SAFEBASE

Trends in Enterprise Trust 2024

Five focus areas to build and maintain customer trust

Table of contents

Introduction

This year marked a tipping point in the world of enterprise trust.

Highly visible breaches, like the MOVEit incident and the Okta breach, caused ripple effects across their enormous, interconnected customer bases. The AI hype cycle reached a fever pitch, as many companies raced to publicize their AI-enabled products — and to assure customers of its safety.

Meanwhile, the SEC filed an official complaint against software company SolarWinds following its high-profile 2020 cyberattack and charged its former CISO, Tim Brown, with fraud. The landmark case is the first time the securities commission has taken a public company to court following a cybersecurity incident — and the most visible instance in which a security officer has been deemed personally responsible. While the end of this story is still being written — and remains highly controversial — the story reflects the growing recognition of the impact of trust on business success.

These crucial events of 2023 solidified an emerging movement in cybersecurity: a move toward sustainable, scalable trust, built on a foundation of transparency and proactivity.

Five trends that will define trust in 2024

Five trends that will define trust in 2024

Business leaders across all industries now recognize the direct connection between trust and business success. To that end, many have spent the past year formalizing programs for building and maintaining trust with buyers and customers, including the development of new, trust-focused teams, as well as investments in communications efforts and more streamlined workflows between buyers and sellers.

In addition, company leaders have focused on driving mindset shifts for their organizations, empowering all employees with the resources they need to be stewards of trust and transparency. These efforts will become more embedded into the way organizations do business, moving customer trust and security from a nice-to-have to a foundational part of their business strategy.

As a trust-minded organization, there are five trends you need to know about in 2024 to ensure you stay ahead of your competition while building customer trust:

Brand-building through cybersecurity

The rise of the Chief Trust Officer

AI hype cycle giving way to guidance

Streamlining the security review experience

Operationalizing transparency and proactivity

Trend 1: Brand-building through cybersecurity

Trend 1:
Brand-building through cybersecurity

In the year to come, more enterprise companies will set their sights on promoting what their buyers care most about: cybersecurity. Enterprise buyers today recognize the potential impact of a third-party breach on their own company's safety and reputation and are now evaluating all software purchases based on a vendor's cybersecurity position.

These efforts may include far-reaching brand and PR campaigns (see: Dell touting its trustworthiness in the media), but will more commonly manifest in simply making cybersecurity more visible to potential buyers. This includes the development of a Trust & Safety center on a company's website or the inclusion of cybersecurity-focused content on a corporate blog.

It may also take the form of messaging provided to sales and customer success teams to relay to potential buyers, or an increased investment in information- and feedback-sharing between cybersecurity and go-to-market teams.

Your role in 2024

Investing in external marketing efforts focused on your cybersecurity stance will position your company to tell a stronger story about your commitment to security and transparency. Not only will this allow your company to put cybersecurity at the same level as a new product feature or a high-profile customer testimonial, it will also help develop a sense of trust from the very beginning of your relationship with your buyers.

If you haven't already considered how your organization can bring cybersecurity front and center for your brand, look to companies like HubSpot, OpenAI, and Asana for inspiration. Each has developed a robust web presence highlighting their security position and making their cybersecurity resources easily accessible. To take it a step further, Twilio has created a series of content focused on educating its audience on security-related topics, aligning its brand with security and trust.

By moving cybersecurity from the last step in the sales cycle to a front-and-center value proposition of your product, you'll position your organization to build trust more quickly and meaningfully than ever before.

Trend 2: Rise of the Chief Trust Officer

Trend 2:
Rise of the Chief Trust Officer

In the past year, the increase of corporate leadership positions directly responsible for customer trust has continued its already rapid trajectory. This role is often dubbed the “Chief Trust Officer,” or “CTrO” for short.

Organizations like Workday, Salesforce, Atlassian, SAP, and Telus have all created roles in their C-suites to oversee the company’s initiatives to drive trust with buyers. They often act as the customer-facing representative of the company’s security and privacy programs, charged with communicating the organization’s trustworthiness to buyers and maintaining market confidence in the company’s security capabilities. Most Chief Trust Officers have a background in data and cybersecurity, but are accountable for bridging the gap between cybersecurity and the company’s business goals.

Regardless of their particular scope, one key theme for all of these Chief Trust Officers is a focus on transparency. This emphasis is defined as “the need to stay open... and maintain constant communication with customers,” according to Elena Kvochko, Chief Trust Officer at SAP. As a result, these officers must think beyond the technical aspects of security, bringing a level of communications, customer relations, and business strategy skills to the work as well.

An annual Deloitte study reveals that the number of organizations with a “Chief Trust Officer” has nearly tripled in the past year.

