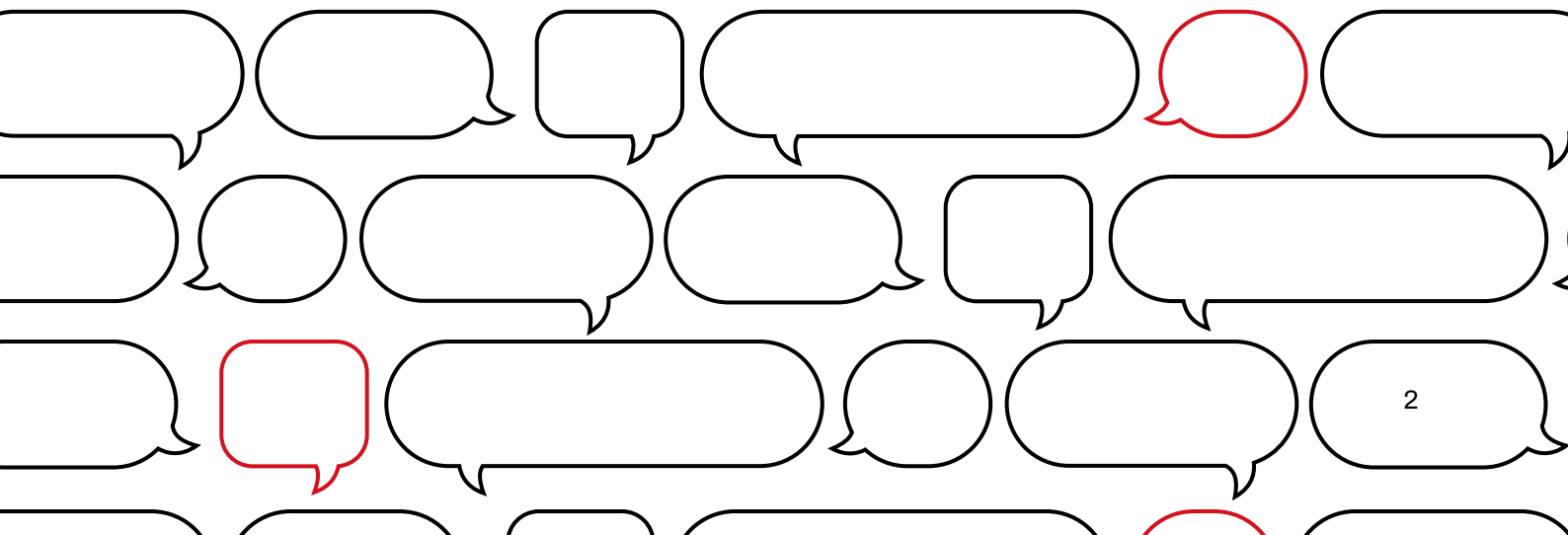
THE STATE OF CYBER SECURITY COMMUNICATION

MISCOMMUNICATION, RISK AND THE ROLE OF PR

whiteoaks
INTERNATIONAL

Contents



Introduction

In cyber security, communication shapes how buyers understand risk, compare solutions and make decisions that can affect operations, compliance, finances and brand reputation.

Yet cyber security is difficult to communicate well. The market is highly competitive and technical, the threat environment is constantly changing and buyers are not always able to assess every product claim in detail.

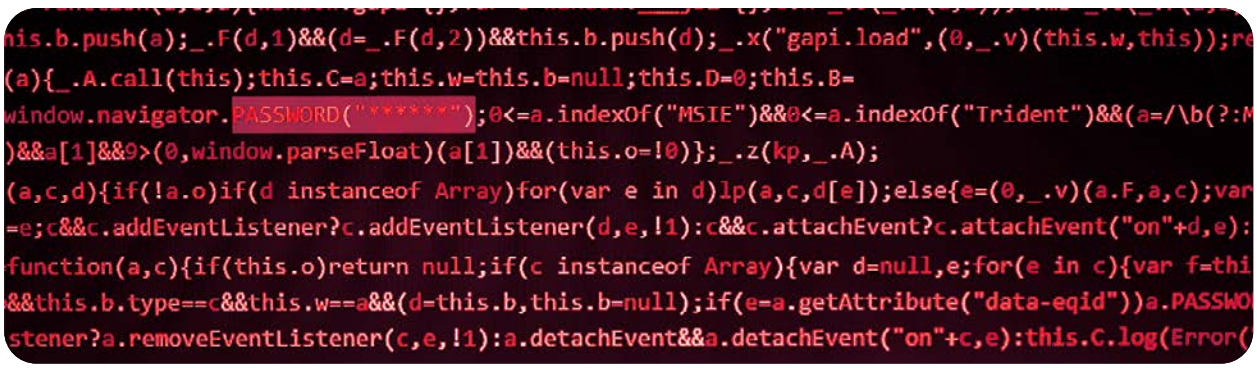
> When PR and marketing are unclear, oversimplified or overconfident, they can distort expectations and widen the gap between what buyers believe they are getting and what a solution can realistically deliver.

