Loss of Consumer Trust Can Be Costly

Companies need to be aware of the negative impact

ARTICLE

Krista Garcia

It's logical to assume consumers might lose trust in a company after a data breach or misuse of personal information. But many businesses vastly underestimate the severity of these security mishaps in the eyes of their consumers.

An April 2018 CA Technologies and Frost & Sullivan study demonstrates this perception gap. They aggregated variables like consumer willingness to share personal information online and belief that companies protect their information to come up with a digital trust score ranked on a scale of 0 to 100. US internet users gave businesses a trust score of 61, the same as the global average. But businesses gave themselves an average score of 75 when asked if consumers trusted them.

Executives and Security Professionals Worldwide Who Have Seen a Strong Negative Impact on Consumer Trust and Bottom Line Following a Data Breach, by Industry, April 2018
% of respondents

	Consumer trust	Bottom line
Healthcare	86%	83%
Advertising/media	70%	74%
Retail/ecommerce	59%	47%
Transportation/logistics	53%	47%
Telecom	47%	47%
Financial services	31%	29%
Public sector	25%	31%
IT	17%	17%

Note: n=208
Source: Frost & Sullivan, "Global State of Digital Trust Survey and Index 2018" sponsored by CA Technologies, July 31, 2018

240106 www.eMarketer.com

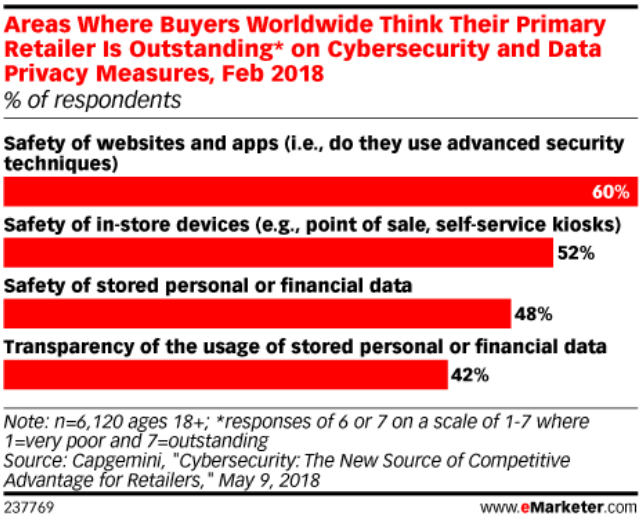
This is important because levels of trust correlate to spending. Consumers across all levels of trust—low, moderate and high—increased spending in the past 12 months, but low-trust consumers decreased spending by larger margins. Forty-three percent of low-trust consumers (those with index scores under 55) increased spending, while 15% decreased spending. By comparison, 57% of high-trust consumers (those with scores of 70 or higher) increased spending, while only 4% spent less.

Research from security company RSA also shows the financial impact that results from losing trust. Nearly seven in 10 internet users in the US and Western Europe have boycotted (or would boycott) a company that repeatedly did not protect their personal data.

Interestingly, the CA Technologies/Frost & Sullivan study showed the retail industry had the biggest gap between loss of consumer trust after a data breach and the monetary effect. Fifty-nine percent of consumers said a breach had negative impact, but 41% of retailers said the breach had financial impact.

Worldwide, 46% of consumers don't believe (or are unsure) that businesses sell their personal data, but 43% of businesses overall said they engage in this practice. For retailers, though, that figure drops to 26%. Financial services (83%) and healthcare (74%) are far bigger offenders.

Buyers worldwide were asked by Capgemini in February to rate the retailer they shopped at most often on different cybersecurity measures. Most (60%) said their primary retailer does an outstanding job of making sure their sites and apps are safe. Not surprisingly, based on the above findings from CA Technologies/Frost & Sullivan, the lowest marks were given to the transparency of personal or financial data (42%).



Internet users in the EU may have less to worry about than others, thanks to the General Data Protection Regulation (GDPR) enactment in May. This new regulation might also have an impact on more explicit terms and conditions for everyone. Only 49% of consumers surveyed by CA Technologies/Frost & Sullivan thought data protection policies provided by companies were easy to understand.