SAFEBASE

Whitepaper

Five Steps to Long-Lasting Customer Trust

Increased Cybersecurity Risk Has Shifted the Customer Trust Landscape

Increased Cybersecurity Risk Has Shifted the Customer Trust Landscape

The past several years have been marked by the crashing of converging forces — both literally and figuratively. The world's connectedness drove us all to isolation. War ignited. Consumers and retailers clashed in their high expectations and low available resources. Technology companies laid off thousands while simultaneously lamenting the difficulties of hiring.

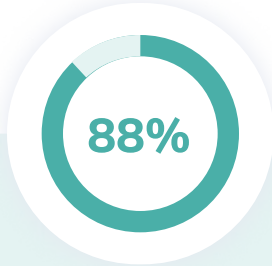
Technology providers across the spectrum have made significant changes in the way they manage and secure their data.

As a result, technology providers across the spectrum have made significant changes in the way they manage and secure their data — and that of their customers. This includes increasing their cybersecurity budgets, investing heavily in employee training programs, and evolving their approaches to cybersecurity to become more embedded in both company culture and their assessments of vendors and partners.

Data Becoming the Cornerstone of the Future of Business

Meanwhile, organizations in every industry, even those considered more “traditional,” are making momentous shifts to move their data into the cloud, while simultaneously developing new strategies that put data, and its connectedness, at the heart of their business models.

This convergence of trends, making people more dispersed, while our technologies grow more connected, means that security is top of mind not just for CISOs and their teams, but for the entire boardroom.



of Boards of Directors view cybersecurity as a business risk

Source: Gartner

Technology Buyers Respond with Heightened Scrutiny

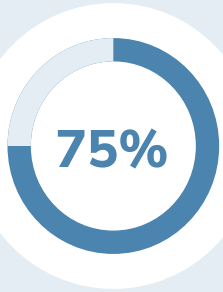
The recognition of heightened security threats – and the outsized impact they have on the business – has spurred significant shifts in the way technology buyers behave as well. Across the spectrum of buyers, from small to enterprise organizations, in every industry and location, security due diligence has become a critical component in the buying decision, as well as to ongoing customer-vendor relationships.

This means that not only have technology buyers become far more discerning in their assessments of vendors, but they are also far less trusting even once an agreement has been signed.

As a result, for technology providers, “customer trust” — a buyer’s lasting feeling of confidence in a seller’s security capabilities — is both more crucial and more difficult to build and maintain than ever before.

Customer Trust:

A buyer’s lasting feeling of confidence in a seller’s security capabilities.



Nearly 75% of B2B purchasers say that “tech vendors typically fall short of being honest.”

Source: Deloitte

Customer Trust: An Intentional, Organization-Wide Effort

In every context, including our social relationships, our romantic partners, and our business partnerships, building and maintaining trust requires intentional effort. It starts with the foundational layer of actually being trustworthy — steering clear of committing those agreed-upon deal-breakers.

Then, one must actively communicate that commitment, create clear and open paths to interaction, while also remaining vigilant, adjusting behavior as time goes on.

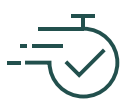
More and more, these motions apply to vendors and their buyer relationships as well. As buyers become more discerning, technology providers must take intentional steps to demonstrate their commitments to trustworthiness, to smooth the path to understanding and validation of trustworthiness, and to continuously make efforts to improve.

Not only do Security and GRC leaders need to continue to uplevel their security positions based on well-known principles of trust, they also need to effectively communicate their security postures to their customers, proactively alert them to updates and response protocols, reduce friction across buyer vetting measures, and ensure proper controls and visibility into the ongoing touchpoints they and their teams have with customers.

In short, Security and GRC leaders need to invest in the five pillars of customer trust:

Transparency

All trust programs and philosophies are well-articulated and easily accessible to the right parties



Proactivity

All relevant information is provided to interested parties in an urgent and holistic manner

Connectivity

Information is updated and communicated via seamless back-and-forth between vendor and customer

Control

Organization has real-time oversight into how information is accessed and utilized

Insight

All principles are continuously improved upon through the use of back-end reporting and alerts

By building on these five pillars, and involving their stakeholders in the process, security and GRC leaders have the opportunity to reap significant rewards, for both their workload and their business's success.

Here’s what each pillar looks like in practice:

Transparency

Transparency is defined as “being easy to perceive or detect.” For security leaders, this means moving pertinent security documentation and information from behind the proverbial wall and serving them to customers in an easily-digestible, easy-to-understand format. All trust programs and perspectives should be organized, well-articulated, and housed in a single, accessible place that tells the full story of a company’s security posture.

Proactivity

Trust in any context isn’t built on reactivity. To achieve customer trust that’s deeply embedded, technology providers must make efforts to communicate their security commitments before the tough questions are asked, in a way that’s easily accessible to buyers and customers (and ideally to the rest of their organization as well). This also means creating lines of communication to proactively provide updates as time goes on, whether it be reporting an improvement or being clear about the company’s response to a potential security breach.