One recurring problem is language that implies certainty where none exists. Claims may overstate protection, simplify technical concepts too far or present nuanced capabilities in absolute terms. As these messages move across website pages, media coverage, social media posts and sales conversations, the gap between presentation and performance can grow, increasing the potential for commercial and reputational risks.

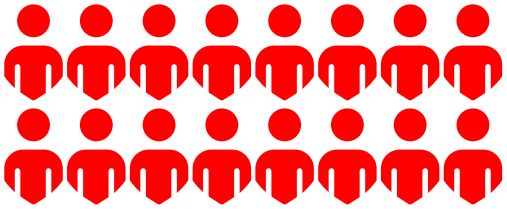
Over time, miscommunication can also affect the wider sector by contributing to scepticism and reducing trust in cyber marketing more broadly.

Despite years of discussion, many in the industry feel little has changed. Miscommunication remains a recurring concern, with implications not only for individual organisations, but also for the credibility of the sector as a whole.

To understand the issue in more detail, Whiteoaks conducted original research with Censuswide among 152 senior marketing, PR and communications professionals working in UK cyber security organisations. The research took place between 12–17 February 2026 and represented a balanced mix of company sizes. The research was supported by a closed, in-person roundtable with senior marketing and communications leaders, whose perspectives are reflected throughout this report.



Snapshot of key findings

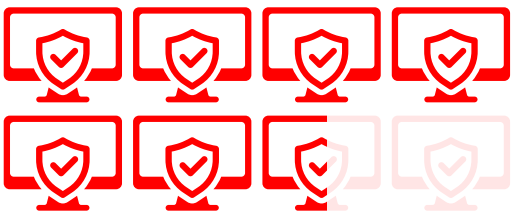


99% **report using terms such as “secure”, “100% protection” or “fully protected”.**

Yet 89% acknowledge that this language may give the impression of complete protection.

47% **say their organisation has experienced commercial or reputational impact** linked to inaccurate or overly simplified messaging, including lost opportunities, reduced confidence and negative brand perception.

75% **routinely include disclaimers, plain English explanations or risk guidance in marketing materials.** However, only 23% say all claims are consistently checked by legal teams before publication.



86% **agree clear and responsible communication can significantly increase customer trust.**

86% **believe cyber industry communications practitioners should achieve a cyber-related accreditation.**

94% **say the industry needs clearer communication standards or a code of practice.**

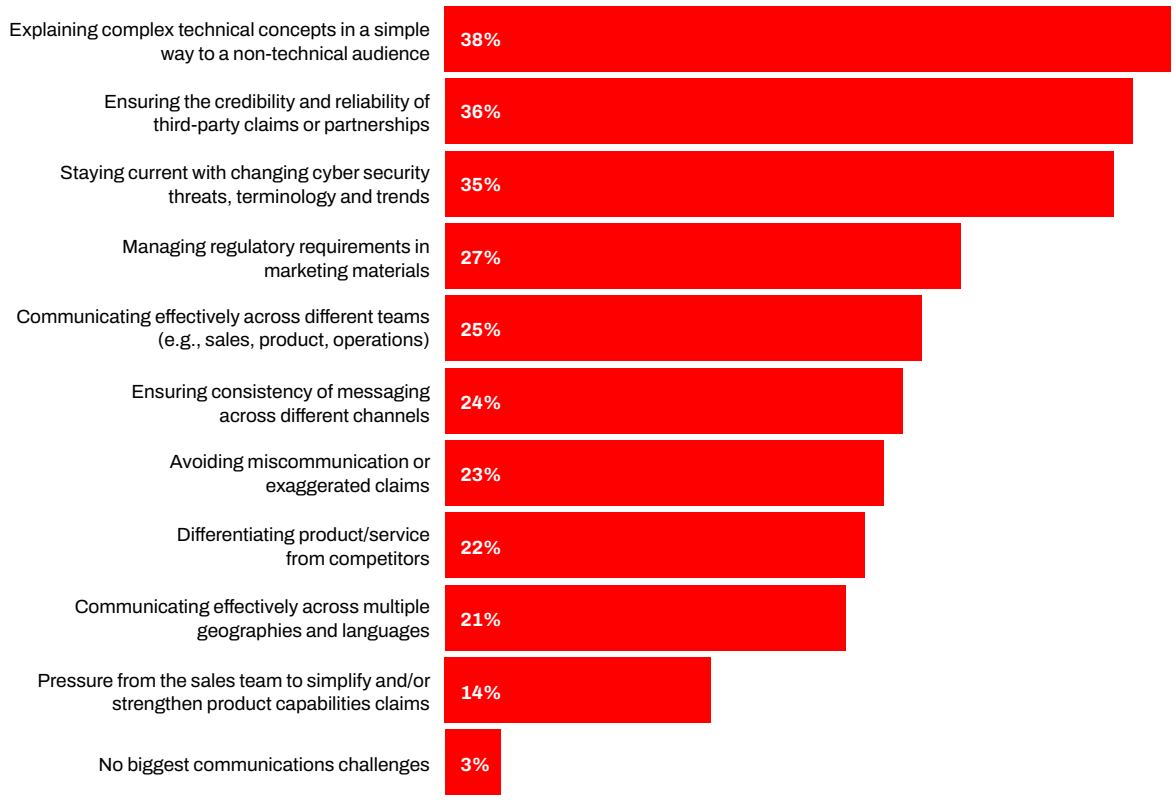
The extent of the miscommunication challenge

Cyber security messaging has to translate technical capability into business relevance for very different audiences, from specialists who expect technical detail to senior decision-makers who need to understand organisational impact without unnecessary jargon.

