Cyber Claims Scenarios for Retail/E-Commerce

Point of Sale Breach

A local clothing boutique suffers a security breach that allowed a threat actor to download malware that collected customer payment information during transactions. The payment processor identified the unusual activity and, following an investigation confirming the breach, assessed fines against the boutique.

The clothing boutique's cyber insurance policy gave them access to:

- A computer security expert to determine how the breach occurred, and to advise the clothing boutique of their payment card (PCI-DSS) security obligations; and
- Funds to cover the fines assessed by the payment processor.

Cyber Deception

The finance department of a small software development company received a payment request by email for their quarterly purchase of company laptops. The email claimed that payment was overdue and failure to pay immediately would result in repossession of the laptops. This email was not sent by the laptop manufacturer, but by a bad actor who knows the software company's purchasing habits. The finance department immediately transferred funds to the ACH provided in the email.

- Provided that the restaurant followed proper verification procedures, their cyber insurance policy could reimburse the firm for the transferred payment.

Ransomware

An independent museum experienced a ransomware event that decrypted its computer systems. The gift shop was affected, along with payroll data. The museum received a message from a threat actor demanding a large sum of money to unlock the computers.

The museum's cyber insurance policy gave them access to

- A digital forensics firm to assist in the recovery of their data from non-impacted backups.
- Privacy counsel to assist in preparing regulatory notices and coordinating credit monitoring for employees whose Social Security numbers were exposed; and no ransom demand was paid because the museum could make a full recovery.