Understanding First-to-Market versus Secure-to-Market

Technology, Privacy, and eCommerce

Banner artwork by Irina Strelnikova / *Shutterstock.com*

What is “secure” and “first” to market strategy and why it matters

In today's digital economy, businesses are under intense pressure to be the first to market with new products and services or sparkly enhancements to existing products. However, this constant push to launch new and improved stuff can often come at the expense of user security. We've all heard the phrase "move fast and break things," which emphasizes the benefits of being first to market and iterating once established. Inherent in this is that things may get broken. In the digital economy, often the thing that gets broken is user trust, data privacy, and security.

First to market

As businesses strive to be first to market, the temptation to cut corners on privacy engagement, reviews, and security assessments can be strong. The consequences of this includes misinformation, over-collection of personal information, and security incidents potentially involving sensitive data or data concerning minors. In addition to the obvious impact on users, these incidents can have a devastating impact on businesses, both financially and reputationally.

Striving to be the first to market a product can lead to many errors and data security issues. Aleutie / *Shutterstock.com*

> As businesses strive to be first to market, the temptation to cut corner on privacy engagement, reviews, and security assessments can be strong.

A “first-to-market" strategy can be a high-risk, high-reward approach. It can be a high-stakes gamble where winning entails establishing brand recognition, cultivating customer loyalty, setting new industry standards, and cerates strong barriers to fend off potential competitors.

However, it is not without its own set of challenges. Consider Equifax, one of the major US credit bureaus (Equifax Settlement with FTC). In 2017, a colossal data breach exposed the personal data of over 147 million Americans, all thanks to a known vulnerability in Apache Struts. Shockingly, it is reported that Equifax was aware of the vulnerability for months but chose the “first to market” route, launching a new credit scoring system, rather than patching the security hole. Ultimately, “first-to-market" cost Equifax US$575 million, and potentially up to US$700 million, as part of a global settlement with the Federal Trade Commission, the Consumer Financial Protection Bureau (CFPB), and 50 US states and territories.

Secure-to-market

On the other hand, “secure-to-market" is the more cautious and less appealing twin, prioritizing security and protecting user privacy, but taking the slower, more meticulous path. It may seem like a killjoy compared to “first-to-market,” but, on closer inspection, has enormous appeal.


The "secure-to-market" approach may take time to assess through the production cycle but it is a much safer strategy. VectorMine / *Shutterstock.com*

The "secure-to-market" approach recognizes the critical need to protect users from these pervasive threats. It acknowledges that in a world where data is not just a commodity but the lifeblood of and most valuable asset of many big data, fintech, and social media companies, the responsibility to safeguard this information has never been more important. The "secure-to-market" strategy invests time in securing a product or service throughout the product development lifecycle, including privacy assessments, security audits, third-party penetration testing, privacy impact assessments, transfer impact assessments, and ensuring that all potential vulnerabilities are addressed before launch.

Yet, it is distressingly difficult to sell "secure-to-market" to product teams, especially when balanced against revenue and overly optimistic "What could possibly go wrong?" projections.

Why it matters

The global average cost of a data breach in 2023 is reported to be US$4.45 million, a 15 percent increase over three years (IBM Cost of Data Breach Report 2023). However, there's more to this cost than just the monetary figure. The intangible but invaluable components of reputation and goodwill are also on the line. If a company's claim to fame becomes “running fast and breaking things,” it’s hardly a legacy to inspire trust. A reputational hit like this can shake consumer trust and even push well-intentioned lawmakers to draft hasty laws in an attempt to safeguard the booming online marketplace.

Remember Zoom's meteoric rise during the 2020 COVID-19 pandemic? Zoom’s rapid response and innovation were essential to facilitate the vast numbers of us suddenly forced to telework at the start of the pandemic. The company raced to dominate the telework market, but in the process, “Zoom-bombing" became a buzzword. Uninvited participants crashed meetings, revealing the price of hasty

“first-to-market" strategies.

Zoom’s experience demonstrates the delicate tightrope businesses often face when trying to meet the demands of the moment while ensuring robust security measures. Remember that speed, while crucial to meet the demands of the moment, must be balanced with robust security measures.