At the same time, providers are under pressure to stand out in a crowded and highly competitive market, with 22% of research respondents identifying differentiation from competitors as one of the biggest communication challenges in the sector. That may encourage stronger and more definitive claims, even when the reality is more nuanced.

The research shows that these pressures are felt across the communications process. The most common challenges include explaining complex technical concepts to non-technical audiences (38%), followed by checking the credibility of third-party claims or partnerships (36%) and staying current with changing threats, terminology and trends (35%). A further 27% point to managing regulatory requirements in marketing materials, while 25% cite the challenge of communicating effectively across different teams.

What are the biggest communication challenges you face when marketing cyber security products or services?

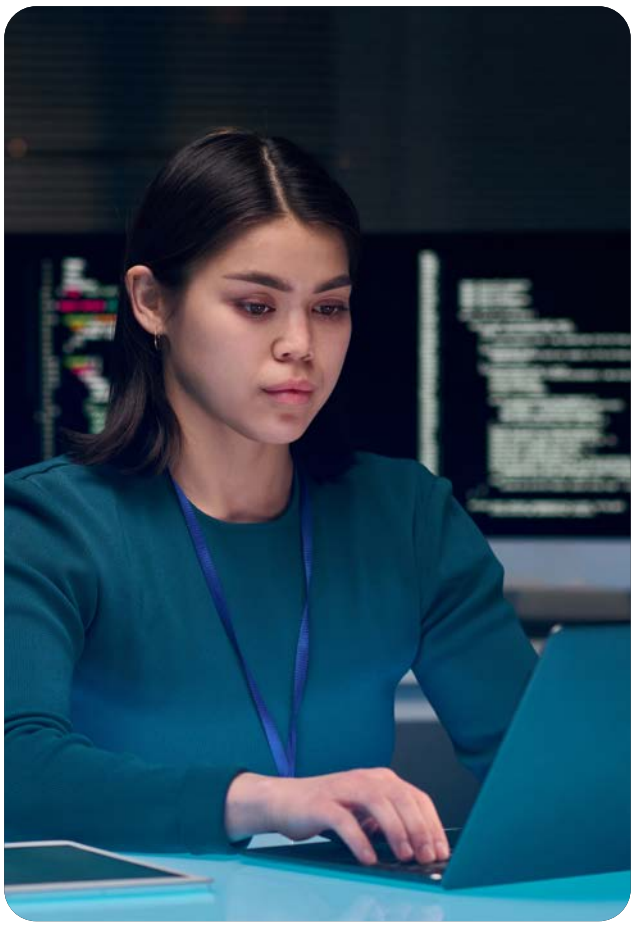


Rather than pointing to one dominant issue, the responses show pressure-points across technical explanation, evidence, internal alignment and market positioning. A message may begin as a technically accurate description of capability, then become shorter, broader or more definitive as it is adapted for different audiences or commercial conversations.

This helps explain why cyber security communication can be difficult to manage consistently. The same proposition may need to work for technical experts, procurement teams, senior decision-makers and board-level audiences.

Each group may need a different level of detail, but each version still needs to reflect the same product reality.

In practice, that might mean building a non-technical decision-maker version, a technical evaluator version and a financial stakeholder version of the same proposition. The aim is not to create competing narratives, but to give each audience the information they need without changing the underlying meaning.



"People are making bold claims, and as a marketer, you are trying to keep up while also being honest. Ultimately, it comes down to delivering a good service to customers. If you are dishonest upfront, people are going to be disappointed further down the line, and that creates distrust.

That is one of the biggest communications challenges in cyber security: getting the right message to the right audience at the right time. The audience is incredibly diverse, so you need to convince different stakeholders that you have the right solution, without oversimplifying the message so much that the specificity is lost.

That is very much the role of marketing in cyber security. You are the translator between the technical teams, the commercial teams, and the people who ultimately need to understand the business value. Buyers may have been mis-sold to, locked into contracts or faced unexpected price increases, so authenticity is essential to building trust and avoiding frustration towards suppliers."

Michelle Caulfield-Harris
Marketing Director at Red Helix

When language may create false certainty

One of the clearest examples of miscommunication challenges is the language used to describe cyber security protection.

Almost all respondents (99%) report using terms such as “secure”, “100% protection”, “total security” or “fully protected” in marketing materials. Yet 89% acknowledge that this kind of language may give the impression that a product or service provides complete protection against cyber-attacks.

