REPORT

The Cybersecurity Trust Reality in 2026

Insights from a vendor-agnostic survey of 5,000 IT and security leaders

SOPHOS

Introduction

When organizations select a cybersecurity vendor, they're placing critical operational resilience — people, data, and revenue — into that supplier's hands.

Yet despite this reliance, most organizations lack confidence in the vendors they depend on to keep them secure, according to new Sophos research.

To understand the reality of cybersecurity trust, Sophos commissioned an independent, vendor-agnostic global survey of 5,000 IT and security decision-makers across 17 countries. Conducted by Vanson Bourne, a specialist research firm, the survey provides a statistically significant, real-world picture of how trust is built, and lost, between cybersecurity buyers and vendors.

5,000

IT and security leaders across 17 countries participated in a vendor-agnostic global survey

Key learnings

Trust is lacking: Only 5% of IT leaders say that both they and their organization have full trust in their cybersecurity vendors.

Verified evidence is a primary driver of trust: IT teams and senior leadership agree that verifiable artifacts of cybersecurity maturity are the most significant indicator of trustworthiness.

Assessing vendor trustworthiness remains challenging: 79% of organizations find it challenging to assess the trustworthiness of new cybersecurity providers, while 62% find it challenging for their existing vendors. Respondents cited several factors that reduced confidence in vendors, chief among them being because information the vendor provided wasn't factual or detailed enough.

This lack of trust has consequences: 51% of respondents say that lack of trust leads to anxiety that the organization is more likely to experience a significant cyber incident.

Practitioners and leadership don't often agree: 78% of respondents say that their IT team and senior leadership team/board differ in opinion on the trustworthiness of their organization's cybersecurity vendors. Nearly one-third of companies who responded to Sophos' survey say this disagreement happens "often."

Trustworthiness is difficult to assess

Only 5% of IT leaders say that both they and their organization have full trust in their cybersecurity vendors.

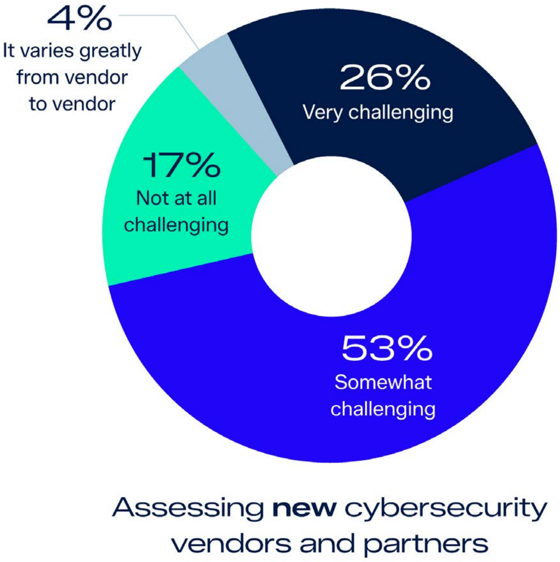
When you're looking to your cybersecurity vendor to keep your network secure and operations up and running, trust is key. Cybersecurity providers are the ones defending your business 24/7, even on nights and weekends, and when IT team members are on vacation. For small business owners, they may not even have dedicated IT staff, and their cybersecurity products or services can act like an employee of their own.

Before organizations can decide who to trust, they face an even more fundamental challenge: Simply evaluating a vendor's trustworthiness in the first place.

According to the survey, 79% of respondents say it's challenging to assess the trustworthiness of new cybersecurity vendors or partners, highlighting a widespread struggle to compare products, validate claims, and understand whether a prospective provider can truly safeguard the business. 62% also struggle to evaluate the trustworthiness of the vendors they're already working with — a signal that trust gaps don't disappear once a contract is signed (Figure 1).

79%

of companies surveyed said it's challenging to assess the trustworthiness of new cybersecurity vendors/partners.



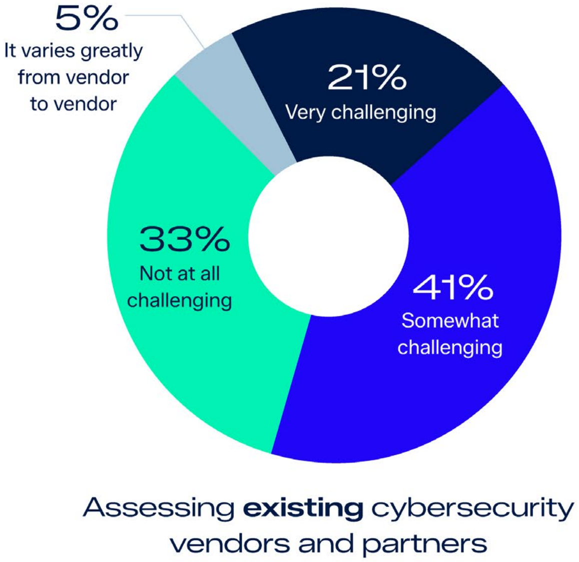


Figure 1: In general, how challenging, if at all, is it for your organization to assess the trustworthiness of cybersecurity vendors and partners? n=5,000

Barriers to assessing trust

Respondents pointed to several barriers to trust — most rooted in transparency. Many struggle to interpret vendor claims, assess technical details, or find the information they need to make confident decisions.

