Financial Services Cyberattacks

Chubb: $200 billion total assets

For many years, cybercriminals have focused their attacks on banks, credit unions and investment firms. But given the bounty of information held by insurance companies, it was only a matter of time before hackers started going after traditional insurance companies.

In March 2020, one of the most notable breaches to hit the industry came to light, when it was made public that Chubb, one of the largest insurance companies in the world, had been hit by a ransomware attack. The New Jersey-based insurance company had fallen victim to Maze ransomware, a particularly sophisticated variant known to spread like wildfire throughout a network, and difficult to root out.

As if foreshadowing this highly publicized incident, Digital Guardian released a report in January 2020 pointing out the growth that it was starting to see in insurance company cyber-intrusions. (And, ironically, Chubb had put out its own cyber-awareness report the year before, called Cyber Attack Inevitability.)

“We are arriving at the place where any digitized business can become a target of a cyberattack," said John Horn, practice director for cybersecurity at Aite-Novarica. “Insurance companies are no exception.”

Elephant Insurance Services: 2.7 million consumers

Elephant Insurance Services in Henrico, Virginia reported in May that it was hit with a breach affecting more than 2.7 million consumers. In a statement on the matter, Elephant said it took "prompt measures to secure its systems, investigate this incident, and determine what information may be affected." The firm also said it "reported the incident to federal law enforcement and is notifying appropriate state regulatory agencies."

The breach exposed names and driver's license numbers, or other identity card numbers, according to Elephant Insurance. The company said it notified consumers about the breach one month after discovering it.

Lakeview Loan Servicing: 2.5 million customers

Lakeview Loan Servicing, the fourth-largest mortgage loan servicer in the U.S., said in March that a breach it suffered last year affected more than 2.5 million consumers, exposing account numbers including or credit and debit card numbers.

"Like many other organizations, Lakeview experienced a security incident in 2021," the company said of the latest breach. "Steps were taken to immediately contain the incident, law enforcement was notified, and a thorough investigation was conducted by a forensic investigation firm. Lakeview's operations were not disrupted."

Equifax: 147 million customers

The Equifax data breach was nothing short of a disaster. A string of terrible cybersecurity practices made the security breach almost too easy for cybercriminals.

There are four primary flaws that facilitated the security breach.

1. The company failed to patch a well-known vulnerability (CVE-2017-5638) for its Open Source developing framework - Apache Struts. At the time of the breach, the patch for CVE-2017-5638 had been available for 6 months.
2. Equifax failed to segment its ecosystem, so the attackers were able to seamlessly access multiple servers after gaining access through the web portal breach.
3. The hackers found usernames and passwords sorted in plain text, which were used to escalate privileges to achieve deeper access.
4. The hackers were able to exfiltrate data undetected for months because Equifax failed to renew an encryption certificate for one of their internal tools.

On top of all this, over a month had elapsed before Equifax finally publicized the breach. During this period, top executives sold company stock, giving rise to insider trading accusations.

More than 40% of the population of America was potentially impacted by the Equifax data breach.

The following data was compromised:

- Names
- Dates of birth
- Social security numbers
- Driver's license numbers
- Credit card numbers

Due to the highly sensitive nature of Personally Identifiable Information (PII) and financial information that was compromised, Equifax was fined $700 million for the breach.

JP Morgan Chase & Co: 83 million customers

Cyberattackers, allegedly located in Brazil, managed to penetrate JP Morgans' perimeter, gain the highest level of administrative privilege and achieve root access to more than 90 of its servers.

Surprisingly, rather than leveraging available account privileges to steal financial information, only customer contact information was stolen. This very unclimactic outcome suggests the objective of the attack was to only steal specific customer details - possibly for use in future targeted cyberattacks.

The following data was compromised in the JPMorgan Chase data breach:

- Internal login details for a JPMorgan employee
- Customer names
- Email addresses
- Phone numbers

Experian: 24 million customers

A threat actor claiming to be a representative for one of Experian's clients convinced a staff member of the Experian South African office to relinquish sensitive internal data.

Experian claimed that the information that was provided was not highly-sensitive, but rather data that are commonly exchanged during the normal course of business.

According to the South African Banking Risk Information Center (SABRIC) - one of the authorities involved in investigations - 24 million customers and almost 800,000 businesses were impacted by the breach.

The following customer information was disclosed to the threat actor:

- Mobile phone numbers
- Home phone numbers
- Work numbers
- Email addresses
- Residential addresses
- Places of work
- Work addresses
- Job titles
- Job start dates

According to Experian, the threat actor intended to use the stolen data to create marketing leads for insurance and credit-related services.