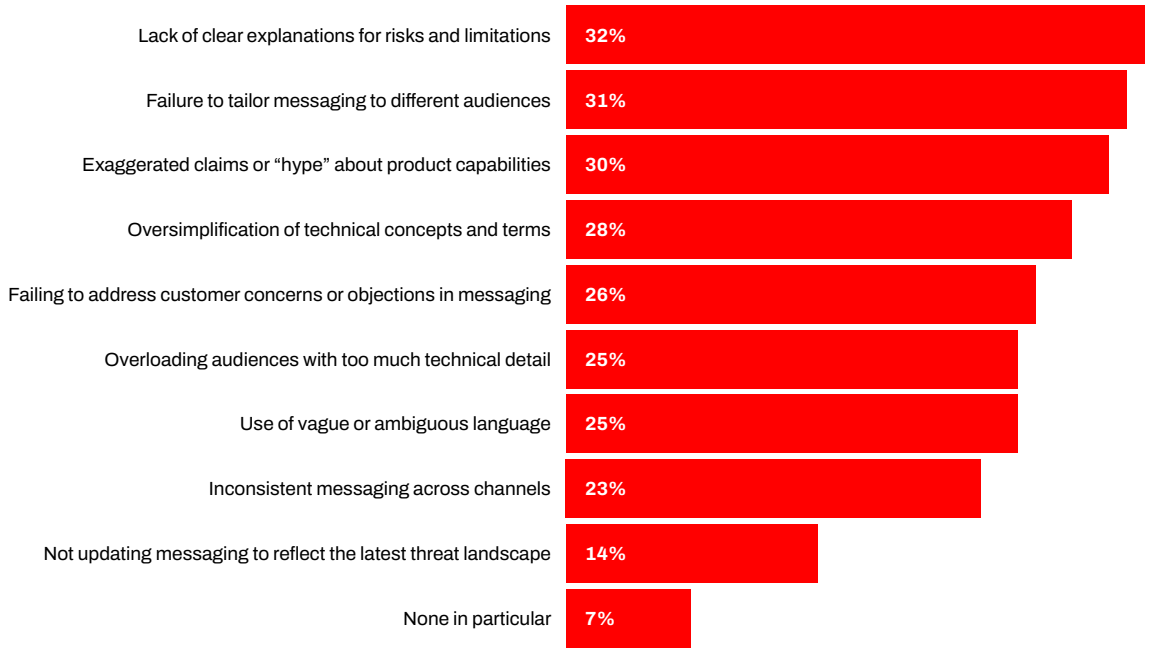
That creates a gap between intent and interpretation. A provider may use these terms to make a proposition feel confident and easy to understand. However, a buyer may read them as a stronger promise, particularly if they do not have the technical knowledge to challenge what is being implied.

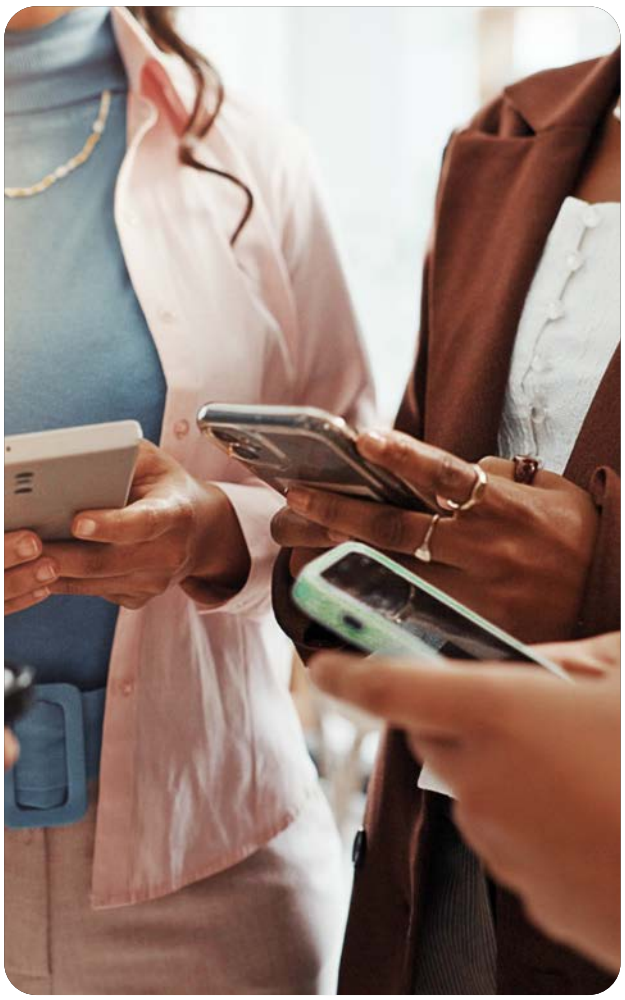
Cyber security can reduce exposure and strengthen resilience, but it cannot remove risk entirely. People, processes, behaviours and changing threat conditions all influence how protected an organisation really is. When language suggests complete protection, it may create expectations that no solution can meet.

A more grounded approach would focus on what a solution can realistically deliver. Rather than implying complete protection, messaging should be framed around risk reduction, mitigation, resilience, layers of defence, specific use cases, evidenced capabilities and the limitations as well as the benefits of a solution.

This suggests respondents perceive the issue to extend beyond isolated cases, reflecting a broader communication challenge shaped by the pressure to simplify complex capabilities and differentiate quickly.

