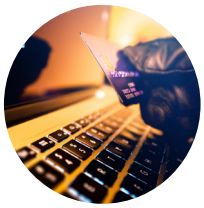
CLAIMS EXAMPLES

"There are two types of companies: those who have been hacked and those that will be."

Robert Mueller, FBI Director 2012

The CFO of an insurance brokerage in Virginia discovered that a fraudulent third party had compromised his computer and was attempting to wire money out of the brokerage's bank account. Upon forensic review, it was determined that the hacker had gained access to confidential information such as social security numbers and sensitive financial information.

In late 2017, a mid-sized insurance agency found that malicious links were being sent internally as well as to their clients from their Human Resources department. It was discovered that one of their employee's Office 365 accounts had been compromised and the malicious emails had been sent to everyone on their contact list. The employee immediately changed their O365 credentials. However, forensics was still needed to determine how the perpetrator had accessed the system and whether PII had been stolen or compromised.



A small insurance agency in Northern California experienced a ransomware attack while their office was closed for the weekend. While the malware initially accessed their systems on Friday, it didn't lock them down until the weekend. The agency's IT department identified the ransomware attack on Sunday. The agency decided not to pay the ransom and immediately began work on removing the malware. Upon removal, roughly 30% of data was still corrupted and a few computers were not usable. The insured accrued about $50,000 in costs for recovery of data and computer restoration.

An insurance agency received an email from a wholesale broker asking them to forward payment for a policy that recently bound. The employee who received the email overlooked that this was a fraudulent request and was being transferred into an account that the agency had never remitted payment to. Upon completion of the transfer, the agency quickly learned they were victim of a social engineering / funds transfer fraud scam and had transferred $42,000 to an unintended recipient.

The CFO of an insurance brokerage in California received their phone bill and was surprised to see it priced at $18,000 for the month, whereas their bill is normally well under $1,000. The agency quickly learned they were included in a widespread telephone hacking scheme that affected numerous businesses. Hackers set up a phone number where if called, the caller would be charged $3 per minute. Hackers then tapped into the broker's VOIP (voice over internet protocol) phone system and racked up a massive phone bill over the course of a few weeks.

COST ANALYSIS

What does it cost your business when 100,000 records are breached?

SAN FRANCISCO | **LONDON** | **LOS ANGELES**

750 BATTERY STREET, 7TH FLOOR, SAN FRANCISCO, CA 94111
415.257.2170
PATRICK@EVOLVEMGA.COM
WWW.EVOLVEMGA.COM

evolve