CHUBB®

Cyber InFocus

Fourth Quarter, 2018

Bringing cyber risks to life

The holidays are a joyous time, filled with increased sales for many retailers. But for a growing number of retailers, it's also a time of increased losses suffered at the hands of cyber criminals. In fact, we typically see a 35% increase in the number of cyber claims across all types and sizes of retail businesses this time of year.[1] The good news is, by understanding recent trends and educating our insureds about how to protect their businesses, we can help reduce their exposure to loss, not only during the holidays– but every day.

Visit the Chubb Cyber Index to learn about data-driven cyber trends.

> "Every cyber incident is different. Ensuring Chubb clients understand that, and are prepared for the disruption, reduces the total impact of any incident."
>
> **Matt Prevost**
> SVP, Chubb
> *Financial Lines*

Retail Cyber Trends

New technologies continue to have a tremendous impact on how, when, and where people make purchases, but they also open businesses up to vulnerabilities that leave them susceptible to a variety of cyber attacks and privacy-related claims. While the specific types of these cyber attacks are constantly evolving, three that can be especially problematic for retailers during this holiday season are children's information collection, DDoS attack, and credit card breach.

Retail Cyber Claims account for

8%

of all industry claims across North America.[1]

During the holiday season, we see a

35%

increase in Retail Cyber claims.[1]

Online Businesses Are Paying Hefty Fines for Collecting Children's Information

What it is

The Children's Online Privacy Protection Act (COPPA) was enacted by Congress in 1998 and is enforced by the Federal Trade Commission (FTC). It was designed to protect children aged 13 and under from having their personal information collected and disclosed in connection with websites, apps, online games, e-commerce shopping, and other online services. Its mission is to ensure that parents are in control of any information that is collected from their children.[2]

How it works

1. Businesses that provide websites, apps, online shopping, and other services that interact with children online are required to provide a privacy policy that includes parental consent.
2. Parents must affirmatively "opt-in" in order for their children's information to be collected.
3. Parents, or anyone who believes an operator is violating COPPA, may submit a complaint to the FTC.
4. If a business does not comply with COPPA, the FTC can enforce fines of more than $40,000 per violation.

Trend

Over the past several years, the FTC has imposed some very significant civil penalties against companies that did not comply with COPPA when marketing online to children.

Chubb Insight

Given the large amount of online content that is marketed toward children and recent crackdowns on noncompliance, it's more important than ever that we help our clients fully understand and comply with the provisions of COPPA.

To learn more about cyber risks facing the retail industry, please review our recent Webinar and Blog Post - both found on www.chubb.com/cyber

DDoS Attacks Continue to Flood Systems, Taking More Business Offline

What it is

A Distributed Denial of Service (DDoS) attack occurs when a victim's computer system is overwhelmed by bogus internet traffic. The attack disables the computer system and prevents it from conducting normal operations as its network is overwhelmed by the attack.

How it works

1. Multiple computer systems and machines that are infected with malware (sometimes called "bots") send internet traffic to the victim's system.
2. The system is then flooded–preventing normal business traffic from getting through to its legitimate destination.
3. Because the attack is coming from a number of different sources, it's very difficult to control or shut it down.

Trend

We have recently seen DDoS attacks affect many different types of businesses–including banks, news websites, and online retailers–with the objective of taking them offline.

Chubb Insight

Our panel of forensic firms have experience in handling DDoS attacks. In addition to providing first-party coverage for the incident response, our cyber policies are designed to cover business interruption losses that may occur if an insured's system is brought down by a DDoS attack.

Credit Card Breaches on the Rise as Email Phishing Attacks Increase

What it is

This type of cyber attack is a double threat. Criminals may obtain credit card account numbers through compromised point-of-sales (POS) systems or in stores through stored credit card data on servers. They then use the credit card information to make purchases, but it's usually the retailers who are left holding the bag. In addition to investigative charges, legal fees, and public relations costs, a retailer may also have to pay the credit card brand's costs to replace the stolen credit cards and could be subject to class-action lawsuits and regulatory inquiries.

On average, retailers pay

$3-$5

per credit card replacement.[1]

How it works

1. A cybercriminal sends an email containing a malicious link.
2. Once the link is clicked, malware (malicious software) is installed on a computer system and routed to a server where credit card information is processed.
3. The cybercriminal is able to collect consumer credit card data and use it to make fraudulent purchases.

Trend

Historically, cyber criminals have used credit card readers and malicious code on POS systems to obtain customer credit card data. However, with the recent rise in social-based claims, we have seen a direct increase in the amount of card data that is compromised through email phishing attacks that place malware on computer systems.

Chubb Insight

Comprehensive employee training on how to identify suspicious emails can help prevent these types of credit card breaches. In addition, a retailer should ensure that its cyber insurance policies contain not only first-party coverage to respond to a credit card breach, but also coverage for card brand-issued assessments that may arise. Retailers who intend to accept credit card payments, and store, process, and transmit cardholder data, need to make sure their data storage facility is PCI compliant and that they meet all the requirements of the Payment Card Industry Data Security Standard (PCI DSS).

Chubb. Insured.℠

[1] SOURCE: Chubb Claims Data, Q3 2018
[2] SOURCE: https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#COPPA%20Enforcement

Form: 30-01-0082 (918)