How Data Breaches Have Aged And Evolved

cyber security risk management

Summary: Banks can always do more when it comes to cyber breaches and threats. We provide the latest insights from Verizon's 2018 Data Breach Investigations Report.

An AARP survey of adults 18Ys+ finds 76% of Americans 50Ys and older say they want to stay in their current residence and 77% would like to live in their community as long as possible. Also, while 33% of those who own a home say they expect it will need major modifications to accommodate their aging needs, 24% of those 50Ys+ plan to relocate and move instead.

No matter your age or stage in life, when it comes to how banks are handling cyber breaches and threats, there is a lot more that can be done. Look no further than Verizon's 2018 Data Breach Investigations Report (DBIR), considered by many as the guide to what's happening in enterprise cyber-attacks

Verizon looked at more than 53,000 global incidents that resulted in more than 2,200 successful system breaches across several verticals, including education, government, healthcare retail, and financial services over the past year. The findings paint a detailed, if somewhat disturbing picture of how the business of cybercrime and its attack vectors are evolving.

In some ways, for example, the more things change, the more they stay the same across all industries. For instance, 68% of enterprise breaches still take a month or more to be discovered, according to respondents. In many, if not most cases, attackers are relying on the same tried and tested malware, phishing techniques, and fraud scams that they have been employing for years. Case in point, arguably the most damaging attacks of the past year have relied on variants of older malware strains, known and unpatched vulnerabilities, and social engineering.

The biggest obvious challenge for the banking industry is that with 76% of all breaches being financially motivated, banks have a big target on their backs. Even worse, cyber thieves have long since realized that community banks may be less equipped to identify certain scams.

However, the report did point to some trends and insights that could aid community banks in better understanding how breaches could be impacting them, and what they can do to mitigate the risk of a successful attack.

Small businesses are a bigger target than ever. Financial services are not the most compromised sector. Rather, healthcare organizations were on the receiving end of 24% of attacks to take that position. But, small businesses were victims in 58% of all attacks, which is one of the biggest and most alarming changes in the cybercrime landscape in the past year.

Sophisticated attackers are the biggest concern. About 73% of attacks are conducted by outsiders vs. 25% that came from insiders. Even more worrisome, 60% of outsider attacks were backed by organized crime rings or nation-state groups. User errors like sending an email to the wrong recipient or incorrectly configuring web servers play a role in only 17% of breaches.

Ransomware is on the rise. It's been 5Ys since ransomware emerged as a threat, and this most recent year was the first time it was the most prevalent form of malware. Ransomware was identified in roughly two out of five of all malware exploits. Off-the-shelf tools, ease of use, and little risk (since attackers don't need to resell their stolen data, just hold it ransom) have made this a favored attack of advanced and newbie attackers alike.

DEPOSIT OPPORTUNITY YIELDING 2.30%

In an effort to expand our relationships, PCBB is pleased to offer community banks a money market deposit account rate of 2.30%, subject to availability. Contact operations@pcbb.com.