trademark, title or service mark.

ALERAGROUP

CYBER RISK CLAIM SCENARIOS

Actual and potential claims resulting from cyber risk exposures

Loss of Digital Assets

A regional retailer contracted with a third-party service provider. A burglar stole two laptops from the provider containing the data of more than 800,000 of the retailer's clients. Under applicable notification laws, the retailer was required to notify affected individuals. Total expenses incurred for notification and crisis management to customers was nearly $5 million.[1]

Cyber Business Interruption

A computer worm directing infected computers to launch a denial of service attack against a regional computer consulting and application outsourcing firm caused an 18-hour shutdown of the entity's computer systems. In addition to extensive costs and expenses for repairing and restoring its system, the firm incurred business interruption expenses totaling approximately $875,000.[1]

Security Event Costs

An employee of a rehabilitation center improperly disposed of 4,000 client records in violation of the center's privacy policy. The center settled the claim with the Commonwealth of Massachusetts, agreeing to pay fines and penalties. It also extended $890,000 in customer redress funds for credit monitoring on behalf of the victims.[1]

Cyber Extortion Threat

An overseas vendor contracted by a U.S. IT company left universal administrator defaults installed on the company's server and paid a "hacker for hire" $20,000 to exploit the vulnerability. The hacker threated to post the records of millions of registered users on a blog available for all to see. The extortion payment and additional expenses were expected to exceed $2 million.[1]

Funds Transfer Fraud

An insured received an email that appeared to be from its bank but was not. The insured's employee opened the email, which activated a Trojan horse computer virus that read key strokes from the employee's computer. The perpetrator used this means to obtain banking and password information and initiate a fraudulent electronic wire transfer from the insured's bank account.[2]

Computer Fraud

An organized crime ring gains unauthorized access to the insured's accounts payable in its computer system and alters the bank routing information on outgoing payments. The result: $1 million transferred to the crime ring's account.[2]

Social Engineering Fraud

The controller for a distributor of component parts was responsible for making regular payments to overseas vendors. After months of working with a particular vendor and receiving regular shipments, the controller received an email that appeared to come from his vendor contact, indicating that the vendor's bank was having issues with accepting payments and asking if the next payment could be made to a new bank. Verification was a challenge. After the supposed vendor applied some pressure, the controller paid the invoice via wire transfer. When the real vendor realized payment was overdue, the fraud was revealed. The fraudster absconded with the almost $250,000 payment.[3]

Data Breach

A restaurant's point-of-sale machines are illegally skimmed with a hidden electronic device for eight months, affecting 1,000 cards. Some cardholders become identity-theft victims and pay for their own credit monitoring. Others are unable to recover funds stolen from their bank accounts because too much time has passed before they discover the fraudulent activity. Victims unite and sue the restaurant for costs incurred.[4]

Network Security/Privacy Liability

An employee's company laptop is stolen from his home. The laptop contains private financial information of some of your customers, who sue you for damages resulting from your failure to protect their private financial information.[2]

Employee Privacy Liability

An employee of a private high school mistakenly distributes 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 is compromised.[1]

Electronic Media Liability

You place advertisements on your website and in your direct mailings to announce a new service offered by one of your partners. The advertising contains material that your partner's competitor claims it owns. The competitor sues you, contending you are liable for damages caused by unauthorized use of the advertising material.[2]

1 Source: Philadelphia Insurance Companies
2 Source: The Travelers Insurance Companies
3 Source: Chubb Insurance
4 Source: United States Liability Insurance Group (USLI)

Published August 2020.

ALERAGROUP