What, if anything, do you think are the most common pitfalls in cyber security communications that lead to miscommunication?





The research also shows that miscommunication is not only caused by the most obvious claims. The most common pitfall is unclear explanation of risk and limitations, cited by nearly one-in-three (32%) respondents. This is followed by failure to tailor messaging to different audiences (31%), exaggerated capability claims (30%) and oversimplifying technical concepts (28%). A quarter also point to overloading audiences with technical detail (25%) and vague or ambiguous language (25%).

The findings also show that overclaiming is widely recognised across the sector.

Seven-in-ten (70%) respondents say they have either been involved in, or are aware of, marketing or PR content that included unsubstantiated, misleading or excessive claims.

More than half (51%) have seen this happen, while nearly a third (30%) have been directly involved.

This suggests respondents perceive the issue to extend beyond isolated cases, reflecting a broader communication challenge shaped by the pressure to simplify complex capabilities and differentiate quickly.

"Too often, cyber resilience is communicated as though technology alone can make an organisation 100% secure. It cannot. People, processes and behaviours all create risk too, so when brands oversell what technology can do, they create more confusion and ultimately more risk.

We need to get better at explaining cyber resilience in a way that helps people take the right action. If I buy a car, nobody lifts the bonnet and explains exactly how the engine works. They tell me the benefits and what I need to know to make the right decision. Yet in cyber, we often move quickly into threat landscapes, end-to-end encryption and technical terminology that does not always mean anything in context to the buyer.

For SME business owners in particular, the call to action should not be to learn every detail of cyber resilience. We do not teach every business owner every type of law; we teach them when to hire a lawyer. True cyber resilience needs the same kind of practical communication, focused on risk, relevance and action. That includes consideration also of staff training, policy, and practicing an incident response and its recovery."

Joanna Goddard, Chief Experience Officer
National Ambassador Programme at National Cyber Resilience Centre Group

The cost of miscommunication

Miscommunication is not purely a language issue. The research respondents report commercial and reputational consequences associated with inaccurate or oversimplified messaging.

Nearly half (47%) of respondents say their organisation has experienced commercial or reputational impact linked to inaccurate or oversimplified messaging.

Reported impacts include lost opportunities, reduced confidence, negative perception, lost clients, missed deals, reduced customer satisfaction, legal exposure and negative media coverage.

Respondents also recognise the wider risks. Nearly three quarters (72%) agree that oversimplification in marketing materials may mislead potential clients, while 77% agree that poor communication could lead to lost business opportunities.

This is particularly important in cyber security because buyers are not making low-risk decisions. They are making choices that can affect operational resilience, regulatory exposure and reputation. If they misunderstand what a product can realistically deliver, they may make decisions based on unrealistic assumptions about protection levels.

Research respondents also recognise potential reputational and legal risks.

More than three quarters (78%) agree that miscommunication can damage reputation, while 72% agree exaggerated or fluffy language can increase legal risk.

At the same time, commercial pressure appears to be one factor shaping how capabilities are described. Six-in-ten (61%) respondents say commercial pressures influence how capabilities are described, with around half (51%) indicating this happens to a moderate extent and another 10% saying it happens to large extent.

That combination creates a difficult environment for communications teams. The findings suggest the need to stand out may push messaging towards stronger claims, while the consequences of those claims are becoming harder to ignore.

This points to the need to communicate cyber security as risk management rather than total protection. Responsible messaging should explain the risk being addressed, how the solution helps reduce that risk, what it does not solve and what residual risk remains. The stronger the claim, the stronger the evidence needs to be.

"Legal liability arises when a claim does not match what is actually delivered. In more established sectors, such as law, marketing is very controlled and disciplined. Cyber security is still earlier in that development, and there is a gap between executive board decision-making and the people trying to provide good advice around cyber resilience.

Data protection law has tried to future-proof the security obligation as much as possible, because what is considered appropriate security changes over time. Cyber resilience is on a similar trajectory, but it is still at an earlier stage. That creates uncertainty around what should be expected of providers.

There are useful lessons from other areas of risk. In health and safety, individual directors can be prosecuted, and that has had a real impact on board behaviour. Similar conversations happened when GDPR came in, and personal responsibility may become a bigger part of cyber risk in future. Clearer guidance would help reduce ambiguity and give organisations a better understanding of the standards they should be able to rely on."

Laura Irvine
Head of Regulatory Law at Davidson Chalmers Stewart

Why current safeguards may not be enough

Many organisations have checks in place, but the research suggests they are not being applied consistently enough to prevent inaccurate or oversimplified messaging from reaching the market.

Confidence in messaging is high. Most respondents (86%) say they are confident their company's marketing and PR content accurately reflects product capabilities, including 50% who strongly agree. Yet that confidence sits alongside inconsistent legal review processes and reported misunderstanding among target audiences.

This suggests organisations may be assessing accuracy from an internal perspective, rather than from the buyer's point of view. A claim may reflect product capability, but still be too broad, too compressed or too easily misread once it reaches the market.

Only 23% of respondents say all claims are checked by legal teams before publication.

A further 36% say claims are often checked by legal teams and 30% say this happens sometimes.

