The future of cybersecurity PR in the new age of AI

Why credibility, authority and strategic communications will become more valuable than ever



Foreword

The Future of Cybersecurity PR in the Age of AI

A point of view from PRPR

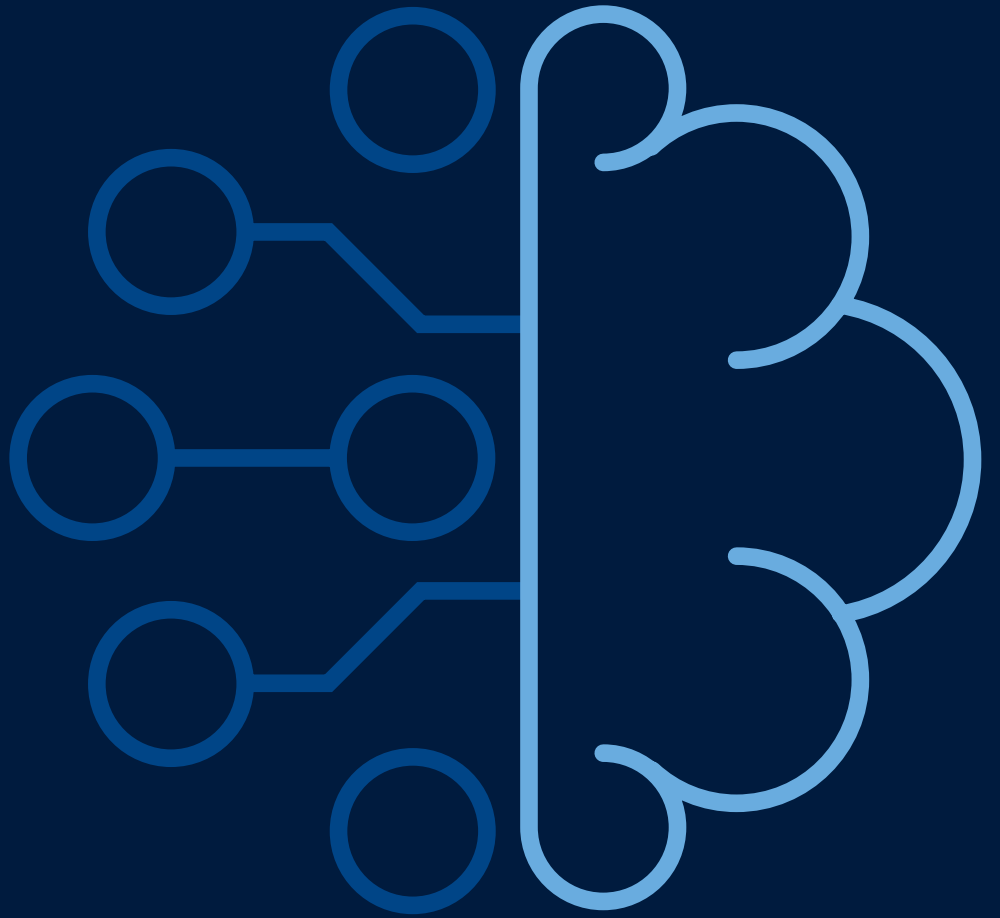
AI is dominating discussion across the cybersecurity industry. Much of the conversation is focused on automation, productivity and cyber defence. Far less attention has been given to the way AI is changing how cybersecurity companies establish authority, build credibility and compete for growth.

At PRPR, we believe this shift will fundamentally redefine the role of strategic communications over the coming decade.

This paper brings together research from Gartner, McKinsey, the UK Government and wider industry analysis alongside PRPR's own experience working with cybersecurity companies to explore how authority is a strategic competitive advantage in an AI-driven market.

We hope it provides useful insight for cybersecurity leaders as they rethink communications, reputation and growth in the age of AI.

Allie Andrews
CEO, PRPR



Executive summary

Artificial intelligence is transforming cybersecurity in ways that extend far beyond technology itself. While much attention has focused on AI's impact on threat detection, software development and security operations, a quieter transformation is taking place. AI is fundamentally changing how cybersecurity companies earn trust, build authority, influence buying decisions and compete for growth.

For more than two decades, digital communications have been driven by a relatively simple principle. Organisations created content, optimised it for search engines and distributed it across digital channels. Visibility was often the primary objective, and organisations that produced the most relevant content frequently gained a competitive advantage.

AI is fundamentally changing this model. AI is making content easier to produce and harder to distinguish. If content is abundant, trust is an even more valuable differentiator.

Generative AI has dramatically reduced the barriers to content creation. Marketing teams can now produce blogs, white papers, social media content, reports, videos and campaign assets at a scale that would previously have required significant investment in people and resources. What was once a specialist capability is rapidly becoming a commodity.

The challenge facing cybersecurity organisations is changing. The issue is no longer the ability to create content. The issue is the ability to establish credibility and authority in an industry saturated with increasingly similar information, competing claims and AI-generated commentary.

Artificial intelligence is also transforming how information is discovered. Buyers are turning to AI-powered platforms such as ChatGPT, Microsoft Copilot, Google Gemini and AI-enhanced search experiences to research technologies, understand emerging threats and evaluate potential providers. This means visibility is influenced more by the authority signals surrounding an organisation than just advertising spend and content volume. Independent research, analyst recognition, media visibility, executive expertise and third-party validation all contribute to how organisations are represented in AI-driven information ecosystems. As a result, discoverability is becoming increasingly linked to credibility.

This shift is taking place at a time when the cybersecurity industry itself is becoming more competitive. According to the UK Government's 2026 Cyber Security Sectoral Analysis, the sector continues to experience sustained double-digit growth, with revenues approaching £15 billion and thousands of organisations competing across a rapidly expanding market.

Demand for cybersecurity expertise continues to increase, but so too does the number of vendors, consultancies, MSSPs and service providers competing for the attention of the same customers, investors and stakeholders.

In a market like this, technical excellence alone is rarely enough to guarantee market leadership. Buyers are confronted with competing claims, overlapping capabilities and similar messaging. Faced with this complexity, they naturally rely on signals that help them identify organisations they perceive as credible, authoritative and capable of delivering successful outcomes.

These signals include analyst recognition, independent research, executive visibility, thought leadership, media commentary, industry awards, customer advocacy and recognised expertise.

Historically, public relations has been viewed as a supporting communications function focused primarily on generating awareness. In the coming decade, its role will expand considerably. PR will help organisations build authority, shape industry conversations, strengthen stakeholder confidence, improve discoverability within AI-driven information ecosystems and establish the external validation that both buyers and AI systems increasingly rely upon.

This paper argues that cybersecurity organisations are entering a period in which reputation, expertise and market influence are becoming more important sources of competitive advantage.

As AI transforms how information is created, distributed, discovered and consumed, success will increasingly depend on more than the volume of content an organisation publishes or how frequently it communicates. The organisations that stand out will be those recognised as authoritative and credible voices within their markets.

In an AI-driven marketplace, organisations will not compete solely for attention. They will compete for authority. Those that establish recognised expertise, contribute meaningfully to industry conversations and build strong reputation capital will be significantly better positioned to influence both human decision-makers and the AI systems that shape discovery, evaluation and purchasing journeys.