So, why does "first-to-market" hold such allure? One argument to explain the pervasiveness of this strategy is that it naturally aligns with intellectual property theories, which assert that individuals have the right to enjoy the "fruits of their labor."

This viewpoint recognizes an interest in being the first to invent or innovate, and if successful, it may allow businesses to reap the well-deserved rewards of their hard work. However, the critical question remains: Can embracing this notion serve as a valid excuse to neglect privacy and security? In the eyes of most, businesses bear an inherent, if not a contractual and legal, responsibility to safeguard their customers' privacy, even if it entails a slight delay in reaching the market.

> Remember that speed, while crucial to meet the demands of the moment, must be balanced with robust security measures.

“First-to-market" and “secure-to-market" are not mutually exclusive

The twin concepts of “first-to-market" and “secure-to-market" can coexist, ensuring the safety and trust of users while driving innovation. However, this requires deliberate action. Businesses must navigate the fine line between speed and security by incorporating a well-rounded approach to product development and release.

One way to achieve this balance is by adopting a proactive mindset towards security and privacy from the outset. Privacy by design, a principle originating from privacy law, emphasizes integrating privacy considerations into the very architecture of products and services. By doing so, companies can reduce the need for retroactive security measures and minimize the risk of data breaches.

Furthermore, fostering a culture of responsibility and accountability within organizations is essential. This involves educating product teams, executives, and employees about the importance of privacy and security, not only from a legal or regulatory perspective but also as a fundamental ethical duty. A commitment to safeguarding user data should be part of a company's lived values.

Employees inside the organization should commit to being educated on the fundamentals of privacy and security to protect user data. AB Graphic / *Shutterstock.com*

> Privacy lawyers and compliance professionals remain the torchbearers, underscoring the vital importance of "secure to market" with industry-wide collaboration and the sharing of best practices can help businesses stay on the cutting edge of privacy and security.

The White House is considering new cybersecurity regulations, and there is a growing call from the technology sector for Congress to pass a federal privacy bill to replace the many state laws modeled after the EU's General Data Protection Regulation. Given the current gridlock in Congress, it's unlikely we'll see national privacy legislation soon. In this waiting game, privacy lawyers and compliance professionals remain the torchbearers, underscoring the vital importance of "secure to market" with industry-wide collaboration and the sharing of best practices can help businesses stay on the cutting edge of privacy and security. This can involve participation in industry associations, attending conferences, and sharing knowledge and experiences with peers.

When reputation really matters

In conclusion, although convincing stakeholders to prioritize the “secure-to-market" approach might sometimes feel like a sales pitch in itself, the effort is well worth it. This strategy demands a comprehensive approach that incorporates privacy by design, education, involving users, and collaborating with the wider industry. Ultimately, this approach not only serves the best interests of users but also aids companies in preserving their reputation and navigating the intricate terrain of privacy law and regulation more adeptly.

Join ACC

Disclaimer: The information in any resource in this website should not be construed as legal advice or as a legal opinion on specific facts, and should not be considered representing the views of its authors, its authors’ employers, its sponsors, and/or ACC. These resources are not intended as a definitive statement on the subject addressed. Rather, they are intended to serve as a tool providing practical guidance and references for the busy in-house practitioner and other readers.

Lisa Glover-Gardin

Adjunct Professor of Law

Lisa Glover-Gardin, Adjunct Professor of Law at Santa Clara University, specializes in Privacy and Technology. With a notable career, she held positions such as Senior Director and Global Head of Privacy Legal at PayPal and Managing Senior Counsel at Google LLC. During her tenure at Google, she played a key role in building Google's Third-Party Data Protection Compliance program. Before dedicating her focus entirely to Privacy, she led Quantum Corp's global employment law and compliance team.

Active in the community, Glover-Gardin has served in leadership roles on boards such as The Girl Scouts of Northern California, Hayward Unified School District, Hayward Area Recreation District Foundation, and as a two-term Commissioner for the City of Hayward. She holds an LLM from the University of California, Berkeley (Bolt) School of Law, a JD from Santa Clara University Law School, and a BA and MBA from San Francisco State University. A Certified Information Privacy Professional (CIPP/US), Glover-Gardin also serves as a faculty member at Practicing Law Institute (PLI).