Technical collaboration is more common as 33% say they always work with technical teams to ensure messaging reflects product capabilities. A further 43% say this happens often and 18% say it happens sometimes.

That technical input is important, but it does not fully address the communication risk. A claim can be accurate from a product perspective, but still be interpreted too broadly by a buyer. The more a claim is shortened, simplified or adapted for marketing, the more important it becomes to check not only whether it is accurate, but whether it is likely to be understood as intended.

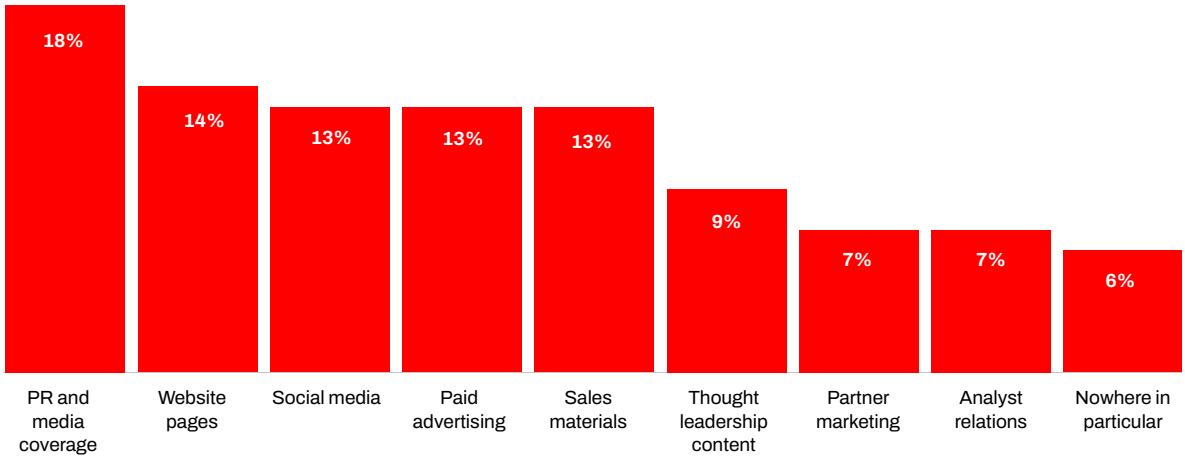
Many teams are also trying to add more context.

Three quarters (75%) of respondents say they routinely include disclaimers, plain English explanations or risk guidance in marketing materials. Yet misunderstanding remains common, with 30% saying messaging is often misunderstood, 42% saying this happens sometimes and 10% saying it is always misunderstood.

The findings suggest that disclaimers and explanatory content have value, but they may not be enough to offset claims that are too broad or too absolute in the first place. A qualifying line may reduce risk, but it will not always correct the impression created by a headline, sales message or product claim that implies more than the solution can deliver.

The same issue applies across channels. Respondents say accuracy is most likely to be lost in PR and media coverage, cited by 18%.

Where, if anywhere, do you think cyber security messaging is most likely to lose accuracy?



Websites and landing pages are cited by 14%, while social media, paid advertising and sales materials are each cited by 13%. Thought leadership is cited less often, at 9%.

These findings suggest the problem is not tied to one format. Accuracy can weaken as claims are adapted, shortened or reused. A carefully qualified product message may become more assertive in a headline, broader in a sales deck or less specific in social content.

The issue is therefore not only whether a claim is approved at the start. It is whether the meaning remains accurate as that claim moves across the buyer journey.

For cyber security organisations, this could point to the need for stronger shared ownership. Communications, technical, legal and sales teams all have a role in making sure claims remain accurate, proportionate and understandable wherever they appear.

Building trust through responsible communication

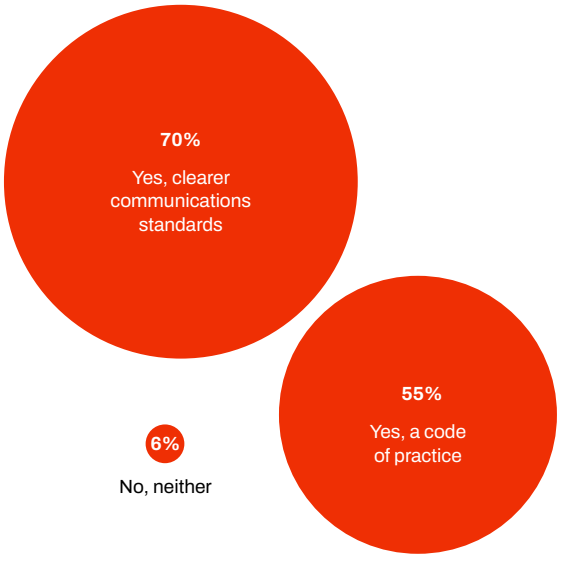
Clearer communication in cyber security is not only about reducing risk, but also about creating an opportunity to build trust.

Most respondents (86%) agree that clear and responsible communication can significantly increase customer trust. Almost all respondents (97%) agree that PR plays an important role in reducing the risks associated with miscommunication in cyber security marketing.