The future of cybersecurity PR is not primarily about generating attention. It is about helping organisations earn the authority that customers, journalists, analysts and increasingly AI systems rely upon when deciding who to trust. In an AI-driven economy, authority is one of the few sustainable competitive advantages that technology alone cannot create.

Contents

Foreword

Executive summary

1. The AI communications revolution
   - 1.1 The hidden challenge of democratisation
   - 1.2 Volume is only part of the challenge
   - 1.3 Recognising AI-generated content
     - 1.3.1 The Psychology of Trust
2. Growth, competition and the differentiation challenge
   - 2.1 Increased competition
   - 2.2 The AI authority paradox
3. The decline of technical differentiation and the rise of the authority economy
   - 3.1 The authority economy
   - 3.2 PR's strategic role
   - 3.3 Reputation capital
4. AI discoverability and the rise of GEO
5. Reputation, misinformation and resilience
   - 5.1 Reputation capital as resilience
   - 5.2 Authenticity as a strategic asset
   - 5.3 The convergence of cybersecurity and communications
6. The PRPR Authority Model
   - 6.1 How to use the PRPR Authority Model
   - 6.2 Stage One: Visibility
   - 6.3 Stage Two: Recognition
   - 6.4 Stage Three: Credibility
   - 6.5 Stage Four: Influence
   - 6.6 Stage Five: Authority
   - 6.7 Why the model matters
   - 6.8 PRPR Authority Audit
   - 6.9 Key questions for leadership teams
7. The future role of cybersecurity PR
   - 7.1 Communications as a competitive advantage
8. Conclusion

1. The AI communications revolution

AI could be described as the most significant technological shift since the emergence of the internet. While there is considerable debate about the pace and scale of its long-term impact, there is little disagreement that AI is already transforming how organisations operate.

Across industries, businesses are exploring opportunities to use AI to automate routine activities, improve productivity and enhance decision-making. In cybersecurity, AI is being used to support threat detection, automate investigations, accelerate incident response and improve operational efficiency. Much of the industry discussion has understandably focused on these operational benefits and the role AI will play in strengthening cyber resilience.

However, one of the most immediate and visible impacts of AI is taking place within communications.

For the first time, organisations have access to tools capable of producing professional-quality content quickly, efficiently and at scale. Activities that previously required significant investment in writing, editing, design and research can now be completed in a fraction of the time.

Research from McKinsey suggests that marketing and sales functions are among the areas most likely to benefit from generative AI adoption, largely because of the technology's ability to accelerate content creation and customer engagement activities. Across industries, organisations are already using AI to produce blogs, reports, presentations, videos, social media content and customer communications at unprecedented speed.

At first glance, this appears overwhelmingly positive.

Increased efficiency allows organisations to communicate more frequently, reach broader audiences and operate with greater agility. Smaller companies gain access to capabilities that were previously available only to larger competitors with substantial marketing budgets. The ease of content creation enables organisations of all sizes to compete more effectively for visibility.

1.1 The hidden challenge of democratisation

Historically, organisations that invested in thought leadership, research and high-quality content had a genuine competitive advantage because creating authoritative content needed significant expertise, time and resources.

AI has dramatically lowered those barriers. Today, a start-up with a small marketing team can produce articles, reports, commentary and campaign assets at a scale that was once only possible for much larger organisations. Content production is becoming increasingly democratised. The challenge is creating content that is genuinely original, credible and worth paying attention to.

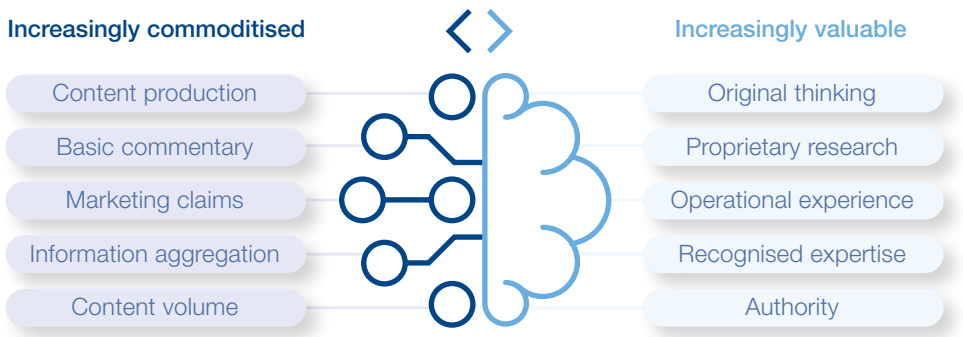
1.2 Volume is only part of the challenge

The widespread adoption of generative AI also means there is a growing degree of content homogenisation. Because many organisations rely on similar tools, prompts, publicly available information and content-generation approaches, the resulting output often follows familiar structures, repeats widely available insights and reaches similar conclusions. While this content may be accurate and professionally presented, it is not necessarily distinctive or adding anything to the conversation.

This is a significant challenge for cybersecurity organisations.

If multiple vendors are publishing articles on the same topics, using similar language, citing similar research and making similar claims, content alone becomes a less effective means of differentiation. The ability to generate information is no longer scarce. The ability to generate genuinely original insight is.

Differentiation: from commoditised content to competitive advantage



As AI-generated content becomes common, the characteristics that differentiate organisations are changing. Original thinking will become more valuable. Proprietary research will become more valuable. Operational experience will become more valuable. Recognised expertise will become more valuable. In short, anything that cannot easily be replicated by AI will be increasingly important sources of competitive advantage. And this is particularly significant within cybersecurity.

Security leaders already operate within a complex environment that suffers with information overload. On any given day they may encounter threat intelligence reports, vulnerability disclosures, regulatory updates, analyst commentary, industry predictions, vendor announcements and research findings from multiple sources.

As more organisations adopt AI-enabled communications, buyers are faced with the challenge of distinguishing meaningful expertise from marketing noise. They also need to identify genuine insight and original analysis amid a growing volume of AI content that is repackaging information already available elsewhere. In this environment, authenticity, expertise and independent validation are important indicators of value.

1.3 Recognising AI-generated content

Journalists, analysts and experienced buyers are more and more adept at recognising generic AI-generated content. As the volume of AI-assisted communications continues to grow, these audiences are placing greater value on perspectives that demonstrate authentic expertise, original analysis and direct experience.

As AI makes content easier and faster to produce, its value will increasingly come from the quality of the thinking behind it. Organisations with genuine expertise, original perspectives and something meaningful to contribute will have a stronger voice in industry conversations.

The communications challenge of the next decade will not be creating content. It will be earning confidence.

When people are confronted with overwhelming quantities of information, they naturally seek shortcuts that help them determine which sources deserve their attention. Rather than evaluating every claim independently, they instinctively look for signals that indicate expertise, credibility and relevance.

This is not a new phenomenon. Humans rely on cognitive shortcuts and recognisable signals to navigate complexity. Research in psychology demonstrates that people naturally seek patterns, coherence and trusted reference points when confronted with large volumes of information. Rather than evaluating every piece of information independently, we use signals that help us quickly assess relevance, credibility and value.

