SAFEBASE

Whitepaper

Create a Culture of Trust and Transparency

A Guide for Security and GRC Leaders

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.

These and myriad other tectonic shifts altered the way we connect as people, and changed the way businesses think about both future success and their relationships with customers.

Cybersecurity Emerges as the Revenue Enabler of the Future

In the business world, remote and hybrid work have become unambiguous as the future of work, while systems across every mode of technology have become more seamlessly integrated than ever before.

For Security and GRC leaders, these trends have come together to solidify the role of cybersecurity as not only a crucial focus area, but as central to an organization's ability to grow in the years ahead.

In response, leaders in the security space have either been forced or inspired to reimagine their contributions to their respective organizations. Traditionally viewed as a backstop against potential threats at best, and a scapegoat at worst, Security & GRC leaders are emerging as critical inputs to the company's business strategy.

More than that, they are investing in approaches and systems that acknowledge the role of cybersecurity, and more broadly, "trust," as a revenue enabler — a true competitive advantage.

Security and GRC leaders are investing in approaches and systems that acknowledge the role of cybersecurity, and more broadly, "trust," as a revenue enabler.

CISOs & Security Leaders as Business Leaders

In addition to rapid evolutions to the organization's cybersecurity plans, these changes also mean shifts in the role of security leaders. An increasing number of organizations in all industries are placing cybersecurity experts at the executive and boardroom tables. Chief Information Security Officers (CISOs) and their delegates are viewed more and more as business partners to the rest of the company, emerging from decades of behind-the-scenes defense to proactively providing insight to the overall company's growth strategy.

CISOs & Security Leaders as Culture Shapers

An innovative group of security leaders are taking their understanding of their roles a step further — positioning themselves and their teams as critical shapers of company culture.

They recognize that to make cybersecurity a critical part of business growth, they must take pains to not only educate all organization-wide employees on the company's security protocols and perspectives, but to also enlist their help as champions and advocates.

Leaders like former Salesforce Chief Trust Officer Jim Alkove are making it their job to embed "trust" as one of the company's distinct values. In his time at Salesforce, he was joined by other business leaders in setting the requirement that all 60,000 employees play an active role in maintaining a high bar of trustworthiness. More than that, every employee was made responsible for spreading the message of Salesforce's commitment to trust with customers, buyers, and partners as a unique value proposition.

"We've become a more integrated global society and we've become more interdependent on the success of our companies working together, not just from a sales perspective, but now from an actual live operational perspective... so, there's a lot more of these trust conversations coming to the fore driven by customers. But also you're starting to see regulators and governments push this agenda as well."

Jim Alkove | Former Chief Trust Officer, Salesforce

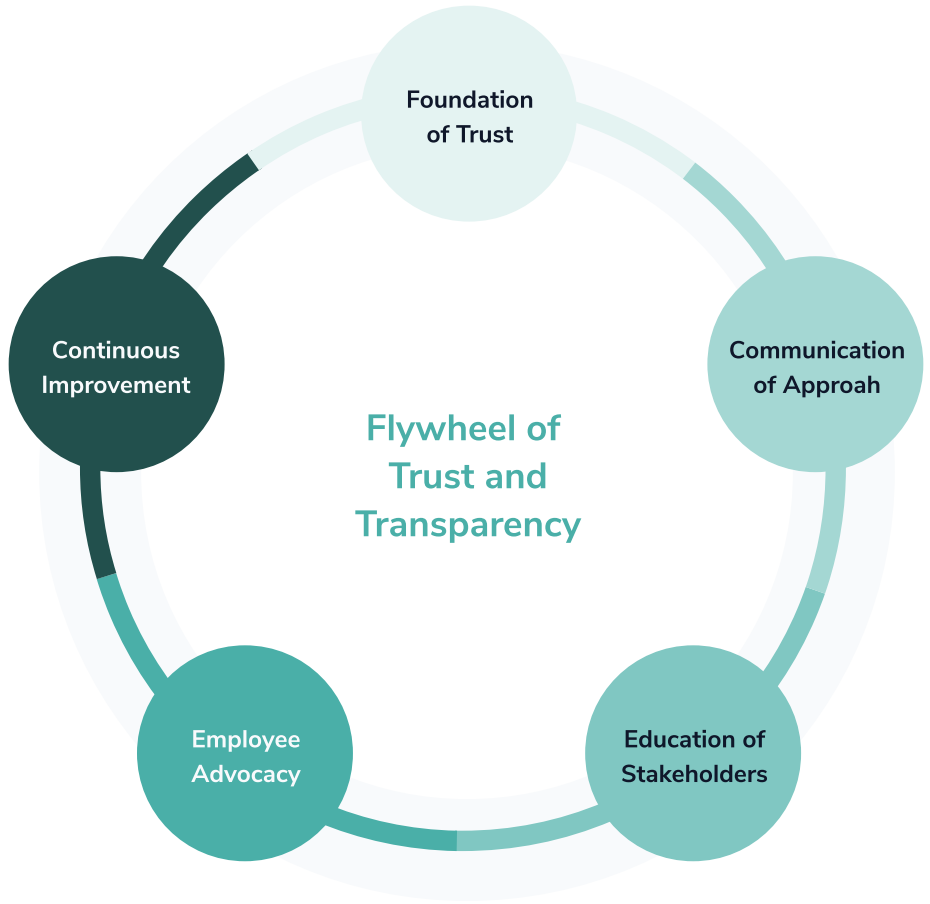
In short, innovative cybersecurity leaders are making it their business to create a culture of trust and transparency.