Nearly half (47%) say the information vendors provide isn't factual or detailed enough, and 45% find that information hard to interpret or understand. A further 43% admit they lack the skills or knowledge to assess vendors effectively, 41% encounter conflicting information, and 38% struggle simply to find the information they need (Figure 2).

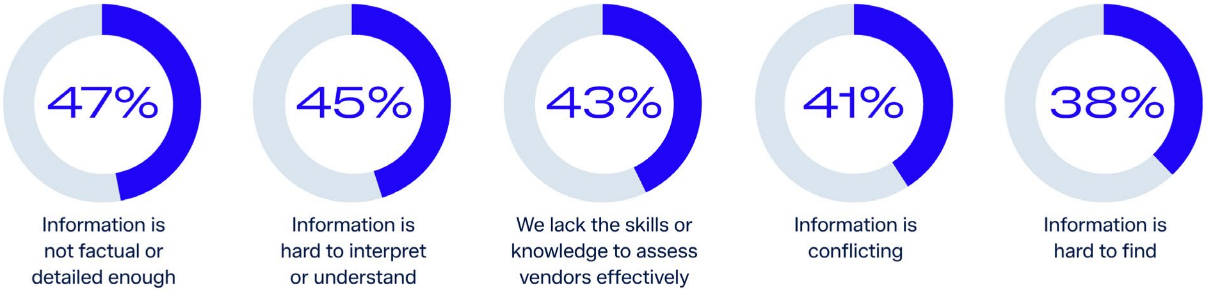


Figure 2: Why does your organization find it difficult to assess the trustworthiness of cybersecurity vendors? n=4,483

The biggest area of difference between small businesses (sub-250 employees) and enterprises (1,000+ employees) is that SMBs are much more likely to lack the skills or knowledge needed to assess vendor trustworthiness effectively — SMBs chose that as an issue 8% more than those respondents at enterprises (Figure 3).

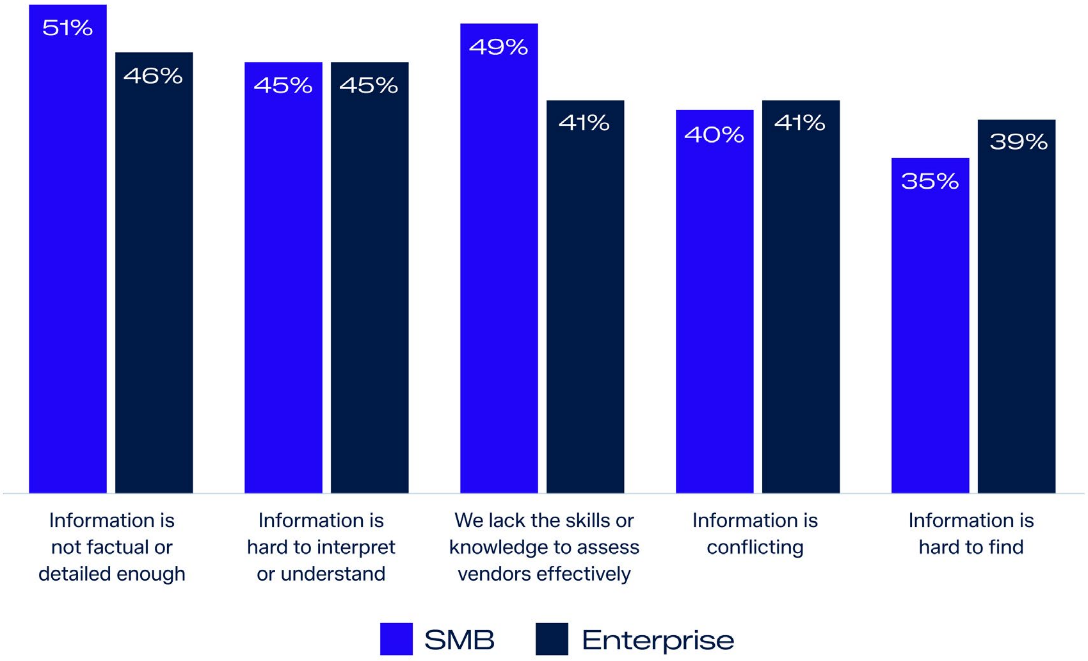


Figure 3: Why does your organization find it difficult to assess the trustworthiness of cybersecurity vendors? n=504 (SMBs), 2,260 (Enterprises).

Lack of trust has consequences

This research quantifies the impact that a lack of trust between a security vendor and their customers is a significant issue in multiple ways. When asked about the impact of not having full trust in their cybersecurity vendors, respondents highlighted a mix of emotional and operational consequences:

- **51%** report increased concern that their organization may experience a significant cyber incident.
- **45%** say it makes them more likely to switch vendors — an expensive and disruptive process for most organizations.
- **42%** see increased oversight requirements.
- **41%** report reduced peace of mind regarding their cybersecurity posture.
- **38%** report concern that they or their organization may have made an incorrect vendor selection.