That role needs to be understood properly. PR and communications teams are not just responsible for making messages more compelling. They can help translate between technical teams, commercial teams and the audiences that need to understand the business value.

That means challenging unsupported claims, keeping messaging consistent across channels, communicating limitations and helping organisations explain cyber security as risk management rather than complete protection.

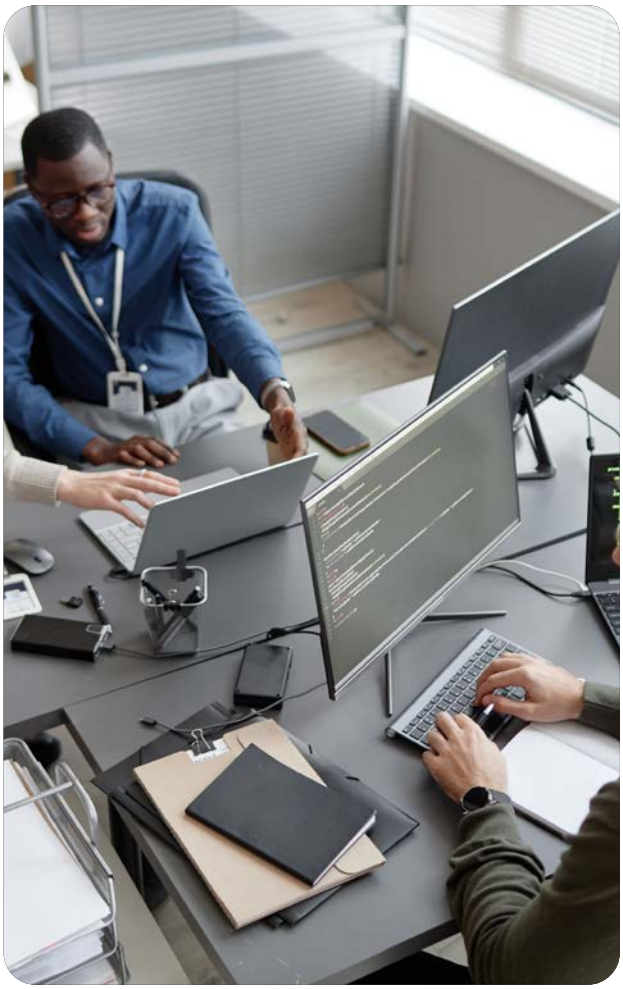
Do you believe the cyber security industry needs clearer communications standards or a code of practice to reduce the risk of miscommunication?



It also means supporting internal communication.

Cyber security is often treated as a technical or operational issue, but communication shapes how employees understand risk, how boards make decisions and how leadership teams respond when incidents occur.

There is also strong support for higher standards across the industry. Almost all respondents (94%) say the industry needs clearer communication standards or a code of practice to reduce miscommunication. More than eight-in-ten (86%) believe cyber industry communications practitioners should achieve a cyber-related accreditation or certification.



This appetite for greater structure reflects the level of complexity involved. Communicating cyber security requires technical understanding, commercial judgement and sensitivity to how claims may be interpreted. More than a third (35%) also say they find it challenging to stay current with changing threats, terminology and trends.

Clearer standards could help set expectations around evidence, language, claims, limitations and review processes. They could also help reduce the risk of exaggeration or unfounded claims in market-facing content.

There may also be lessons from more established risk-based sectors, where professional standards shape how services are described and how responsibility is understood. Business leaders do not need to become lawyers to understand the value of legal advice. In the same way, they should not need to become technical experts to understand when cyber security support is needed or what role it should play.

The findings suggest many professionals in the industry want more structure. The proposed voluntary code of practice is a practical way to begin setting those expectations.

"There is a real opportunity for the cyber security industry to improve how solutions are communicated. Buyers need clear, accurate and trustworthy information, particularly in a field where the decisions they make can affect operations, compliance and reputation.

PR has an important role to play in that. It can help translate technical capability into language that different audiences can understand, while also challenging claims that risk creating unrealistic expectations. Responsible communication should not make cyber security marketing less effective. It should make it more credible."

Hayley Goff,
Chief Executive Officer at Whiteoaks International

Conclusion

The findings in this report suggest many professionals perceive miscommunication in cyber security marketing as an issue affecting the wider industry, shaped by how messaging is developed, interpreted and adapted across different audiences and channels.