Connectivity

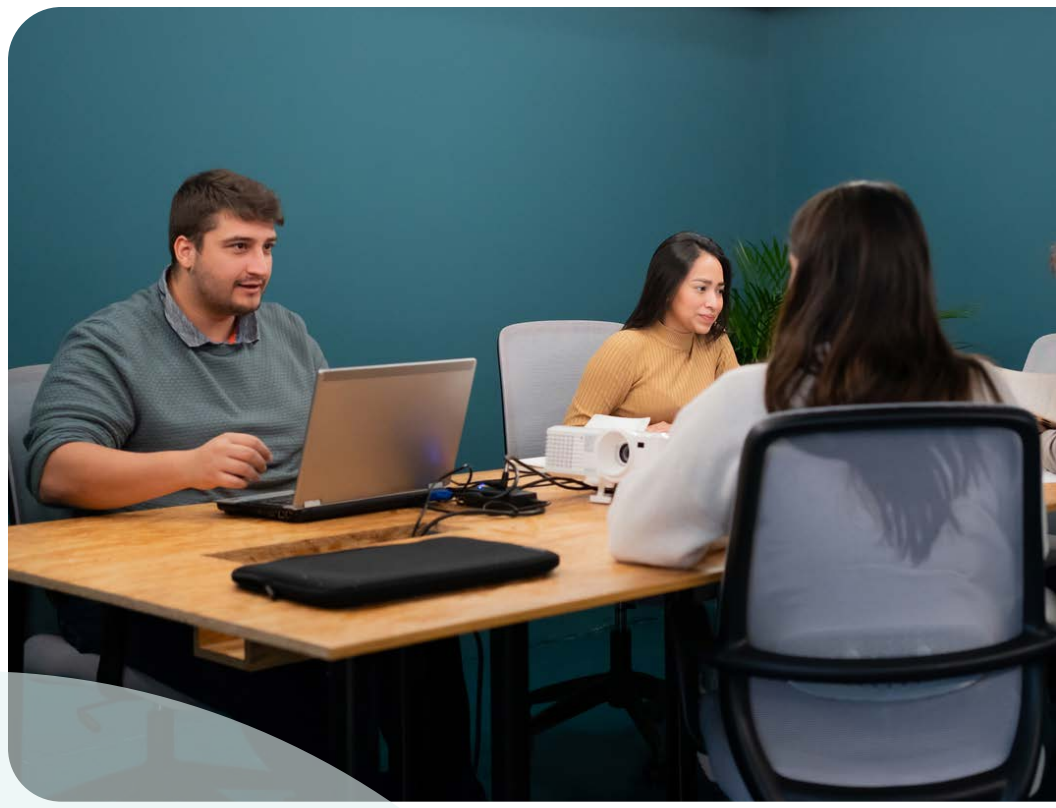
At its core, trust is powered by intentionality — by actively clearing pathways for one another, smoothing interactions, and creating open lines of communication. The journey to customer trust is no different. Security leaders can take major steps toward ongoing buyer confidence by creating streamlined flows of information between buyers and the company, reducing friction in the review process, and eliminating the back-and-forth that is a hallmark of security reviews. Connectivity also reflects the efforts to create streamlined paths to the sharing of information — reducing opportunities for the flow of information to break, such as between sellers and their prospective customers.

Control

Without a firm grasp on the accuracy and proliferation of sensitive information, all other efforts to create long-lasting customer trust are likely to be wasted. This means building systems that put security teams — not their stakeholders or customers — in control of sensitive information and documentation. This includes both access controls as to who can receive access to what documentation and for how long, as well as documented oversight on an ongoing basis.

Insight

The final step after developing control over the flow of information is to understand if efforts are working on the path to building and maintaining customer trust. This requires building an infrastructure that connects customer trust data with other critical business data, providing real-time insight into program effectiveness. Security leaders can continuously improve their efforts — both in the creation and maintenance of customer trust, as well as the impact it has on the business.



Invest in Customer Trust to Spark Business Growth

Creating a solid foundation of “trust” is never “done” — that’s why forward-thinking Security and GRC leaders today have made significant investments in developing strong security postures and continuously improving their vigilance and resilience. Yet, few security leaders take the extra steps to create truly long-lasting trust with their customers, beginning when they are buyers. Those that do are bound to reap rewards — not just tactically, but more importantly, in areas critical to the success of the business.

Benefits of Investing in Customer Trust

Business Outcomes

- Shortened deal cycles
- Higher-value contracts
- Stronger long-term customer confidence

Process Outcomes

- Dramatically reduced security questionnaires
- Minimal back-and-forth across security teams, go-to-market teams, and buyers/customers
- Greater control of sensitive information and documentation

SAFEBASE

SafeBase can help.

SafeBase is the customer trust platform that helps enterprise organizations increase buyer confidence, develop stronger customer relationships, and streamline security review efforts.

SafeBase facilitates customer trust by providing the infrastructure and tools to help GRC and customer trust teams master the five pillars of customer trust. Get in touch with us to learn how enterprise organizations like LinkedIn, Jamf, Instacart, and Clickup are saving their teams time and creating better customer experiences through their partnerships with SafeBase.

Visit safebase.io to learn more.

Get in Touch