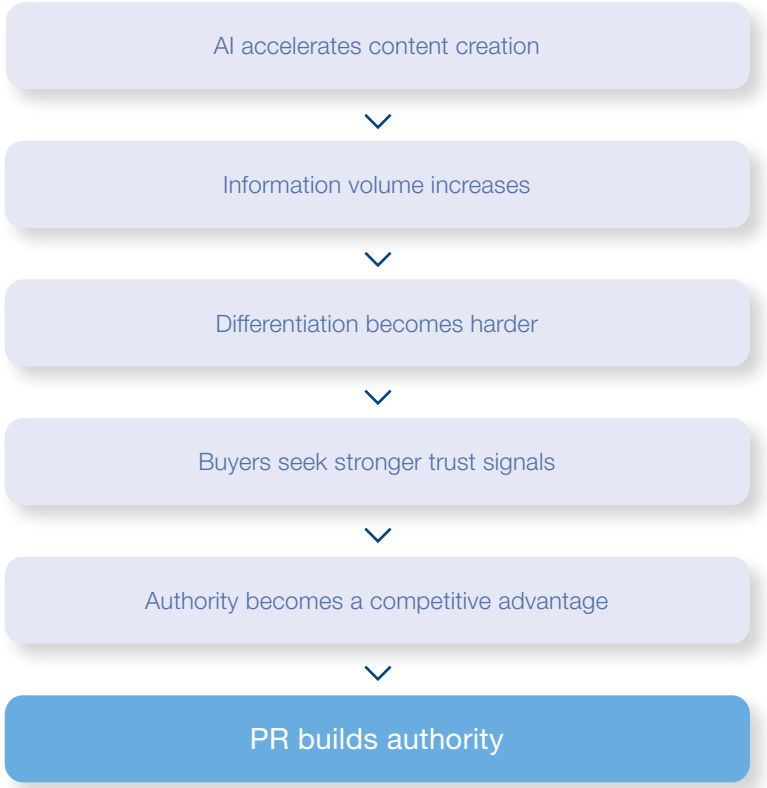
1.3.1 The Psychology of Trust

Gestalt psychology suggests that people look for patterns and coherent signals when processing complex information. In crowded cybersecurity markets, authority is often formed not through a single interaction but through the cumulative effect of multiple signals, including media visibility, analyst recognition, executive expertise, independent research and peer recommendation. Together, these create a perception of credibility that influences decision-making.

What is changing now is the degree to which these signals influence decision-making. As information becomes more abundant and difficult to differentiate, stakeholders place greater emphasis on the cues that help them identify expertise and reduce uncertainty. In cybersecurity, those cues will include recognised experts, independent research, analyst recognition, media visibility and trusted third-party validation.

The AI authority gap

Why authority is a key competitive advantage.



Public relations has traditionally been viewed as a mechanism for amplifying organisational messages and generating awareness. In the age of AI, its role is becoming considerably more strategic. The value of PR now lies in helping organisations establish the external credibility, recognised expertise and independent validation that make those messages believable. It also plays a critical role in ensuring that expertise is visible within the information ecosystems where customers, journalists, analysts and AI platforms increasingly seek answers.

Organisations that recognise this shift early and invest in building credibility, influence and recognised expertise will be significantly better positioned to compete.

2. Growth, competition and the differentiation challenge

The cybersecurity industry is experiencing a period of remarkable growth. Increasing cyber threats, expanding regulatory requirements, digital transformation initiatives and growing awareness of cyber risk at board level have all contributed to sustained demand for cybersecurity products and services. Organisations across both the public and private sectors are investing heavily in capabilities designed to improve resilience, reduce risk and strengthen operational security.

The UK's cybersecurity sector provides a useful illustration of this trend. According to the UK Government's Cyber Security Sectoral Analysis 2026, the sector generated £14.7 billion in revenue during the last year, representing annual growth of 11%. The number of cybersecurity firms operating in the UK increased by 20% to 2,603 organisations, with 438 new companies entering the market in a single year. Employment across the sector reached almost 70,000 professionals, while its contribution to the UK economy grew to £9.1 billion in Gross Value Added (GVA). Investment activity also remained strong, with £184 million raised across 47 dedicated cybersecurity investment deals during 2025.

These figures demonstrate a sector expanding in both scale and capability, attracting new investment, new entrants and increasing customer demand. New companies continue to enter the market, while established providers expand their offerings to address emerging challenges such as cloud security, digital resilience, AI governance and managed security services.

On the surface, this appears overwhelmingly positive. Demand is increasing, investment remains strong and cybersecurity has secured a permanent place on board agendas. The sector is benefiting from sustained growth, increased market attention and a growing recognition that cyber resilience is now a business imperative rather than a purely technical concern.

2.1 Increased competition

Growth also creates new competitive pressures.

As markets expand, they attract new entrants, new investment and new forms of competition. Emerging technologies create new categories; investors seek opportunities in high-growth sectors and established organisations broaden their portfolios to capture evolving customer demand. Over time, the result is a more crowded and more competitive marketplace.

This dynamic is visible across virtually every segment of cybersecurity. Managed detection and response providers compete against a growing number of alternative providers offering similar services. Security consultancies face increasing competition from both established firms and specialist challengers. Platform vendors compete against organisations promoting remarkably similar capabilities and outcomes. Even highly specialised markets are becoming more competitive as organisations seek to establish positions in areas such as AI security, cloud security, cyber resilience and digital risk management.

From a buyer's perspective, this growth has created a significantly more complex decision-making environment.

Visit the websites of twenty cybersecurity vendors and a remarkably consistent picture emerges. Most promise AI-powered protection, proactive defence, greater resilience, reduced risk and measurable business outcomes. The challenge for buyers is deciding which organisations are most likely to deliver on those promises.

Many of these claims are completely valid, which makes meaningful differentiation difficult.

Research into B2B purchasing behaviour consistently demonstrates that buyers seek ways to reduce uncertainty when making complex purchasing decisions. This is particularly true within cybersecurity, where decisions often involve significant financial investment, operational implications and risk exposure. Few decision-makers have the time, resources or technical expertise required to conduct exhaustive evaluations of every available provider. Instead, they rely on signals that help them identify organisations they believe are most likely to deliver successful outcomes.

Importantly, these signals often extend beyond technical capability.

Industry recognition, analyst commentary, independent research, customer advocacy, executive visibility and media presence all contribute to broader perceptions of expertise and market standing. Collectively, they help buyers assess credibility, reduce uncertainty and build confidence in prospective partners.

This becomes even more important as markets become more competitive. Faced with a growing number of organisations offering apparently similar capabilities, buyers become less reliant on individual marketing claims and more reliant on independent signals that help them identify organisations they believe are credible, trustworthy and capable of delivering successful outcomes.

2.2 The AI authority paradox

Many of the signals that influence whether organisations are surfaced, referenced or recommended by AI-powered search and discovery platforms are the very signals that cannot easily be generated through AI alone. Analyst recognition, earned media coverage, independent research, executive authority and recognised expertise, for example, are becoming important indicators of organisational credibility.

Thought leadership provides a useful example. While AI can assist with content creation, it cannot create genuine expertise, proprietary insight or the credibility that comes from recognised industry experience. The most valuable thought leadership is rooted in original research, real-world experience and unique perspectives rather than information that is already widely available online. It is also increasingly valued by journalists and industry publications; many of whom will be more selective about the content they publish as AI-generated material becomes commonplace.