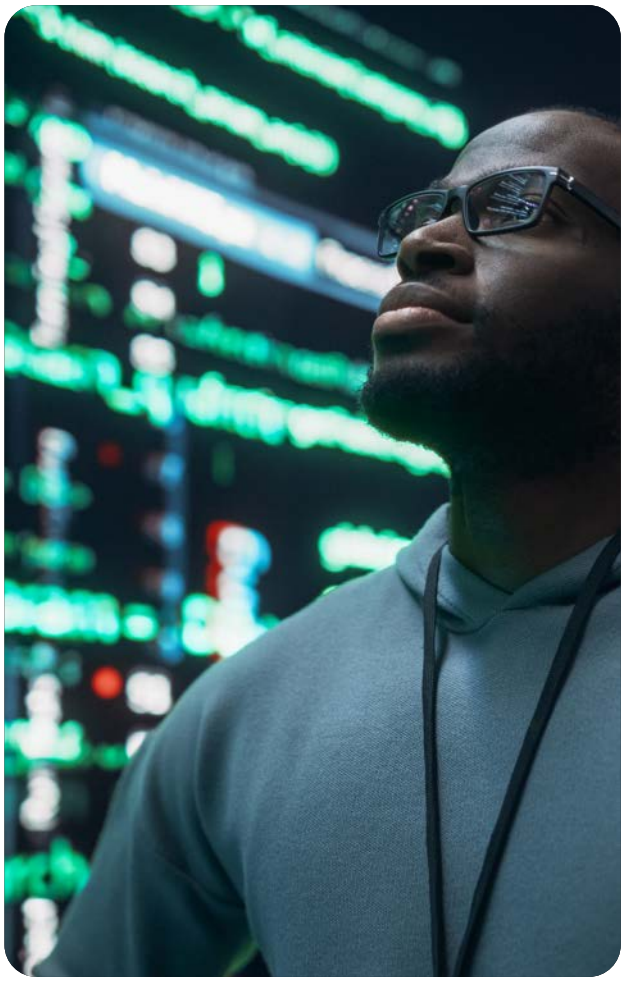
Many professionals understand the risks and recognise that absolute claims can create unrealistic expectations, overstated language can increase legal and reputational exposure, and that poor communication may affect commercial outcomes. Yet respondents still report seeing the same issues appear.

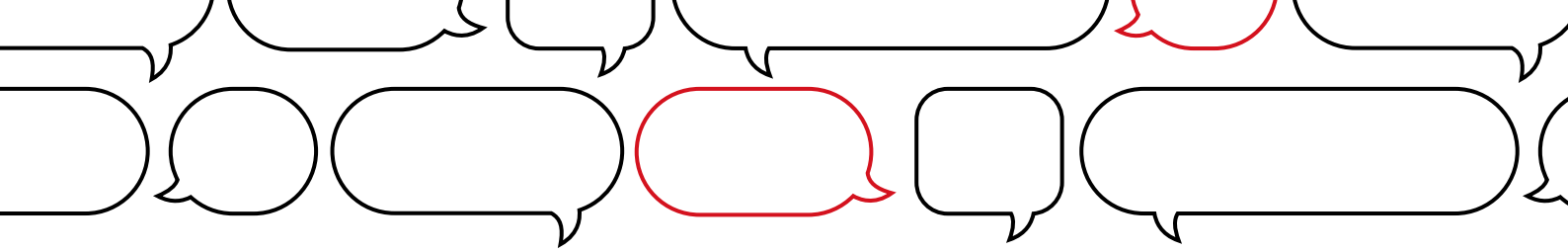
This reinforces the growing importance of communication as a discipline in its own right. PR and communications teams are not just amplifiers of messaging, but translators between technical, commercial and non-technical audiences, responsible for maintaining clarity, consistency and credibility across complex environments.

Addressing these challenges does not sit with any one function or organisation. It requires a more coordinated approach across the industry, spanning vendors, agencies, technical teams and communications professionals. Greater consistency in how capabilities are described, stronger validation of claims and closer collaboration between stakeholders will all play a role.

The research also shows the industry is open to change. Strong support for clearer standards and greater professionalisation reflects an appetite for a more structured approach to cyber security communication.

Reducing the credibility gap will likely depend on how effectively the industry can align technical accuracy, commercial communication and audience understanding. The proposed voluntary code of practice that follows is intended as a practical step towards that goal, helping the sector build greater trust in how cyber security capabilities are communicated and acted upon.





A proposed voluntary code of practice for cyber security communications

The findings in this report point to a clear industry challenge: cyber security communications are becoming increasingly vulnerable to exaggeration, ambiguity and loss of meaning across channels.

Improving this will likely require more than better marketing. It requires a shared commitment across the industry to clearer, more responsible communication standards.

To support this, we propose the following voluntary code of practice for marketing, PR and communications professionals working in the cyber security sector. Its aim is to encourage greater clarity, consistency and credibility in how cyber security products, services and risks are communicated.

This proposed voluntary code is intended as a discussion framework to encourage responsible communication practices. It is not a formal industry standard. We welcome input from across the cyber security industry to help refine the principles and support more responsible communication standards.

Get in touch with us at hello@whiteoaks.co.uk

Proposed voluntary code of practice for cyber security communications

As a signatory to this code, I commit to the following principles. I will:

- Ensure honesty, clarity and transparency in all communications
- Avoid exaggerated or absolute claims such as “100% protection”, “total security” or similar terminology
- Use clear, accessible language wherever possible and explain technical terms where needed
- Ensure claims are evidence-based and can be substantiated
- Represent products, services and partnerships accurately and without omission
- Avoid ambiguity around capabilities, integrations or interoperability
- Ensure testimonials and case studies do not create misleading impressions
- Encourage collaboration between communications, technical and legal teams where appropriate
- Review messaging from the perspective of the intended audience to ensure it is clear, relevant and understandable
- Encourage partners, suppliers and stakeholders to follow similar standards of responsible communication


whiteoaks
INTERNATIONAL