# CYBER UPDATE

SCS AGENCY INSURANCE

## Data Breaches Rose 68% in 2021, Hitting a New High With No Signs of Slowing

According to the Identity Theft Resource Center's (ITRC) annual report—which advocated for more effective laws and regulations to better protect victims of identity fraud—2021 marked a milestone year with a record-setting number of data compromise events.

ITRC recorded 1,862 data compromise events in 2021, up 68% from 2020 and 23% over the previous high of 1,506. Although the number of individuals affected dropped 5% to nearly 294 million, the number of events involving loss of sensitive personal information (e.g., Social Security numbers) increased slightly.

"We may look back at 2021 as the year when we moved from the era of identity theft to identity fraud," Eva Velasquez, ITRC president and CEO, said. "The number of breaches in 2021 was alarming. Many of the cyberattacks committed were highly sophisticated and complex, requiring aggressive defenses to prevent them. If those defenses failed, too often we saw an inadequate level of transparency for consumers to protect themselves from identity fraud. There is no reason to believe the level of data compromises will suddenly decline in 2022."

The type of events that gave rise to data compromise continued to evolve, with ransomware-related data breaches doubling year-over-year in both 2020 and 2021. Ransomware was once thought of as a data encryption event rather than data loss, but ITRC predicted that, at the current growth rate, ransomware will overtake phishing as the top cause of data compromise in 2022.

According to the report, attacks on suppliers or vendors rose in 2021—up to 93 events from 69 in 2020. Topping the list of supply-chain events in 2021 was the Blackbaud ransomware attack. This attack, which occurred in 2020 and affected 480 entities, impacted another 122 entities and over 254,000 individuals in 2021.

Malicious cyberattacks were most frequently the root cause of data compromises and were responsible for 1,613 breaches or exposures. These attacks involve phishing, smishing, business email compromise (BEC), ransomware, malware, zero-day attacks, credential stuffing, and other attack methods. Human and system errors remain an issue, accounting for 179 events in 2021, according to ITRC.

While the mass collection of personally identifiable information doesn't appear to be the primary goal of cybercriminals, individuals still find themselves in the crossfire between cyber gangs and their targets. Consumer information now frequently becomes the avenue into organizations through social engineering or stolen credentials.

Unfortunately, ITRC found fewer than 5% of affected individuals fully secure their personal data after receiving a data breach notice. This may not be entirely consumers' fault. According to ITRC, transparency and timeliness of breach notices have decreased, and individuals are often unaware of how to reduce the impact of compromised personal data.

"Our current legal, regulatory, and policy frameworks at the state and federal levels of government do not adequately address the growing and evolving threats that data breaches represent to individuals, organizations and society as a whole," Velasquez said. "It is not the ITRC's purpose or place to name and shame organizations that have experienced a data compromise, but we do advocate for solutions to these issues."