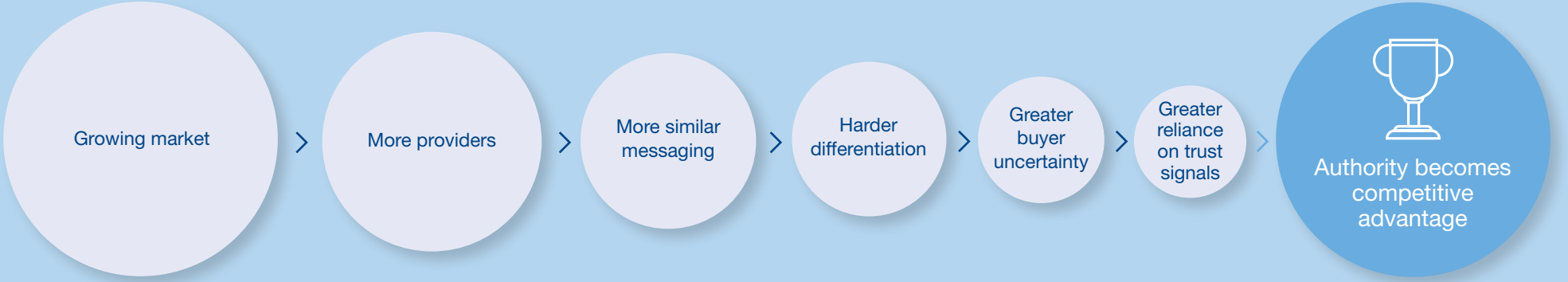
This is one of the reasons organisations such as CrowdStrike, Palo Alto Networks and Microsoft have invested heavily in original research, thought leadership and executive visibility alongside product development. Their market influence is not derived solely from technology. It is reinforced by their ability to shape conversations, contribute valuable insights and establish recognised positions of authority within the industry.

As competition increases, the organisations most likely to stand out will be those that combine technical excellence with recognised authority. Technology is still essential, but market leadership will depend on how convincingly that expertise is demonstrated and recognised beyond an organisation's own marketing.

In many respects, this is a shift from competing on technology alone to competing on influence. And influence, unlike content, cannot be automated.

The competition gap

How market growth and crowded messaging increase buyer uncertainty.



3. The decline of technical differentiation and the rise of the authority economy

For much of the cybersecurity industry's history, competitive advantage has been linked to technical differentiation.

Vendors succeeded by developing capabilities that competitors could not easily replicate. Security providers established market positions through specialised expertise, proprietary technologies or unique approaches to securing against emerging threats. In many cases, buyers could clearly identify meaningful distinctions between competing solutions.

While innovation is still essential, the nature of showing differentiation is changing. Many areas of cybersecurity are crowded and similar in the eyes of buyers. Technologies are still evolving but the language used to describe them is now remarkably consistent. Across the industry, vendors promote artificial intelligence, automation, threat intelligence, Zero Trust architectures, cyber resilience and cloud security capabilities. While genuine differences may exist beneath the surface, these distinctions are not always obvious to prospective customers.

This challenge is not unique to cybersecurity. It is common in maturing technology markets.

Over time, capabilities that were once considered differentiators become expected features. Competitors adopt similar approaches; customer expectations evolve; and technological advantages are more difficult to sustain. As markets mature, buyers are less focused on individual features and more on broader indicators of organisational capability and long-term value.

Consider the managed detection and response market. Most providers now offer 24/7 monitoring, threat hunting, incident response capabilities and advanced analytics. Similarly, many cloud security providers promote comprehensive visibility, risk reduction and regulatory compliance support. The challenge for buyers is determining which organisations are most capable of delivering on them.

The result is that technical differentiation alone is difficult to communicate. And this creates an important shift in how purchasing decisions are made.

When purchasing decisions involve significant complexity or risk, buyers seek additional signals that help them assess confidence and reduce uncertainty. These signals often include analyst recognition, peer recommendations, executive credibility, customer references, independent research and broader market reputation.

In cybersecurity, where purchasing decisions often carry substantial operational, financial and reputational consequences, these factors can be particularly influential.

When organisations are selecting a cybersecurity partner, they are not simply purchasing technology. They are selecting a provider that may have access to sensitive systems, critical infrastructure, confidential information and strategic decision-making processes. The perceived reliability of that provider therefore becomes an important component of the evaluation process.

AI is accelerating the production of marketing content across the industry. As organisations gain access to sophisticated content creation tools, the volume of reports, articles, thought leadership and promotional material is increasing. The result is more information and greater difficulty in distinguishing genuine expertise from well-produced content.

Audiences are often evaluating the source of information as carefully as the information itself. Buyers want confidence that the expertise behind content is genuine.

3.1 The authority economy

In many ways this is the emergence of what might be described as an authority economy. Within an authority economy, influence is determined by the degree to which that organisation is recognised as actually being a reliable source of insight and not the volume of information an organisation produces.

This is important because credibility cannot be automated in the same way as content creation. Generative AI can help with writing reports, producing commentary and creating marketing materials. It cannot by itself establish market authority. Authority is earned through consistent demonstration of expertise and through recognition by external stakeholders.

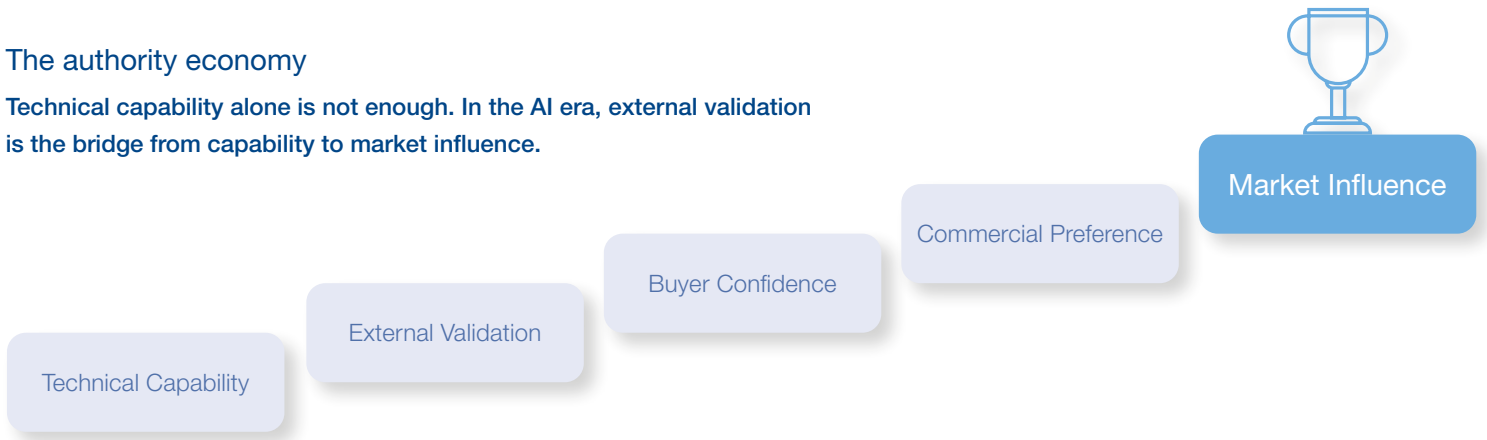
This is why you will always get organisations that appear to exert influence that extends far beyond their market share.

