

What companies are doing to reduce cybersecurity risk

Article

In the absence of regular outreach to consumers for feedback on cybersecurity practices, there is often a disconnect between what the company is doing and what the consumer thinks is happening. Since cybersecurity has historically been siloed within the IT department, there's often a similar disconnect within a company among departments. It's important to shrink these gaps in understanding as threats grow.

Marketing and communications departments must now address technical data issues and not just ones related to reputation and consumer trust. This will happen more frequently as privacy practices grow in complexity and overlap with security. According to a survey from Duke University's Fuqua School of Business, nearly two-thirds of US CMOs have promised not to sell customers' personal information and ask for consent before using customer data. But only a bit more than one-third had developed a brand privacy policy.

Actions Their Company Has Taken to Increase the Trust of Their Brand in the Face of Privacy Concerns According to US CMOs, Feb 2022

% of respondents



Source: Duke University's Fuqua School of Business, "The CMO Survey: February 2022" commissioned by Deloitte and American Marketing Association, Feb 28, 2022

273884

eMarketer | InsiderIntelligence.com

Marketers are adjusting both their privacy communications and their data handling practices. Companies used to include information on privacy actions in their environmental, social, and governance reporting as a bare minimum. But many are now doing more than that. Some are making privacy the center of entire advertising campaigns. At the same time, some are implementing customer data protection practices that can include the use of data relationship management programs and data clean rooms.

- Companies should address any disconnect between consumers' perceptions about their data practices and the reality. In January, Boston Consulting Group reported 57% of consumers believe companies are selling their data, while few brands actually consider themselves to be doing so.
- Data privacy has been at the center of several marketing campaigns over the last few years. Apple launched an ad campaign earlier this year designed to educate consumers about their

data protection and security practices. The campaign ran on billboards as well as on social media video sites.

The ongoing shift to first-party data will lead to new security problems. As companies end their use of third-party identifiers, data clean rooms are becoming a popular way to fully leverage first-party data by combining it with data from outside sources. Data clean rooms are online platforms where companies can share data with advertisers in a safe manner without violating privacy practices.

In theory, these clean rooms don't expose any sensitive consumer data, but in practice, the involvement of more players and locations creates more security risks. As a result, companies should strive for consistent, well-aligned security practices and privacy standards.

Read the full report.

Report by Jessica Lis Aug 11, 2022

The Cybersecurity Risk

