Cyber Risks are a Reality in the Retail/Hospitality Industry

Some of the biggest cyber attacks in history have happened to major brick-and-mortar stores, online retailers, and hospitality organizations. It makes sense—these types of organizations maintain a large amount of personal data and records, including credit card numbers, social security information, financial records, travel patterns, and other types of sensitive information, so they are more susceptible to theft. The responsibility of holding this type of sensitive information makes it essential for these types of organizations to understand the importance of cyber security and privacy—particularly as we approach the holiday shopping and travel season.

But where do the greatest risks lie?

According to data from the Chubb Cyber Index℠, hacking and phishing attacks topped the list of risks retailers and hospitality organizations faced in 2018. Phishing attacks occur when internal employees click on malware. With a greater number of part-time employees working during the holiday shopping season, the risk for human error increases. Hackers will prey on companies when they are most vulnerable to maximize their potential return. Both of these types of attacks can often be prevented with proper education and strong password hygiene.

Cyber risk for Retail/Hospitality industry continues to evolve with a high risk for hacking, often via a phishing attempt:

2016 Top Actions for Retail/Hospitality:
- Malware (13%)
- Theft/Tampering (24%)
- Hacks (27%)

2017 Top Actions for Retail/Hospitality:
- Malware (19%)
- Privacy Violations (21%)
- Phishing (17%)

2018 Top Risks for Retail/Hospitality:
- Hacks (20%)
- Human Error (18%)

Fast Facts

More than 57% of the cyber incidents reported to Chubb by the retail/hospitality industry were caused by someone inside the organization. And an additional 12% of the incidents were caused by an industry partner. These actions compromised servers 28% of the time and people 30% of the time.

Caused by someone inside the organization: 57%

Caused by an industry partner: 12%

*Data from the Chubb Cyber Index℠
1. **Ransomware attack cripples systems**

An Insured that sells retail goods was struck with a virulent strain of ransomware that encrypted its data, crippled its systems, and demanded $25,000 in Bitcoin. After consulting with their Chubb cyber claims representative, as well as an incident response coach and forensic expert from Chubb’s cyber panel, the Insured decided to pay the ransom. The Insured received a decryption key that permitted access to the once-encrypted data. A forensic accountant was also retained from the Chubb cyber panel and assisted in the calculation of the Insured’s business interruption (BI) loss. After comparing the Insured’s sales from the time of the attack to records of previous sales, Chubb paid a BI loss of more than $200,000.

2. **DDoS attack halts business**

An Insured was the victim of a denial of service (DDoS) attack from an unknown source. The attack caused a 22-hour outage to the company’s website and a continued degradation of service for an additional 4 days. The incident resulted in the company’s inability to sell subscriptions to customers through its website. This event resulted in approximately $750,000 in business interruption losses, and an additional $40,000 was spent on forensic accounting services.

3. **Incident response team lessons the impact**

A retail chain in Canada suffered a ransomware attack which infiltrated its servers, computer systems, cash registers, online store, and website. The retail chain retained Chubb-preferred vendors to mitigate the incident, including a cyber incident response coach and a forensic investigator. As a result of the attack, approximately $1M in mitigation expenses and $100,000 in business interruption costs were paid.

---

**Claim Scenarios:**

1. **Employee Education**
   - Identify potential cyber threats
   - Protect sensitive data
   - Escalate issues to the right people

2. **Strong Password Hygiene**
   - Improve cyber security by making it easier to create stronger passwords
   - Automatically log into websites by eliminating manual password entries
   - Change multiple passwords with the click of a button

---

**Services to Help Mitigate Cyber Risk:**

**Employee Education**
- Identify potential cyber threats
- Protect sensitive data
- Escalate issues to the right people

**Strong Password Hygiene**
- Improve cyber security by making it easier to create stronger passwords
- Automatically log into websites by eliminating manual password entries
- Change multiple passwords with the click of a button

---

**Limit your risks now by taking advantage of the services made available to Chubb Cyber policyholders**

*SOURCE: The Chubb Cyber Index (June 2019)​

The claim scenarios described here are intended to show the types of situations that may result in claims. These scenarios should not be compared to any other claim. Whether or to what extent a particular loss is covered depends on the facts and circumstances of the loss, the terms and conditions of the policy as issued and applicable law. Facts may have been changed to protect privacy of the parties involved.

Chubb is the marketing name used to refer to subsidiaries of Chubb Limited providing insurance and related services. For a list of these subsidiaries, please visit our website at www.chubb.com. In the United States, insurance is provided by ACE American Insurance Company and its U.S. based Chubb underwriting company affiliates. All products may not be available in all states. This communication contains product summaries only. Coverage is subject to the language of the policies as actually issued. Surplus lines insurance is sold only through licensed surplus lines producers. Chubb Limited, the parent company of Chubb, is listed on the New York Stock Exchange (NYSE: CB) and is a component of the S&P 500 index.

© 2019 Form: 17-01-0245 (10/19)