Your role in 2024

The year to come is likely to see a swift increase in the appointment of trust-focused leaders across the business landscape. According to Deloitte, nearly half of the organizations that don't yet have a leader responsible for trust indicate that they will in the year to come.

Whether your company is ready to install a trust-focused leader to the C-suite or not, now is the time to consider the accountability structure your organization has in place around trust. Is anyone directly responsible for the level of trust your organization builds with buyers and customers? How are you measuring and reporting on the success of those efforts? Do you have a clear line of sight to the relationship between trust and your business objectives?

In 2024, ensure your company is set up to sustainably build trust by making meaningful shifts to your team's structure and their focus areas.

> "I do believe that the demand for issues around trust will continue to grow in the marketplace so it's very much my personal hope that more companies will embrace it and establish a trust officer equivalent.
>
> **Elena Kvochko**
> Chief Trust Officer, SAP

Trend 3: AI hype cycle gives way to guidance

Trend 3:
AI hype cycle gives way to guidance

Following the unprecedented launch of OpenAI's ChatGPT platform in November 2022, the topic of artificial intelligence has overtaken the corporate world. Overnight, organizations in every industry scrambled to not only embed AI into their products and services, but also to make their markets aware of these new capabilities.

While cybersecurity leaders will continue to look to federal agencies, including the Cybersecurity & Infrastructure Security Agency (CISA) and the White House for guidance and support, your organization needs to develop your own guidelines aimed at mitigating risk and increasing transparency around safe use of AI.

The proliferation of AI has quickly given way to a host of questions for cybersecurity leaders focused on risk management and trust, like:

How can we reduce the risks inherent in the use of AI while still getting the most out of the technology?

How can we avoid misuse of AI as it becomes a major part of our vendor ecosystem?

How can we maintain the trusting relationships we've built with our buyers as we begin or continue to offer AI-enabled products and services?

Your role in 2024

As AI continues to become a meaningful part of our business relationships in the year to come, consider the foundations your team is laying for both mitigating risks and maintaining trust with buyers and customers. Not only do you need to partner with your legal team to develop proper guidelines for internal use, your organization also needs documented security information to share with buyers and customers during a security assessment.

This information should err on the side of transparency, as buying organizations aim to mitigate the ever-growing list of risks AI poses to cybersecurity. Start by developing pointed questions to ask potential AI vendors to assess the safety of their products and ensure you're prepared to answer the same questions for your own buyers.

On the next page, we've provided a list of the top questions you'll want to ensure you've answered in order to maintain trust with AI buyers.

Top eleven questions to answer about your company's AI security

As your company begins to sell AI-enabled capabilities, buyers will seek assurances that these products are secure. Make sure you've answered the top eleven questions on AI security and stored the responses so they're easily accessible during a security review.

1. **Do the organization's personnel and partners receive AI risk management training to enable them to perform their duties and responsibilities consistent with related policies, procedures, and agreements?**
2. **Will customer data be used to train artificial intelligence, machine learning, automation, or deep learning?**
3. **Does the organization have an AI Development and Management Policy?**
4. **Does the organization have policies and procedures in place to define and differentiate roles and responsibilities for human-AI configurations and oversight of AI systems?**
5. **Who is the third-party AI technology behind your product/service?**

6. **Has the third-party AI processor been appropriately vetted for risk? If so, what certifications have they obtained?**

7. **Does the organization implement post-deployment AI system monitoring, including mechanisms for capturing and evaluating user input and other relevant AI actors, appeal and override, decommissioning, incident response, recovery, and change management?**

8. **Does the organization communicate incidents and errors to relevant AI actors and affected communities and follow documented processes for tracking, responding to, and recovering from incidents and errors?**

9. **Does your company engage with generative AI/AGI tools internally or throughout your company's product line?**

10. **If generative AI/AGI is incorporated into the product, please describe any governance policies or procedures.**

11. **Describe the controls in place to ensure our data is transmitted securely and is logically and/or physically segmented from those of other customers.**

Trend 4: Streamlining the security review experience

Trend 4:
Streamlining the security review experience

As trust has solidified its position at the heart of business success, so has the traditional third-party risk assessment process. Traditionally, this assessment process has been dominated by the dreaded security questionnaire — a manual, tedious exercise for all parties. For years, organizations have lamented the inefficiencies inherent in this process, including answering similar questions time and again, too-short SLAs from buyers, and the back-and-forth of sourcing answers from a handful of internal resources.

In 2024, recognizing the permanence of the risk assessment in buying transactions, more and more organizations will implement security questionnaire technology to improve the user experience on both the selling and the buying side of the process.