These are the companies that have not only invested heavily in technology development, they have also invested in building recognised positions within industry conversations. Their executives are frequently quoted in the media. Their research teams regularly publish original threat intelligence. Their insights are referenced by analysts, journalists and policymakers. These organisations have become recognised sources of expertise.

The authority economy

Technical capability alone is not enough. In the AI era, external validation is the bridge from capability to market influence.

When major cyber incidents occur, journalists frequently seek commentary from their experts. When analysts examine industry trends, their research is often referenced. When organisations seek guidance on emerging threats, their perspectives carry weight.



Authority creates confidence and confidence creates market opportunity

3.2 PR's strategic role

Importantly, this influence cannot be created solely through marketing activity. It is built through the consistent demonstration of expertise over time. This helps explain why public relations is so important now within cybersecurity.

Historically, PR was associated with awareness generation. Success was frequently measured through media coverage, impressions or share of voice. While these metrics are still useful, they do not fully capture the strategic role communications plays now.

The most effective cybersecurity PR programmes do not simply amplify messages. They help organisations establish authority. They create opportunities for experts to contribute to industry discussions. They support the publication of original research. They facilitate relationships with journalists, analysts and influencers. They help ensure that expertise is visible to the audiences that matter most. Collectively, these activities build reputation capital.

3.3 Reputation capital

Reputation capital is the accumulated value of an organisation's credibility, expertise and market standing. Like financial capital, it can generate tangible returns. It influences purchasing decisions, supports business development, strengthens stakeholder confidence and improves resilience during periods of uncertainty.

Perhaps most importantly, reputation capital is more valuable as information becomes more abundant.

When buyers are confronted with hundreds of competing messages, they rarely evaluate each equally. Instead, they gravitate towards sources they already recognise as credible. Familiarity, expertise and previous positive experiences all influence how information is interpreted.

The reinforcing cycle



For many years, communications strategies were primarily designed to support marketing objectives with visibility often considered the ultimate goal. The assumption was that greater awareness would naturally lead to increased commercial success.

But in an environment shaped by AI, that assumption is less reliable.

As content becomes easier to create, audiences are more selective regarding the sources they trust. As markets become more crowded, buyers place greater value on recognised expertise. As technological differentiation becomes harder to communicate, broader perceptions of credibility are more influential.

This is why the future of cybersecurity communications is likely to be defined not by content volume but by authority.

The organisations that thrive over the next decade will not be those that publish the most reports, produce the most social media content or generate the highest number of media mentions. They will be the organisations that consistently demonstrate expertise, contribute meaningful insights to industry conversations and earn recognition as authoritative voices within their markets.

In other words, they will compete on influence, not technology. And influence, unlike content, is one of the few assets that cannot be generated at the click of a button.

4. AI discoverability and the rise of GEO

One of the most significant consequences of artificial intelligence is not the way organisations create content but the way customers discover information in the first place.

For more than two decades, digital visibility has largely been governed by search engines. Organisations invested heavily in websites, content creation and Search Engine Optimisation (SEO) to improve rankings, increase traffic and create opportunities for customer engagement. Although search algorithms evolved considerably over that period, the underlying model remained relatively consistent. Users entered a query, reviewed a list of results and selected the sources they considered most relevant.

That model is changing. Buyers are turning to generative AI platforms such as ChatGPT, Claude, Google Gemini, AI Overviews and Microsoft Copilot to answer questions, compare suppliers and recommend potential partners. Rather than presenting users with pages of search results, these platforms synthesise information from multiple sources and generate direct responses that require far less effort from the user.

This is a major shift in digital behaviour.

Research firms are already anticipating significant changes in how people search for information. Gartner has predicted that traditional search engine volume will decline by 25% as users increasingly adopt AI assistants and virtual agents, while organic search traffic is expected to fall further as generative AI becomes mainstream. Regardless of the precise pace of adoption, organisations will need to optimise for AI systems that interpret, synthesise and recommend information as well as search engines.

This shift also has big implications for B2B buying behaviour. Technology buyers already complete a significant proportion of their purchasing journey before engaging directly with suppliers. As AI becomes part of that research process, the organisations surfaced during these early stages are likely to enjoy a significant competitive advantage long before a formal procurement exercise begins.

The objective is therefore no longer simply to appear within search results. Increasingly, organisations need to become recognised as authoritative enough to be surfaced, referenced and recommended within AI-generated responses.

This emerging discipline has become known as Generative Engine Optimisation (GEO). Like SEO before it, GEO is concerned with improving discoverability. However, the mechanisms through which that discoverability is achieved are changing.

Traditional SEO focused primarily on technical optimisation. Website structure, metadata, backlinks, keyword relevance and page performance all played important roles in determining search rankings. These disciplines are still valuable because AI systems also rely on information published across the web. However, they are only part of the picture.

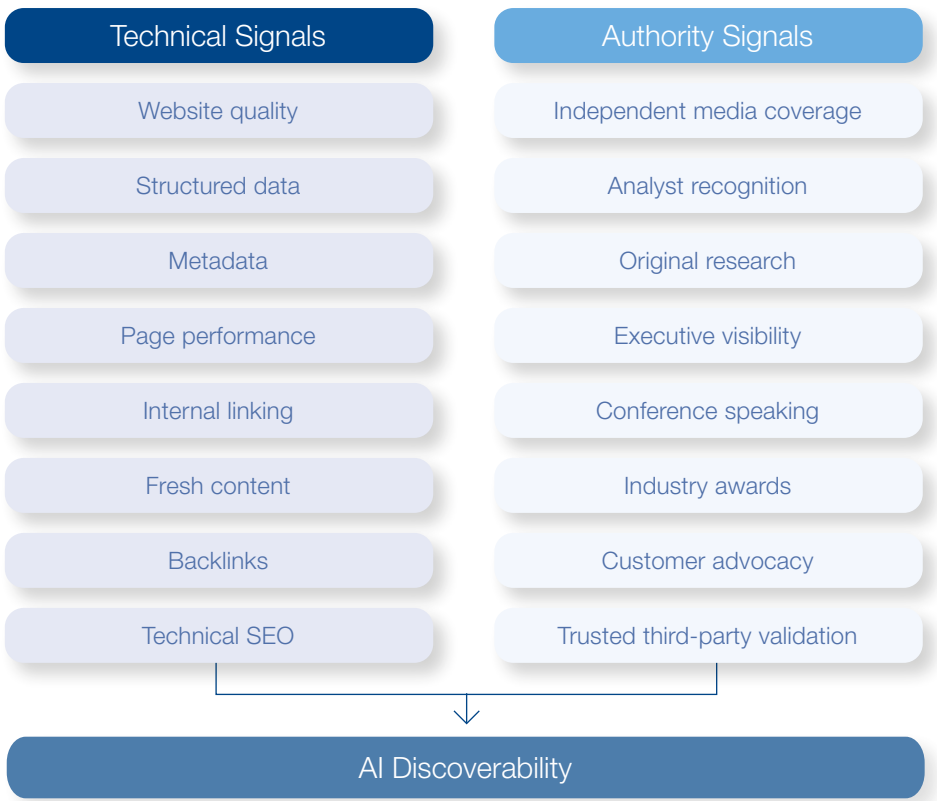
Unlike traditional search engines, generative AI platforms are designed to provide users with direct answers rather than simply directing them towards websites. Although the precise methods used by different AI systems remain proprietary and continue to evolve, there is growing evidence that they place increasing emphasis on broader signals of expertise, authority and credibility when determining which organisations to reference, cite or recommend.

