The Cincinnati Insurance Company

Business Insurance

LOSS SCENARIO EXAMPLES

Cyber Risk Protection

Data breaches and computer attacks pose a growing threat to businesses of all sizes. These examples illustrate that commercial clients of all sizes and types of business can benefit from Cincinnati's cyber risk protection. The scenarios summarized here are based on actual claims and are provided with permission by a specialty vendor serving as a resource for Cincinnati.

COMPUTER ATTACK

1. Computer attack and network security liability – equipment dealer

Scenario: An insured equipment dealer's customers began to receive unusual email that appeared to be sent by the dealer. When a customer contacted the dealer with a question about the message, the business owner grew suspicious and engaged an outside IT consultant to investigate the cause and fix the problem.

First-party results: The consultant discovered a virus on the dealer's system and removed it, but the problem didn't end there. The policy paid for the system restoration costs to remove the virus.

Third-party results: Several weeks later, the dealer received a certified letter from a local lawyer alleging that a former customer's computer had been infected by a virus received in an email message sent from the dealer. According to the letter, the former customer suffered harm related to the virus and incurred significant cost to have it removed. The equipment dealer engaged an attorney and the policy paid the attorney's fees.

Total covered loss for first- and third-party exposure: $48,100

2. Computer attack – transportation company

Scenario: An insured transportation company discovered it had been hacked when its computer system began to act erratically. Core software programs suddenly became unavailable and large amounts of data were deleted. An investigation determined that a former employee gained unauthorized system access using passwords that had never been reset after the person left the company.

Results: The insured company hired an external IT contractor to:

- recover and replace lost data
- replace and restore software
- reconfigure servers and repair other system damage caused during the attack

In addition, the insured incurred expenses related to:

- loss of business income during the time system restoration took place
- retention of a public relations firm to manage customer communications about the attack

Total covered loss for first-party exposure: $33,850

For information, coverage availability in your state, quotes or policy service, please contact your local independent agent recommending coverage.

WAGNER GIBLIN INSURANCE

THE CINCINNATI INSURANCE COMPANIES

Everything Insurance Should Be®

3. Computer attack – retail business

Scenario: An insured retailer lost business income because a virus attacked its computer system causing data corruption and system failure.

Results: The insured retained an external IT resource to remove the virus, remove the infected system software and reinstall uninfected software.

Total covered loss for first-party exposure: $22,000

4. Computer attack – manufacturing business

Scenario: An insured manufacturing business experienced both an unplanned increase in system activity and unscheduled file removal from their network. The business disconnected from the internet and contacted an external IT resource for help. A hacker took over the company's main email servers and used them as spam servers. In addition, the IT contractor discovered that several of the insured's workstations were infected with malware.

Results: The insured hired an outside IT resource to find and remove the malware. Related expenses may be covered, subject to the deductible and limit of insurance, under the computer attack coverage of Cincinnati Network Defender™ or Cincinnati Cyber Defense™.

5. Computer attack – legal firm

Scenario: An employee of an insured legal firm opened a resume that was attached to an email. Opening the document launched hidden malware that encrypted the data on the employee's company computer and on a shared network drive.

Results: The firm engaged an outside IT company to find the problem, remove the malware and restore the computer and the network. Related expenses may be covered, subject to the deductible and limit of insurance, under the computer attack coverage of Network Defender or Cyber Defense.

6. Computer attack & network security liability – business office

Scenario: An employee at an insured business clicked a link in an email that appeared to come from a known contact. Unfortunately, clicking through to the site launched hidden spyware that replicated onto the company's file server.

Results: Someone exploited that spyware to hack into the insured's system, gain access to private client information and then post some of it on a public website. The client whose information was compromised sued the insured for breach of private business information. The defense of this claim may be covered, subject to the deductible and limit of insurance, under the network security liability coverage of Network Defender or Cyber Defense.

DATA BREACH

1. Data breach – apartment building

Scenario: A burglar stole a box of applications from the rental office of an insured apartment building. The completed applications provided the burglar with personal information, including Social Security numbers, for more than 2,500 people.

Results: The apartment manager paid for help sending notification letters to the affected applicants and provided services to assist in the event of identity theft resulting from the data breach.

Total covered loss for notification and service cost: $90,500

2. Data breach – financial

Scenario: An employee at an insured financial services company installed software to simplify file sharing on a company computer. However, a hacker used that software to gain access to the company's computer system and steal the private data of 2,000 clients.

Results: The financial services company paid to mail notification letters and arranged to provide identity recovery services to the 2,000 individuals who were affected by the data breach.