Every employee was made responsible for spreading the message of Salesforce's commitment to trust with customers, buyers, and partners as a unique value proposition.

Building a Company-wide Flywheel of Trust and Transparency

Creating a culture of trust and transparency from the inside out is an intentional, always-on approach that requires a flywheel of programs and philosophies involving all employees.

- It starts with mastering the foundational responsibilities of the Security and GRC teams, establishing best-in-class trust policies and programs that set up the organization to protect its data — and that of its customers and partners — from ongoing and unforeseen threats.
- The work continues into the realm of communication, developing an articulated perspective on that security posture that is consumable by both internal and external stakeholders. Without audience-friendly language and organization, cybersecurity efforts may continue to remain behind the scenes.
- These leaders then build pathways to getting that ever-evolving position in front of their stakeholders, including buyers and customers, removing or reducing barriers to access and making ongoing communication and education a stalwart element of their team's KPIs. Communication and education should be an ongoing part of the cybersecurity team's responsibilities, embedded into the way the team does business.
- Next, they create structures and systems designed to enlist all employees in advocacy for trust and transparency, including ongoing training and reinforcement.
- For go-to-market teams, this advocacy work is even more crucial. Security and GRC leaders must create systems and relationships that embed the communication and education of the company's security philosophies into the sales, customer success, and even marketing motions that drive the company's growth.
- Finally, these leaders flip the traditional cybersecurity script in ensuring visibility of their work across the organization, identifying and expressing the connection between their team's work and the business's goals. They leverage data from their own teams and their partners across the business to prove the value of their trust programs. Meanwhile, these leaders are able to utilize these insights to make ongoing improvements to both their cybersecurity work and their work to education and communicate with partnerships, buyers, and customers.



Begin Your Journey to a Culture of Trust and Transparency

Creating a culture of trust and transparency is not a small feat. Taking small, meaningful steps over time will help you and your team move systematically down the path created by innovative organizations like Salesforce. Here are five ways you can get started on your journey today:

1. Articulate your perspective.

Audit your existing trust programs and take time to develop a clear, concise articulation of your company's perspective on trust and your cybersecurity commitments. If possible, partner with internal experts, like communications and go-to-market teams who can advise on best practices for telling stories to necessary internal and external audiences.

2. Give your most meaningful trust information a home.

Develop an official, accessible "home" for all of your company's critical cybersecurity information and documentation that can be leveraged to express your trust perspective to both company employees and buyers and customers. Create protocols to keep this space up-to-date, reflecting your programs, certifications, and commitments in real time.

3. Develop communication cadences that reinforce your trust message year-round.

Partner with internal experts to identify the channels that will help equip all employees to become trust and transparency advocates. Develop predictable cadences for interfacing with employees across the business, exposing them to the company's security posture and keeping them abreast of updates, learnings, and responses to potential incidents. As part of this work, ensure you are giving cross-functional teams the tools and language to communicate with their external partners, including buyers and customers, partners, the market, and even the media.

4. Forge bonds with cross-functional business leaders.

Implement practices that develop meaningful relationships with organization-wide peers who can help reinforce your message and educational efforts. Forging strong bonds with cross-functional business leaders, such as heads of sales and customer success, marketing, internal communications, legal, and finance, among others, will lead to mutual understanding of cybersecurity's role in their team's success. This understanding can be leveraged for improved communication, education, and even improved trust programs.

5. Give yourself an ROI dashboard.

Begin to build a cybersecurity dashboard by laying out the criteria that will help you connect your team's metrics with those across the business. Real-time access to these insights will enable you to communicate your team's value regularly with peers and organization-wide employees, and ultimately make continuous improvements to your trust programs and your educational work.

Shaping Company Culture: An Investment in Future Success

By developing the infrastructure, programs, and influence to create a culture of trust and transparency, Security and GRC leaders have the opportunity to lay a strong, self-sustaining foundation for the business's growth in the years to come.

The role of cybersecurity in business success will only increase as the world's technology continues its trajectory to become ever-more connected, and buyers demand ever-more transparency around the security of their data. The seeds planted by these leaders now will mean a significant competitive advantage in the future.

SAFEBASE

SafeBase is the customer trust platform that helps organizations increase buyer confidence through improved transparency, proactive communication, and real-time oversight and insights.

Visit safebase.io to learn more.

Book a Demo