Sellers will seek to build programs that help them more effectively communicate their security posture without the manual effort of searching for answers, writing nuanced responses, and even reading responses.

On the buying side, organizations will aim to apply AI to third-party risk assessments, leveraging technology to parse through reams of documentation to quickly identify risks and mitigate the need for a security questionnaire.

Trend 4:
Streamlining the security review experience

Your role in 2024

When you look to the year to come, take stock of the typical security review process your company engages in as buyers conduct their third-party due diligence. What are the recurring friction points you could streamline to make the process faster, less cumbersome, and ultimately more scalable for both your teams and your buyers?

By employing a security review software, your company will be able to shorten sales cycles, have greater control for both buyers and sellers, and see a reduction in the back-and-forth among internal partners and stakeholders. As your business grows, set your team up to build trust with less friction — and give your buyers a differentiated experience as well.

As you look to bring in technology to help streamline security reviews, here are a few things to look for to ensure the process will be more approachable for both organizations involved:

Does the software aggregate security documentation into one sharable repository with a templated layout that's familiar to buyers?

Does the technology support guided security reviews to answer buyer questions before they ask them?

What integrations are available to streamline workflows among teams, as well as provide transparency for cross-functional stakeholders, and visibility into both activities and the impact of those activities?

Does the technology use AI for improved search and to help generate security questionnaire responses based on your existing wealth of knowledge?

Trend 5: Operationalizing transparency and proactivity

Trend 5:
Operationalizing transparency and proactivity

As the spotlight this year turned to the fallout of high-profile cybersecurity incidents, more and more leaders have come to the same conclusion: when it comes to building and maintaining relationships with customers, buyers, partners, stakeholders, and even the media, a lack of transparency is a losing proposition.

To that end, companies will continue investing in formal programs to help them be more transparent and proactive with buyers and customers, following the examples set by organizations like Salesforce. This includes the development of specific communications programs aimed at keeping buyers and customers informed in the wake of a third-party breach, or even to inform them that they haven't been impacted.

Organizations will also put rigor behind their transparency and proactivity efforts by taking steps to arm all employees with easy access to the company's security information. That may include training for sales and customer-facing teams, or the development of resources to help all staff convey the company's security posture in an easily-understandable, personalized way.

This past October, LinkedIn announced the release of a new AI-based chatbot that helps employees and vendors get answers to cybersecurity questions in seconds. The company's CISO, Geoff Belknap, indicated that removing the barriers to understanding internal policies will help employees implement them properly, and more effectively communicate with buyers and customers. For business partners, the chatbot provides "more consistent security information" far more quickly than when they pose their questions to humans. These efforts improve transparency and clarity around LinkedIn's security posture for its most critical stakeholders.

In the year to come, more organizations will make investments in technology that makes communication with employees, partners, customers, and buyers easier and more consistent, removing the friction inherent in conveying security information between companies. As a result, these companies will lay a foundation of transparency and proactivity — a major step toward long-lasting enterprise trust.

Your role in 2024

As you think about operationalizing transparency and proactivity, how would you rate your company's efforts to share security information accurately and quickly? Are there hurdles preventing stakeholders from getting all the information they need? With an orientation toward transparency and proactivity, you may be able to drive trust in a more sustainable way.

Consider the communications channels you can leverage to get security information in front of buyers before they ask, including your website, your front line spokespeople, and ongoing communication like email. Also consider creating clear guidance for the extent of the information you're willing to share, striking the right balance between privacy and transparency.

Transparency and proactivity are the crux of the equation when it comes to building and maintaining enterprise trust. Make sure you're optimizing for these two principles to support your company's growth in 2024.

Investing in a future of transparency

Investing in a future of transparency

The events of the past year have laid bare the direct connection between trust and business success. Forward-thinking organizations have already begun to make investments that will help them build and maintain trust with their enterprise customers in a scalable way.

As your organization looks to build customer trust, implementing these five trends will help you stay ahead of the competition:

Brand-building through cybersecurity

The rise of the Chief Trust Officer

AI hype cycle giving way to guidance

Streamlining the security review experience

Operationalizing transparency and proactivity

In 2024, these investments will find their place as permanent fixtures for trust-minded organizations and will set you up to build and maintain trust and transparency for years to come.

SafeBase is the scalable Trust Center that automates the security review process between buyers and sellers. With a SafeBase Trust Center, companies can seamlessly share sensitive security documentation with buyers and customers, including streamlining the NDA signing process by integrating with your CRM and data warehouse.

If you're ready to take back the time your team spends on security questionnaires, create a better buying experience, and position security as the revenue-driver it is, get in touch with us.

SAFEBASE

Get a demo