evolve

Ransomware & Funds Transfer Fraud

San Francisco
Los Angeles
Denver
New York City
Washington D.C.
Boca Raton

RANSOMWARE ATTACKS

What happens in an attack?

Hackers get businesses to download Ransomware viruses by tricking employees into clicking on phishing emails or exploiting software security vulnerabilities. Once downloaded, Ransomware's objective is to lock up proprietary data, including backups, and even cloud data. The hacker then demands a crypto-currency payment to unlock the data within a time window or destroy all the data.

Ransomware damages exceeded $5,000,000,000 in 2017.
*Reference Below

Every 40 seconds a new business in the United States is attacked by Ransomware.
*Reference Below

Why is a cyber policy essential?

Incident Response Costs: < $100,000

This coverage is almost always triggered when a hack is detected and usually ranges in the tens of thousands of dollars, but can go higher than $100k.

Forensic Experts	Data Breach Attorney	Notification Costs	Credit Monitoring	Public Relations Firm
$350/hr – $500/hr	$350/hr – $500/hr	$3 - $5/ individual	$3 - $5/ individual	$350/hr – $500/hr

Cyber Crime Extortion Costs: < $50,000

These costs are usually below $50k, but vary by the hacker's discretion.

System Damage & Business Interruption: < $1,000,000

When these costs are triggered, the costs will vastly vary based upon the size of the business, system downtime, and repair costs. Note, Business Interruption & Rep Harm are usually the largest cost in a claim when triggered.

- **System Damage & Rectification Costs**
- **Forensic Experts**: $350hr - $500hr
- **Business Interruption:** Lost Profit (% of Revenue)
- **Consequential Reparational Harm**: Lost Profit (% of Revenue)

*Must-Know Ransomware Statistics

evolve

San Francisco
Los Angeles
Denver
New York City
Washington D.C.
Boca Raton

FUNDS TRANSFER FRAUD ATTACKS

What happens in an attack?

Hackers manipulate senior executive officers, employees, or clients with the intention of tricking the business or their client into wiring money into the hacker's bank account. Successful unauthorized Funds Transfer Fraud hacking methods consist of stealing login credentials via phishing or key-logging malware, financial data manipulation, and corporate identity theft.

Wire Transfer Fraud attacks will continue to rise over time because it is the quickest payday in a hacker's world and human error is eminent.

Why is a cyber policy essential?

Incident Response Costs: < $100,000

In the event money is wired out, a business will need the following three professionals to make sure the hacker is out of their system and the security breach is patched. The data breach attorney and PR firm will be brought in, should it be found out additional information is stolen or the story hits the news.

Forensic Experts	Data Breach Attorney	Public Relations Firm
$350/hr – $500/hr	$350/hr – $500/hr	$350/hr – $500/hr

Cyber Crime Costs: < $500,000

These costs are usually below $500k, but vary by the type of attack listed below, the hacker's discretion, and the average transaction or bank account size.

- Funds Transfer Fraud (aka wire transfer fraud or social engineering)
- Theft of Funds Held in Escrow
- Theft of Personal Funds (personal bank account protection for senior executive officers)
- Corporate Identity Theft
- Telephone Hacking
- Fraudulent Communications (3rd party wire transfer fraud)

San Francisco
Los Angeles
Denver
New York City
Washington D.C.
Boca Raton

evolve

CLAIMS EXAMPLES

Ransomware Example

In 2017, a catering company with $25M in revenue had an employee click on a link within an email from what looked like a colleague. This link automatically downloaded a ransomware virus into the catering company's network, locking up all of their computers and data (including backups) connected to the network. The ransomware virus demanded that the catering company pay $3,500 in cryptocurrency to the hacker's bank account, in order to unlock the corresponding computers and files within 24 hours. The catering company was in the process of getting the cryptocurrency in order, when the hackers completely destroyed their data. As a result, the catering company was unable to operate their business for two weeks. Forensic experts worked overtime in that two week period repair the corrupted data, while the catering company experienced business downtime. This claim cost the catering company $775,000. The forensic experts billed the catering company for their work at $75,000. The detrimental $700,000 business interruption cost resulted from the catering company's inability to ship their food from A to B, causing it to spoil. The entire cost was picked up through their cyber policy.

Funds Transfer Fraud Example

(1st Party) In 2017, a midsized trucking company's CEO had his email address compromised. An email was sent to wire money to an existing client, but with new bank account details. The CFO merely thought the client opened up a new bank account and trusted the email from the CEO, which was actually written by the hacker. One payment of $73,000 was wired out without being caught. On the 2nd wire request, the trucking company figured out the money hadn't been received by their client and was stopped. Unfortunately, that first payment of $73,000 was unrecoverable.

(3rd Party) In early 2018, a hacker compromised the email login credentials of an employee at a reputable title company. In the next two days, the hacker, posing as the title company employee, convinced one of the title company's client to wire $350,000 for a new home to what was supposed to be the title company's bank account. A week later, the title company followed up with their client, only to find out that a hacker convinced their client to wire money to the hacker's bank account. An immediate lawsuit followed from the client. This title company had a cyber insurance policy that not only defended them from the lawsuit, but it paid the client for their stolen funds.