Manufacturing, Cyberattacks and Business Interruption

Quiz: Test Your Insurance Knowledge

Read the scenarios below, then consider what type of insurance policy is most likely to apply. Our answers appear at the end of the quiz. Talk to your broker or other trusted adviser about scenarios that could apply to your operations.

1. A cyberattack impairs your ability to ship product to a client that is responsible for 50 percent of your annual sales. The policy most likely to apply to your lost sales is:

A. Cyber Business Interruption and Extra Expense
B. Cyber Contingent Business Interruption
C. Cyber Reputational Harm
D. Errors and Omissions

2. Cyber tampering causes a manufacturing defect in a critical part that you ship to a customer. As a result, the customer suffers $2 million in financial harm due to lost production and sues for damages. The policy most likely to apply to the cost of the recall and replacement is:

A. Cyber Business Interruption and Extra Expenses
B. Cyber Contingent Business Interruption
C. Cyber Reputational Harm
D. Errors and Omissions

3. A critical supplier stops shipments, stating that your company has not paid recent invoices. You lose sales as a result. An investigation determines that a cybercriminal sent an email from the supplier's system to your accounts payable department, changing the payment instructions. Your company has paid according to the new instructions you were given. The policies most likely to apply to the (1) fraudulent payment and (2) lost sales respectively are:

A. (1) Cyber Business Interruption and (2) Extra Expense and Property
B. (1) Not Covered and (2) Cyber Business Interruption
C. (1) Crime with Social Engineering and (2) Not Covered
D. (1) Cyber Liability and (2) Cyber Business Interruption and Extra Expense

4. A cyberattack shuts down your network, impairing your ability to ship product to a client that you are contractually obligated to provide product to each month. Your company incurs $1 million in expenses executing your IT breach response plan and business continuity plan. The policy most likely to apply is:

A. Cyber Business Interruption
B. Cyber Contingent Business Interruption
C. Cyber Extra Expense
D. Errors and Omissions

5. A storm damages the computer controllers on a critical piece of production equipment, halting production and forcing you to outsource the work until your equipment can be fixed. The policy most likely to apply to the cost of fixing your equipment is:

A. Cyber Business Interruption and Extra Expense
B. Cyber Contingent Business Interruption
C. Cyber Reputational Harm
D. Property

6. A storm damages the computer controllers on a critical piece of production equipment, halting production and forcing you to outsource the work until your equipment can be fixed. The policy most likely to apply to the added cost of purchasing extra production capacity is:

A. Cyber Business Interruption
B. Business Interruption
C. Cyber Extra Expense
D. Business Extra Expense

7. A hacker disables the brakes on a vehicle you manufacture, and the owner/driver is injured when he collides with a parked car because he cannot stop. He files a claim for injuries against your company. The policy most likely to apply to this claim is:

A. Cyber Liability
B. Cyber Business Interruption and Extra Expense
C. Casualty
D. Cyber Contingent Business Interruption

8. A computer virus causes machinery on one of your production lines to run until it overheats and becomes severely damaged. Worse, the virus spreads through your network and infects machinery at one of your vendor's locations, causing the same type of damage. The vendor files a claim against your company. The policy most likely to apply to this claim is:

A. Cyber Liability
B. Cyber Business Interruption and Extra Expense
C. Cyber Contingent Business Interruption
D. Errors and Omissions

9. An employee receives what appears to be a routine email from your company's philanthropist president, requesting that a $75,000 wire transfer be made. Later it is discovered that the president made no such request, and the money is gone. The policy most likely to apply to this loss is:

A. Cyber Reputational Harm
B. Crime with Social Engineering
C. Cyber Contingent Business Interruption
D. Directors and Officers

10. A hacker changes settings slightly on your equipment, which results in you shipping out-of-tolerance parts to your client. Your client discovers the problem when he gets a call about thousands of subassemblies that are going to be returned to him. He files a claim against your company. The policy most likely to apply to this loss is:

A. Cyber Business Interruption and Extra Expense
B. Cyber Contingent Business Interruption
C. Cyber Reputational Harm
D. Errors and Omissions

Bonus Question

Your contract logistics freight forwarder's network becomes infected by malware, causing a two-week delay in product reaching your stores. You lose $1 million in sales as a result. The policy most likely to apply is:

A. Cyber Reputational Harm
B. Cyber Business Interruption and Extra Expense
C. Cyber Contingent Business Interruption
D. Errors and Omissions

This information does not constitute advice. Every business and every insurance policy and carrier are different. Always contact your insurance broker or trusted adviser for insurance-related questions.

Answers

1-A; 2-D; 3-C; 4-C; 5-D; 6-D; 7-C; 8-A; 9-B; 10-D; Bonus-C