These reported impacts add to the operational demands already placed on IT and cybersecurity teams.

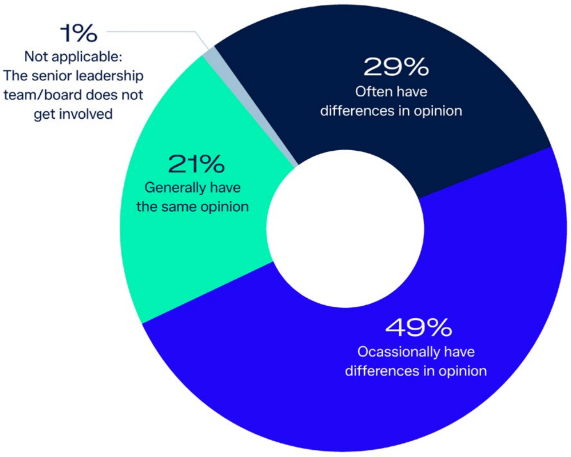
Divergent assessments between IT and leadership

Another critical challenge is misalignment between the people using cybersecurity tools day-to-day and those signing off on the contracts. 78% of respondents say their IT team and senior leadership team or board differ in opinion on the trustworthiness of their cybersecurity vendors, and nearly a third say those disagreements happen "often" (Figure 4).

Respondents indicated that senior leadership remains highly involved in purchasing decisions. Only 1% of organizations reported that the board or senior leadership play no role in cybersecurity purchasing decisions.

1%

of organizations surveyed that said senior leadership plays no role in cybersecurity purchasing decisions.



Differences of opinion in the trustworthiness of vendors
(IT team vs. senior leadership/board)

Figure 4: Do the IT team and the senior leadership team/ board have differences of opinion on the trustworthiness of your organization's cybersecurity vendors? n=5,000.

How to build cybersecurity trust

Respondents indicated that transparent, evidence-based security practices are central to building trust. Organizations want vendors who enable trust through openness, clarity, and evidence-backed security practices.

Across both senior leadership and IT teams, “verifiable artifacts indicative of cybersecurity maturity” ranked as the top driver of trust in cybersecurity vendors. These types of evidence include bug bounty programs, a public Trust Center, advisories detailing vulnerabilities in their products (along with how they were remediated), third-party assessments, and certifications.

“Transparency and timely communications during incidents and disclosures” also ranked as the secod largest driver for SMT members and third among IT team members.

Drivers of trust in cybersecurity vendors

Drivers	SMT/ board	IT/ cyber team	Influencing factors
Primary drivers	#1	#1	Verifiable artifacts indicative of cybersecurity maturity e.g., bug bounty, Trust Center, advisories, 3rd party assessments, certifications
	#2	#3	Transparency and timely communications during incidents and disclosures
	#3	#4	Expert commentary following major cyber incidents e.g., quotes in press, on TV
	#4	#2	Consistent delivery of high-quality cybersecurity services and products
	#5	#5	Performance in analyst reports e.g., Gartner Magic Quadrant
Secondary drivers	#6	#9	Transparency into internal security procedures
	#7	#7	Performance in independent tests e.g., MITRE, SE Labs
	#8	#6	Responsive and reliable support
	#9	#8	Recommendation from your reseller/cybersecurity partner
Tertiary drivers	#10	#13	Caliber of threat research publications
	#11	#12	Coverage in financial and business press
	#12	#11	Experience of others (peers/customers)
	#13	#10	Personal experience

What factors are/would most influence the senior leadership/board's level of trust in a cybersecurity vendor? Responses ranked first
What factors are/would most influence the IT/cybersecurity team's level of trust in a cybersecurity vendor? Responses ranked first

Sophos' commitment to earning our customers' and partners' trust

At Sophos, we understand that trust is built — not claimed — and we work to earn it every day through transparency, integrity, and a steadfast commitment to protecting security and privacy.

At the heart of our efforts is the Sophos Trust Center where we publish security advisories, document product vulnerabilities and remediations, outline our compliance posture, and share how we protect customer data.

This transparency is also demonstrated in Sophos X-Ops' Pacific Rim investigation, which publicly documented a five-year campaign by China-based threat actors and shared detailed tactics, techniques, and procedures (TTPs), indicators of compromise (IOCs), and defensive guidance to help organizations strengthen resilience industry-wide.

By exposing sophisticated nation-state activity, working with governments and other vendors, and being candid about both strengths and weaknesses, Sophos reinforces that trust is something earned daily through honesty, accountability, and a commitment to safeguarding the broader digital ecosystem.

Learn more

For further information on our commitment to enabling trust and the resources we provide to help evaluate trust in Sophos, visit the Trust Center or speak to your Sophos partner or representative.

SOPHOS

For further information visit the Trust Center or speak to your Sophos partner or representative.

United Kingdom and Worldwide Sales Tel: +44 (0)8447 671131 Email: sales@sophos.com	**Australia and New Zealand Sales** Tel: +61 2 9409 9100 Email: sales@sophos.com.au
North America Sales Toll Free: 1-866-866-2802 Email: nasales@sophos.com	**Asia Sales** Tel: +65 62244168 Email: salesasia@sophos.com