Total covered loss for notification and service cost: $70,000

3. Data breach – accounting firm

Scenario: Someone stole a computer containing tax records of 800 clients from an insured accounting firm's office. The clients were located in a four-state area.

Results: The insured hired legal counsel to make sure the firm fulfilled each state's specific breach notification requirements. Affected clients were notified of the theft and advised to get in touch with their banks to place fraud alerts in case of identity theft resulting from the data breach.

Total covered loss for legal review, notification and service cost: $28,000

4. Data breach – convenience store

Scenario: A thief attached a card skimmer to a gas pump and stole debit card and PIN data from 550 customers of an insured convenience store. Using the stolen numbers, the thief fabricated and used counterfeit debit cards to withdraw funds from the customers' accounts via ATMs.

Results: The gas station's owner arranged to mail notification letters and provide services to assist individuals affected by the data breach.

Total covered loss for notification and service cost: $19,250

5. Data breach – doctor's office

Scenario: A burglar stole external data backup media storing patients' personal data from an insured doctor's office.

Results: The doctor paid for assistance sending letters to the patients involved to notify them of the theft and recommend that they set up fraud alerts with credit bureaus and monitor their bank accounts and credit reports.

Total covered loss for notification and service cost: $10,500

IDENTITY RECOVERY

1. Identity recovery – dentist

Scenario: An insured dentist received a summons to appear in court for a case about dental equipment collection and repossession.
Results: An investigator determined that a former employer fraudulently used the insured's personal information to acquire the equipment using personal data without the insured knowing about or giving permission for the acquisition.
Total covered loss for attorney fees: $10,400

2. Identity recovery - business owner

Scenario: A criminal used an insured business owner's personally identifiable information to open fraudulent accounts at four major chain retail stores in the insured's name. The insured was alerted to the identity theft and filed a claim when a representative from one of the stores called with questions about the unauthorized credit application submitted to that store.
Results: The adjuster assigned to the claim referred the insured to a licensed case manager who coordinated these identity recovery actions on behalf of the insured:

- Issued fraud alerts on the insured's credit file with the three main credit reporting agencies to limit further unauthorized activity
- Worked with each of the lenders involved to document and dispute the unauthorized accounts
- Provided a final credit report after working with the lenders to verify that the fraudulent activities had been removed and the insured's credit history was restored to the pre-theft ratings
- Prevented the insured from having to pay any damages due to rapid and thorough response to the identity theft

3. Identity recovery – medical professional

Scenario: A criminal used stolen personal information to open unauthorized accounts in an insured doctor's name, and then used those funds to open lines of credit and pay some rental expenses.
Results: The insured engaged a case manager to place fraud alerts and hired a lawyer to address the fraudulent accounts and help resolve some of the identity theft-related issues.
Total covered loss for attorney fees: $5,600

4. Identity recovery – business owner

Scenario: Someone used an insured business owner's Social Security number without permission to open a bank account.
Results: The business owner hired a lawyer to work with the bank to resolve the issue.
Total covered loss for attorney fees: $1,000

5. Identity recovery – business executive

Scenario: An unauthorized person tried unsuccessfully to open a bank account and gain access to an insured business executive's established line of credit. The thief used personal information without the insured's knowledge or permission.
Results: The business executive lost time away from the job working with a case manager to dispute the fraudulent activity that appeared on the insured's credit history.
Total covered cost of lost wages: $865

6. Identity recovery – business owner

Scenario: An insured business owner applied to refinance a loan but was surprised when it was denied due to a bad credit report showing a fraudulent mortgage taken out using the insured's personal information.
Results: The case manager coordinated placement of fraud alerts on behalf of the insured, who had to pay the reapplication fees to refinance the valid mortgage.
Total covered cost of reapplication fee: $700

7. Identity recovery – business owner

Scenario: An insured business owner's tax return was rejected by the Internal Revenue Service because records showed that a tax return had already been filed in the name of the insured's young child using the same taxpayer identification number.
Results: The insured notified the police, and worked with a case manager to file a physical copy of the valid tax return with the IRS, set fraud alerts with credit bureaus, and contacted the Social Security Administration to make sure that both individuals' Social Security numbers had no other unauthorized activity associated with them. These services do not erode the identity recovery limit of insurance for other expenses—such as lost wages or lawyer's fees—that may be incurred when responding to legal demands for payment of fraudulently incurred debts.

These actual claims and examples are for educational purposes only. Every claim is adjusted according to its own specific set of facts. Whether or not insurance coverage would apply to any claim is dependent on the facts and circumstances of each individual claim and the language of the insurance policy.