How Marketers Can Protect Themselves from Breaches

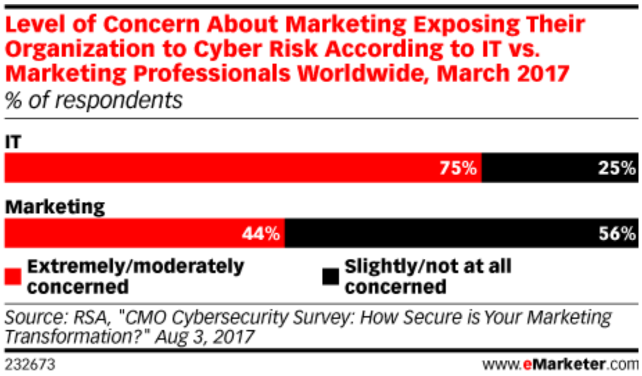
Cybercrime is on the rise

ARTICLE | JANUARY 19, 2018

eMarketer Editors

Rapid advances in digital technology and data collection have led to an impressive rise in data-driven marketing. While these digital tools can greatly improve campaign performance, they can also lead to data security, privacy and ethics concerns.

Though many of today's marketers are still not overly concerned—or intimately involved—with cybersecurity, there are several things they can do now to put themselves in a better position to protect their brand.



Level of Concern About Marketing Exposing Their Organization to Cyber Risk According to IT vs. Marketing Professionals Worldwide, March 2017

% of respondents

Source: RSA, "CMO Cybersecurity Survey: How Secure is Your Marketing Transformation?" Aug 3, 2017

While there is no magic bullet to prevent or fix security issues, there are a number of best practices to consider. A key one? Bone up on technology and security fundamentals.

As mobile and IoT devices multiply, marketers have an obligation to understand the connections between devices and data and the many moving pieces of the marketing data ecosystem. Marketers should know at least the basics of their operation's data collection protocols, data infrastructure, storage parameters and security controls.

Marketers should also understand their limitations. It's just as important to know what you don't know and enlist the right resources when needed.

These are just a few best practices drawn from eMarketer's latest report, "Digital Security in the Age of New Tech: Best Practices for Marketers." The report examines some of the major cybersecurity threats facing businesses today. eMarketer PRO subscribers can access the full report here. Nonsubscribers can learn more here.