CHUBB®

Cyber InFocus

Second Quarter, 2018

Keeping you one step ahead of the trends

Social-based cyber claims, such as business email compromise attacks as well as Bit Paymer ransomware attacks, have continued to rise during the second quarter of 2018. These attacks often render businesses inoperable for extended periods of time, resulting in business interruption claims (BI claims) that could cost businesses millions of dollars in lost revenue. In addition to an increase in volume of cyber attacks, we've seen a marked increase in the amount of ransom that is being demanded during these attacks. That's why it's more important than ever that we understand the far-reaching effects that these cyber attacks have on businesses and help our clients protect themselves.

> "With the rise of phishing scams and business email compromise attacks, effective training of employees to identify and guard against these threats is just as important as any technology-based security solution."
>
> **Anthony Dolce,**
> *VP, Cyber Claims Lead for North America*

Business Email Compromise Trends

Social-based cyber claims account for nearly 20% of Chubb's current cyber claim activity, mainly across the Professional Services and Financial Institutions industries.

Business Email Compromise Attacks

What they are

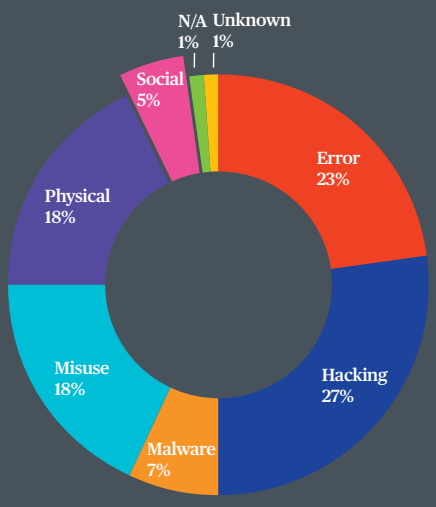
Business email compromise attacks prey on unsuspecting employees by deceiving them into providing passwords and other personal information that allows cyber thieves to access confidential data. These attacks can damage businesses of any size financially–as well as tarnish their reputations.

How they work

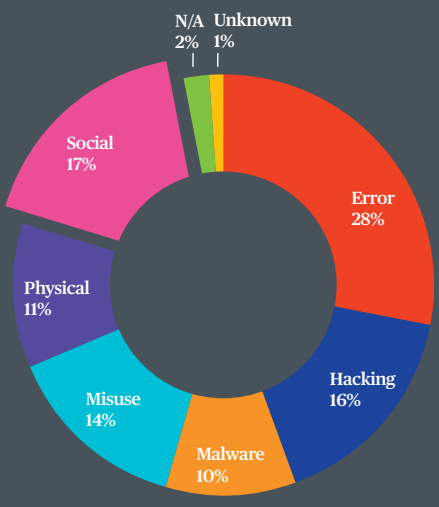
1. A bad actor sends a phishing email to several employees within an organization.
2. An employee responds, thinking the email came from a credible source (usually a supervisor or executive within the organization).
3. The bad actor then uses the employee's login credentials to gain access to the email server and protected information, such as social security numbers.
4. The bad actor can then participate in financial transactions and conduct fraudulent wire transfers.

Claims Count by Action – Comparison

Claim Count by Action
2014-2015



Claim Count by Action
2016-2018



While these attacks can be very difficult to prevent completely, we can help decrease their prevalence and mitigate their damage by making clients aware of how they work and how to recognize suspicious emails.

Bit Paymer

What it is
Bit Paymer ransomware is a relatively new type of attack that first appeared in 2017.

How it works
We have seen it aimed at all sizes of organizations, encrypting all of their networks' files and demanding an exorbitant ransom.

Trend
We have seen ransom demands of up to seven figures in Bit Paymer attacks with negotiations to lower the ransom demands typically failing as attackers know the company can afford it. These attacks are often coupled with another type of malware called a banking trojan that steals financial information.

Chubb Insight
To help protect against this type of malicious attack, it's imperative to ensure that companies have current and secure backups of their data.

Business Interruption Claims in Cyber

What it is
The concept of business interruption (BI) coverage is designed to cover a client's income loss as a result of an event. In the cyber arena, many times ransomware and other types of attacks lead to the client being unable to conduct business operations for a prolonged period of time, which leads to a BI claim under the cyber policy.

Example of how it works

1. The client is a retailer that sells a variety of goods both online and through telephone orders. A virulent strain of ransomware attacked the client's computer system, which also controlled its sales operations and telephone functionality.
2. As a result of the attack, the client's systems were rendered inoperable and its data was encrypted. The attack also encrypted the client's backups, which made it nearly impossible for the client to quickly resume normal business operations.
3. The bad actor sought a large amount of bitcoin in exchange for a decryption key that the client could use to access its data. In this instance, the client refused to pay the ransom.
4. Despite the round-the-clock work of the Chubb Cyber Incident Response Team, because of the large amount of data that needed to be restored, it still took two weeks to fully restore the client's operations.
5. In addition to costs incurred to recover the data from backups and mitigate the situation, the client suffered a BI loss in excess of $500,000.

Trend
BI claims can sometimes be complicated to calculate, and the analysis is very much industry specific. In many instances, a forensic accountant must be retained to assist in the loss analysis.

Chubb Insight
In order to help mitigate the effects of these BI claims, it's important to help our clients understand how these attacks work and build a business continuity plan that includes backups across multiple IT providers.

In 2018,
49%
of Chubb clients have paid the ransom in order to restore their systems–up almost
50%
from previous statistics.

For real-time access to our proprietary data, with insight into current cyber threats and how you can protect your company against them, please visit www.chubb.com/cyber.

Chubb. Insured.℠

Sources: Chubb Claims Data, July, 2018

Form: 30-01-0082 (918)