Discussion surrounding GEO has understandably focused on structured data, technical optimisation and AI-generated content. These are important components of digital visibility. However, for cybersecurity organisations they represent only one part of the challenge.

This paper argues that recognised authority is one of the primary drivers of successful GEO.

Organisations that are consistently referenced by respected industry publications, cited by analysts, recognised through original research and represented by visible subject matter experts create the external authority signals that both buyers and AI platforms associate with expertise. Unlike marketing claims published solely on an organisation's own website, these signals provide independent evidence that expertise has been recognised and validated externally.

The Building Blocks of AI Discoverability



Successful GEO increasingly depends on combining technical optimisation with recognised authority.

For cybersecurity organisations, this has significant implications.

Technical expertise alone is not enough if that expertise cannot be discovered. Equally, producing larger volumes of AI-generated content is unlikely to create sustainable differentiation if competitors are doing exactly the same thing. Competitive advantage depends on demonstrating the qualities that both buyers and AI systems associate with recognised authority.

These qualities include original research, recognised subject matter experts, independent media coverage, analyst recognition, conference presentations, customer advocacy, executive visibility and meaningful contributions to industry debate. Collectively, they create an authority footprint that extends well beyond an organisation's own website.

This development has significant implications for public relations.

Historically, PR has focused on helping organisations influence people. Increasingly, it is also helping organisations influence the information ecosystems that AI systems draw upon. Every piece of independent media coverage, every analyst report, every conference presentation, every published research paper and every executive interview contributes to a richer ecosystem of externally validated expertise. Collectively, these activities strengthen the authority footprint that both human audiences and AI platforms increasingly rely upon when evaluating credibility.

Importantly, the authority signals that strengthen AI discoverability are often the same signals that strengthen organisational resilience. Independent research, trusted media relationships, executive visibility and recognised expertise not only improve the likelihood of being surfaced by AI systems, they also build the stakeholder confidence organisations depend upon during periods of uncertainty. AI is bringing together disciplines that have traditionally been considered separately, linking discoverability, reputation and resilience through a common foundation of recognised authority.

There is an interesting paradox emerging.

Artificial intelligence is making content easier than ever to create, yet the systems built on artificial intelligence increasingly appear to place greater weight on the qualities that content alone cannot provide. AI can generate articles, blogs and reports in seconds, but it cannot independently earn credibility, build trusted relationships or establish recognised expertise.

As AI-generated material becomes more commonplace, these human qualities become more valuable because they provide evidence that expertise is genuine rather than simply well presented.

This also requires organisations to rethink how they evaluate investment in communications. Historically, marketing budgets have often prioritised content production, digital campaigns and lead generation, while public relations has been viewed primarily as a mechanism for increasing awareness. In an AI-driven information environment, those distinctions become increasingly blurred. Activities such as executive profiling, analyst engagement, original research and earned media are no longer simply communications outputs; they are strategic investments that strengthen discoverability, credibility, resilience and long-term market influence simultaneously.

For boards and leadership teams, this is an important shift in perspective. It is important that they question whether communications investment is strengthening the authority that customers, stakeholders and AI systems rely upon when deciding who to trust.

From SEO to GEO

The evolution from search engine optimisation to generative engine optimisation

Search Engine Optimisation	Generative Engine Optimisation
Can search engines find us?	Will AI recommend us?
Optimise websites	Build recognised authority
Improve rankings	Earn recommendations
Generate clicks	Influence buying journeys
Visibility	AI discoverability

The objective of optimisation is evolving from improving rankings to earning recommendations.

In many respects, this is the next evolution of digital visibility. Search engines rewarded organisations that optimised their websites. Generative AI increasingly rewards organisations that build recognised authority.

For cybersecurity organisations, this may prove to be one of the most significant shifts in digital communications since the emergence of search itself. It also provides the bridge to the next stage in the evolution of public relations, where communications is no longer judged simply by the awareness it creates, but by the authority, influence and competitive advantage it helps organisations build.

SEO helps you get found. GEO helps you get recommended.

5. Reputation, misinformation and resilience

For years, cybersecurity professionals described people as the weakest link in security. That perspective has evolved. Organisations now recognise that employees are not simply a source of risk but also an essential layer of defence. Security awareness programmes, training initiatives and the development of strong cyber cultures are all built on the principle that informed people strengthen organisational resilience.

A similar shift is now taking place in relation to reputation.

Historically, reputation management has been viewed primarily as a communications discipline concerned with brand perception, media relations and stakeholder engagement. While these remain important responsibilities, AI is fundamentally changing the nature of reputation risk. Reputation should now be viewed as an integral component of organisational resilience, not simply a communications asset.

AI is dramatically reducing the barriers to creating convincing misinformation. The same technologies that help organisations generate marketing content, automate communications and improve productivity can also be used to fabricate narratives, manipulate audio and video, impersonate executives and distribute misinformation at unprecedented speed and scale.

Deepfake technology illustrates this clearly. Only a few years ago, producing convincing synthetic audio or video required specialist expertise, significant resources and advanced technical capability. Today, sophisticated generative AI tools have made these capabilities widely accessible, while the quality of synthetic media continues to improve and the cost of producing it continues to fall.

Organisations must therefore prepare for a future in which misinformation campaigns are more sophisticated, more targeted and more difficult to identify. The implications extend well beyond politics and social media.

Cybersecurity organisations could face fabricated breach reports, manipulated executive statements, false allegations relating to security failures or coordinated attempts to undermine confidence in their products and services. Publicly listed organisations may become targets for misinformation designed to influence investor confidence, while service providers could face campaigns intended to influence procurement decisions or erode customer trust.

In this environment, reputation effectively becomes part of an organisation's attack surface.

5.1 Reputation capital as resilience

Just as cybercriminals seek to exploit vulnerabilities in networks, identities and cloud infrastructure, they will seek to exploit vulnerabilities in public perception. The challenge is how quickly organisations can establish which information stakeholders believe to be true. This is where reputation becomes strategically important.

When people are presented with conflicting information, they rarely evaluate every claim independently. Instead, they rely on existing perceptions, recognised experts and trusted sources to determine credibility. Organisations that have consistently invested in relationships with customers, journalists, analysts, regulators and industry stakeholders are therefore far better positioned to withstand misinformation than those whose reputations are less well established.

In practical terms, reputation functions as a form of resilience. Just as financial reserves help organisations withstand economic disruption, reputation capital helps them withstand uncertainty. It provides a foundation of confidence that organisations can draw upon when challenged publicly, whether by genuine incidents, misinformation campaigns or AI-enabled impersonation.

This relationship between reputation and resilience is not entirely new. Organisations with strong reputations have historically recovered more effectively from crises than those with weaker stakeholder relationships. What has changed is the speed, sophistication and scale at which misinformation can now spread.

The challenge increasingly mirrors the one faced by cybersecurity teams themselves. Both are fundamentally concerned with anticipating disruption, reducing uncertainty, maintaining confidence and recovering effectively when adverse events occur.

Cybersecurity professionals often define resilience as the ability to anticipate, withstand, recover from and adapt to disruption. The same definition applies equally to organisational reputation.

