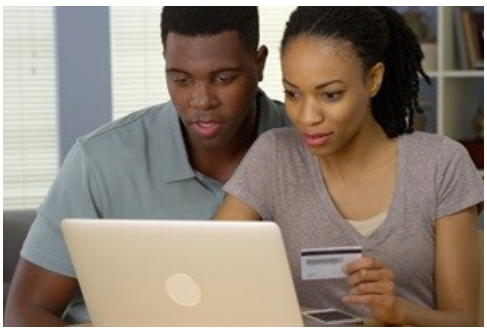
BIZCOMMUNITY

Forrester's predictions indicate CMOs at risk as consumers up experience needs

Forrester's 2017 predictions indicate US online adults want new and engaging digital experiences and will switch companies to find them, IoT will suffer compromise and over 30% of CMOs could be ousted.



© Mark Adams via 123RF

While the company has advised a strong focus on technology to improve customer experience, it has also warned that trying to play catch-up with early technology movers could spell disaster for companies that are unprepared 2017 is the year of action.

The predictions look at business strategy, leadership, customer experience and technology dynamics to examine progress and predict the key events, changes and trends that will occur in 2017.

Customer obsessed or broke

Three years ago, Forrester identified a major shift in the market with the advent of what it refers to as the 'age of the customer', pointing out that the power has now shifted away from companies in favour of the digitally savvy, tech-enabled consumer.

"Your business model is under attack and it is not by your competitors. It is under attack from your customers," writes Cliff Condon, chief research and product officer at Forrester, in his contribution to the 2017 predictions. "Our research shows that more than a third of all US online adults want new and engaging digital experiences. They will switch companies to find these experiences. In this environment, being customer-obsessed can be your only competitive strategy."

Forrester predicts that the next wave of customer experience will profoundly affect companies, pointing to a clear correlation between customer experience and revenue growth.

The company says the pressures resulting from this new market dynamic will result in CEOs being forced to make tough decisions. Forrester predicts that the search for leadership who can navigate the new digital and customer obsession requirements will result in extensive staff turnover, with up to a third of current CMOs being exited.

Playing catch-up may hit hard

Condon points out that technology has been one of the key drivers in empowering customers and will now play an intrinsic role in allowing companies to serve these same customers. Newer technologies such as artificial intelligence (AI), virtual reality (VR) and Internet of Things (IoT) will be employed to drive the change. However, he warns that this may come at a price for companies that do not plan and deploy properly.

“There will be at least one fatal misstep from a business technology novice trying to keep pace — in 2017, we predict that a Fortune 1000 firm will go out of business due to poor resiliency planning following a security breach.”

Expanding on the prediction in one of its security prediction reports, Forrester cites broader connectivity and a growing investment in digital business creating new implications for devices, data and corporate resilience and, with this, new challenges for the security and risk leader.

IoT faces particular challenges

“IoT, in conjunction with cloud and BYOD, alters the fundamental ways we plan for resilience. Targeted espionage, ransomware, IP theft, denial of service, privacy breaches, and loss of customer trust all carry more weight today,” write Amy Demartine and Jeff Pollard, in their new *Predictions 2017: Cybersecurity Risks Intensify* report.

Pointing to the rapid rise of IoT, the report goes on to predict that more than half a million IoT devices will suffer a compromise during 2017.

The rush to deliver to market has exacerbated the challenge and Forrester believes that firms are developing and delivering solutions without solid plans for updates. This leaves the devices open to vulnerabilities, which security teams will not be able to remedy in a hurry.

The report mentions verticals and applications, which are especially vulnerable to attacks. These include fleet management in transportation; security and surveillance apps in government; inventory and warehouse management apps in retail; and industrial asset management in primary manufacturing.

Security attacks initiated in 2017 do not remain limited to hackers looking for commercial gain either. Forrester has warned companies and individuals that current and past political or social statements and donations could expose them to potential attack.

“DDoS attacks, using IoT devices, are becoming a common means of disrupting operations for companies or individuals that threat actors disagree with. If you have never factored geopolitical concerns into your security risk analysis, you ignore them at your own firm’s peril,” the report cautions.