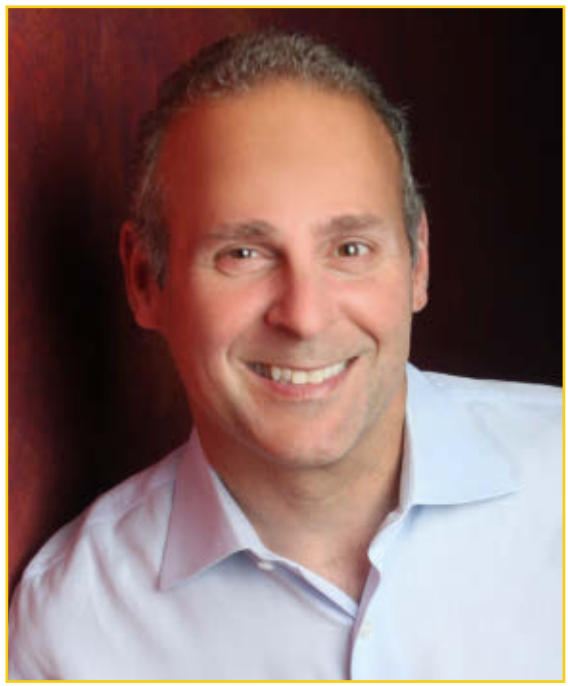
TIME TO FORGE THE **TRUST AND SAFETY** MOVEMENT

BY CRAIG SPIEZLE



OVER THE PAST DECADE a plethora of new "C" titles have emerged in both the public and private sectors. In response to GDPR the Chief Protection Officer has joined the ranks with other "C" level leaders including marketing, revenue, security, finance, operations and privacy. Each of these roles has elevated critical issues to the boardroom. Yet, all too often, they work in isolation. A looming risk is the failure to holistically take a customer-centric approach and understand the aggregate impact of business decisions to trust.

As a proof point one does not have to look any further than what often occurs at the end of sales quarter. Under pressure from Wall Street, a flurry of email campaigns are pushed out and more aggressive name sharing occurs. Websites employ more invasive, and at times, annoying ads. Publishers increasingly blur the lines between editorial and ads. While the privacy community advocates for clearer disclosures and notices, they often take a backseat to revenue goals employing cross-device tracking, device fingerprinting and retargeting. Security teams, while chartered to protect the infrastructure and data, typically do not have voice regarding the security of pages they link to, the ads rendered on their site or the end-user experience.

While these scenarios may appear abstract, I have experienced them first hand. Nearly a decade ago, during my tenure at Microsoft, I was chartered to develop privacy-enhancing features for Internet Explorer. New features were successfully introduced in a beta and embraced by users and consumer advocates. When launch neared, we were derailed. Under pressure from the advertising business groups, and, ironically, the privacy team who were of the compliance mindset, we were forced to remove the features. The impact to possible revenue goals and the risk of alienating ad industry trade groups and partners for

"AS WE APPROACH 2019, I CHALLENGE YOU TO MAKE CONSUMER TRUST AND SAFETY THE FOUNDATION AND GUIDING PRINCIPLE OF YOUR BUSINESS."

political purposes was too high, in the opinion of leadership.

Fast forward to today; working with a client, I recently participated in a meeting with the Chief Information & Security Officer, (CISO), Chief Marketing Officer (CMO), Chief Revenue Officer (CRO) and Chief Privacy Officer (CPO) regarding the security and privacy risks associated with third-party advertising. The CISO raised the concerns regarding advertising links and security threats of the resulting landing page. These included confirmed cases of malvertising and drive-by ransomware downloads. In one instance more than 1,000 third-party trackers were observed on a single website.

The CMO asserted that the CISO should only focus on the link itself and worry about the risk of breaches to the company. Others chimed in, stating the company was not responsible for the user experience of an advertiser's website or their respective privacy practices. The CPO concurred, stating the company's privacy policy provides air coverage informing users they click at their own risk. The CRO jumped in saying it was not their responsibility to tell an advertiser how to secure their site and she did not want to add friction to the advertiser campaign onboarding process.

The CISO responded and said he believed this was short-sighted and we need to take a more comprehensive, long-term view, providing the user a trustworthy experience. A parallel was made that this was not unlike a physical store, where we have a responsibility to help protect customers from harm. If we know there is a risk of pickpockets, we need to hire security or put in place deterrents and make our stores a safer environment to visit. He argued we need to hold advertisers accountable to take steps to prevent harm to our customers. He asserts that revenue objectives would be met over time with increased site metrics and click-through performance. The debate escalated with others stating there is no guaranteed safety. The meeting disbanded and the status quo prevailed.

This debate highlights the need for a sea change including roles and responsibilities. It is about the need to shift from the mindset of focusing on compliance to one of customer stewardship. I propose the creation of another member of the C suite, the Chief Trust & Safety Officer. Ideally, such a role would encompass the entire user experience and redefine the role of the CISO. This role would balance the short- and long-term impact to the user, and, most importantly, the long-term impact on the organization's brand, calibrated to the "risk appetite" of the executive teams.

As we approach 2019, I challenge you to make consumer trust and safety the foundation and guiding principle of your business. Make a New Year's resolution to elevate the Chief Trust and Safety Officer to the board. Respecting the consumer experience will yield long-term dividends, driving revenue, user engagement, and the market value of the organization. MQ

The AgeLight Advisory Group helps clients accelerate the adoption of security and privacy-enhancing practices and policies, and navigate the complex environment accelerating their go-to-market strategies. https://Agelight.com/