Like cyber resilience, reputational resilience cannot be developed during a crisis. It requires sustained investment long before disruption occurs. Organisations that consistently invest in thought leadership, executive visibility, stakeholder engagement, original research and industry participation build a reservoir of credibility that becomes invaluable when they come under scrutiny.

When a significant breach occurs, journalists seek comment from recognised experts. Analysts evaluate the wider implications. Customers look to trusted advisers for reassurance, while regulators and policymakers assess both technical responses and organisational communications. Throughout this process, stakeholders naturally gravitate towards organisations they already perceive as knowledgeable, credible and authoritative.

Their perspectives are more likely to be sought, their explanations more likely to be believed and their ability to influence the wider narrative stronger than organisations attempting to establish credibility for the first time during a crisis.

Organisations that remain largely invisible until an incident occurs often find themselves trying to build authority precisely when they need it most.

Reputation as a strategic resilience asset



5.2 Authenticity as a strategic asset

As AI-generated misinformation becomes more sophisticated, authenticity is more valuable because it cannot easily be replicated.

AI may be able to imitate an executive's appearance or reproduce an organisation's tone of voice. What it cannot easily replicate is the confidence created through years of demonstrated expertise, visible leadership, independent validation and trusted relationships. Authenticity therefore is a strategic asset and not just a desirable brand characteristic.

This has important implications for public relations. Historically, communications has been viewed primarily as a driver of growth. Organisations invested in PR to increase awareness, strengthen market presence and support commercial objectives. But AI is significantly expanding the strategic role of communications.

By helping organisations establish recognised authority, maintain stakeholder confidence and build trusted relationships with customers, journalists, analysts and policymakers, PR creates assets that are particularly valuable during periods of uncertainty.

This is especially relevant in cybersecurity because cybersecurity companies are not just providers of products and services; they are also trusted interpreters of a complex threat landscape. Customers, journalists, policymakers and business leaders rely on them to explain emerging risks, interpret new technologies and provide guidance during periods of uncertainty.

At the same time, those organisations may themselves become targets of misinformation, fabricated incidents or AI-enabled impersonation. Their ability to maintain confidence depends not only on technical resilience but also on reputational resilience.

5.3 The convergence of cybersecurity and communications

Cybersecurity leaders and communications leaders have traditionally operated as separate disciplines. AI is bringing these responsibilities much closer together because both seek to reduce uncertainty and maintain confidence during periods of disruption. Ultimately, both contribute directly to organisational resilience.

As AI continues to blur the boundaries between information, misinformation and synthetic content, this convergence is likely to accelerate.

The organisations that prove most resilient will be those that recognise reputation as more than a marketing asset or communications objective. They will view it as a strategic business capability, investing in authority, stakeholder relationships and recognised expertise long before they face significant public scrutiny.

The same activities that strengthen authority, improve discoverability and build market influence also strengthen organisational resilience. Thought leadership, original research, executive profiling, media engagement and independent validation are not simply communications activities; they are long-term investments in organisational credibility.

That reality may fundamentally change how cybersecurity organisations think about public relations in the years ahead.



6. The PRPR Authority Model

A framework for building authority in the age of AI

Throughout this paper we have argued that AI is fundamentally changing how cybersecurity organisations compete. It is transforming how information is created, how expertise is evaluated, how buyers make decisions and how organisations are discovered within increasingly AI-driven information ecosystems.

As content becomes easier to produce and markets become more competitive, visibility alone is no longer enough. Sustainable competitive advantage increasingly depends on recognised expertise, independent validation and the ability to build authority over time.

Traditionally, communications programmes were designed primarily to increase awareness. Success was measured through outputs such as media coverage, impressions, website traffic and social engagement. While these are useful indicators of activity, they reveal relatively little about whether an organisation is becoming more influential within its market.

It is important now to measure how authoritative an organisation has become. To help organisations do that, PRPR has developed the PRPR Authority Model.

The model describes five progressive stages that cybersecurity organisations can use to strengthen market position, build influence and establish recognised authority. Rather than viewing communications as a series of campaigns, it encourages organisations to think of authority as a strategic asset that compounds over time.

Although organisations may display characteristics of multiple stages, most will find that one stage best reflects their current level of market maturity.

The PRPR Authority Model

Five progressive stages. Each builds on the previous one, creating clear pathway from visibility to authority.



6.1 How to use the PRPR Authority Model

The PRPR Authority Model is designed to help cybersecurity organisations assess how effectively they are building recognised authority within their market.

Instead of measuring communications through individual activities or campaign outputs, the model encourages organisations to consider their overall level of market maturity. Each stage builds on the one before it. Visibility creates recognition, recognition supports credibility, credibility enables influence and sustained influence ultimately develops into recognised authority.

Organisations can use the model in three ways:

- **Assess current maturity** by identifying the stage that best reflects their current market position.
- **Identify capability gaps** by understanding which elements of authority require further investment.
- **Prioritise communications activity** around the actions that will move the organisation towards the next stage, rather than simply increasing the volume of communications.

Authority is not built through a single campaign. It develops through consistent investment over time and should be viewed as a long-term strategic asset rather than a short-term communications objective.

6.2 Stage One: Visibility

The question

Can the market find you?

Visibility is the foundation of market presence. Organisations cannot become recognised authorities if customers, analysts, journalists and partners are unaware they exist. At this stage, the focus is on building awareness through search visibility, digital marketing, content, events, social media and other promotional activities.

Visibility remains essential, but in today's cybersecurity market it is only the starting point. Many organisations achieve visibility without becoming influential because awareness alone rarely creates confidence.

Typical indicators

- Website traffic
- Search visibility
- Content reach
- Social engagement
- Event participation

Primary objective: **Awareness**

6.3 Stage Two: Recognition

The question

Does the market know who you are?

Recognition begins when visibility develops into a clear market identity. Organisations are no longer simply present; they become associated with particular technologies, specialist capabilities or areas of expertise.

Consistency is the defining characteristic of this stage. Positioning becomes clearer, messaging becomes more coherent and stakeholders begin to recognise the organisation for what it does best.

Recognition creates the platform upon which authority is built because buyers are significantly more likely to trust organisations they already know.

Typical indicators

- Share of voice
- Brand awareness
- Industry mentions
- Speaking invitations
- Analyst awareness

Primary objective: **Familiarity**

6.4 Stage Three: Credibility

The question

Does the market believe you?

This is where meaningful differentiation begins.

Visibility and recognition can be created through marketing activity. Credibility has to be earned. It develops when organisational claims are consistently reinforced through independent evidence, demonstrated expertise and trusted third-party validation.

Original research, analyst recognition, customer advocacy, media commentary, industry awards and successful client outcomes all contribute to perceptions of credibility. They reduce uncertainty by giving buyers confidence that expertise is genuine rather than self-proclaimed.

Within an AI-driven information environment, credibility becomes even more valuable because many of these external signals influence how AI systems assess authority and determine which organisations to reference.

Typical indicators

- Analyst citations
- Independent research
- Customer advocacy
- Industry awards
- Earned media
- External endorsements

Primary objective: **Confidence**

6.5 Stage Four: Influence

The question

Does the market listen to you?

Influence represents a significant shift in organisational maturity. Rather than simply participating in industry conversations, organisations begin shaping them. Their executives are sought out for commentary, their research informs debate and their perspectives help define discussions surrounding emerging threats, regulation and the future of cybersecurity.

Influence reinforces every stage that precedes it. Greater influence generates additional visibility, strengthens credibility and creates more opportunities for independent validation. Over time, recognised expertise attracts further opportunities to demonstrate expertise, creating a powerful self-reinforcing cycle.

Typical indicators

- Regular media commentary
- Conference keynote invitations
- Policy participation
- Research citations
- Analyst engagement
- Industry leadership roles

Primary objective: **Relevance**

6.6 Stage Five: Authority

The question

Does the market trust and follow you?

Authority represents the highest level of organisational maturity.

At this stage, organisations become recognised reference points within their markets. Their expertise is trusted, their opinions influence decision-making and their research helps shape how the wider industry understands emerging risks, regulation and technology.

Authority extends beyond reputation. It influences purchasing decisions, strengthens organisational resilience, improves AI discoverability, attracts talent and creates commercial advantage.

Perhaps most importantly, authority is self-reinforcing. Organisations recognised as industry leaders are more likely to be quoted by journalists, referenced by analysts, invited to speak at major conferences and surfaced by AI-powered information platforms. Each opportunity further strengthens their authority, making it progressively harder for competitors to displace them.

This is one of the reasons recognised authority is one of the few competitive advantages artificial intelligence cannot easily replicate.

Typical indicators

- Trusted adviser status
- Consistent analyst recognition
- Executive thought leadership
- Significant research influence
- High-profile industry visibility
- Strong stakeholder confidence

Authority is not a final destination.
It is an asset that must be continually reinforced and strengthened

Authority compounds over time



Authority is cumulative. Every piece of original research reinforces expertise. Every executive interview strengthens recognition. Every analyst relationship builds credibility. Every independent endorsement contributes to broader market confidence.

Collectively, these activities create reputation capital that supports commercial growth, strengthens resilience and improves long-term competitive position.

6.7 Why the model matters

The PRPR Authority Model encourages organisations to think differently about strategic communications. Rather than asking how much activity communications generates, it asks whether that activity is progressively moving the organisation from visibility towards recognised authority.

The qualities that define authority are also the qualities that artificial intelligence struggles to replicate. AI can generate articles, reports and presentations, but it cannot independently earn trust, build industry relationships or establish recognised expertise. Those qualities develop gradually through meaningful contribution, external validation and consistent demonstration of value.

Ultimately, the model shifts the conversation from communications outputs to business outcomes. The objective is not simply to create more content or secure more media coverage. It is to build recognised authority that supports sustainable growth.

Organisations that progress through these five stages will not simply become more visible. They will become more influential, more resilient and more competitive.

That is the journey represented by the PRPR Authority Model and, increasingly, it is the journey that will define market leadership in the age of artificial intelligence.

6.8 PRPR Authority Audit

The PRPR Authority Model can also be used as a simple maturity assessment.

Most organisations will recognise themselves within one of the five stages. The objective is not to reach the highest level as quickly as possible, but to understand which capabilities should be strengthened to progress over time.

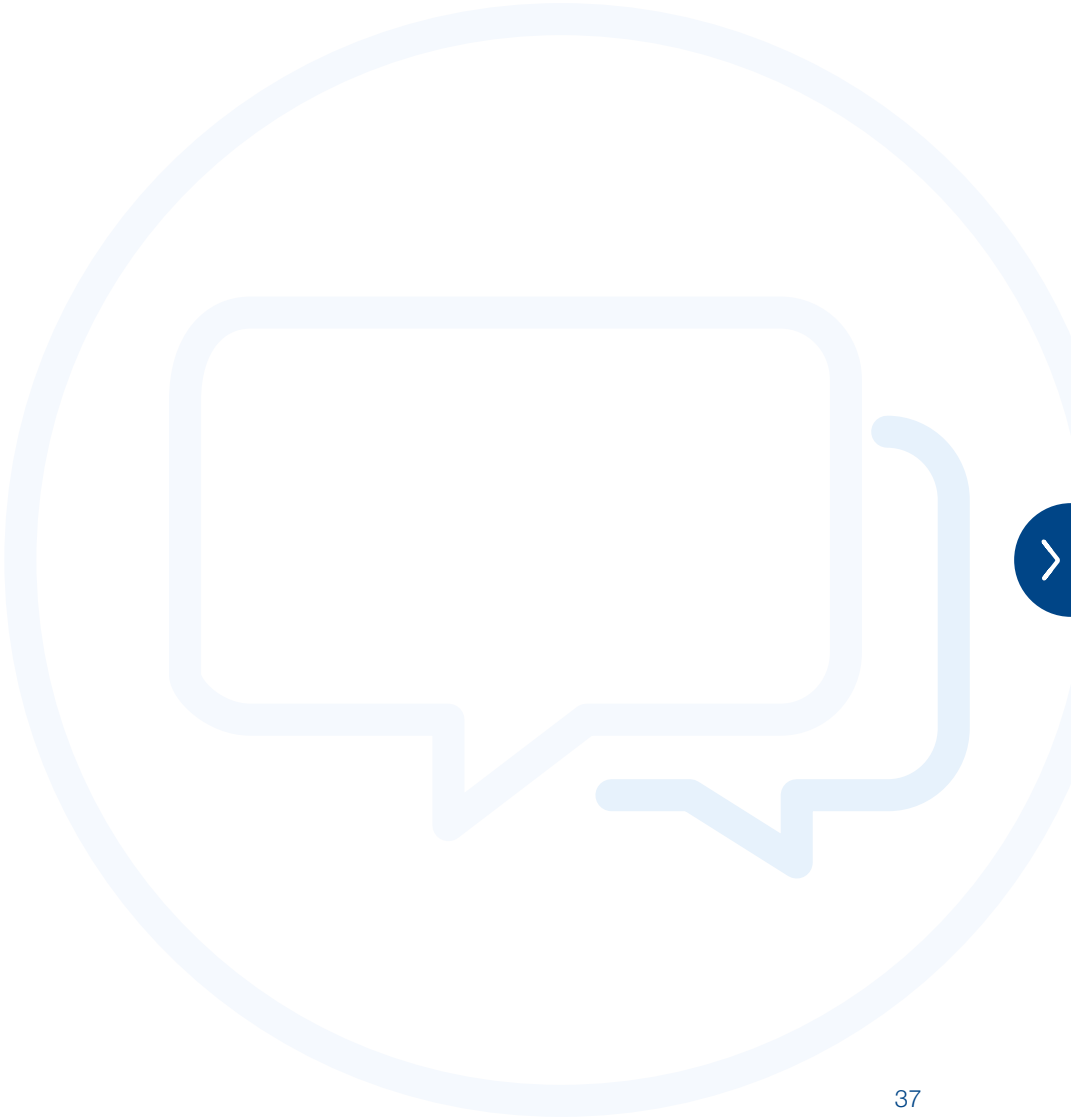
Audit

Stage	Characteristics	Typical Focus
1. Visibility	The organisation is active in the market but has limited recognition beyond existing customers.	Increase awareness and discoverability.
2. Recognition	Buyers recognise the organisation and associate it with particular technologies or services.	Strengthen positioning and consistency.
3. Credibility	Independent validation begins to reinforce market claims through research, media, analyst recognition and customer advocacy.	Build confidence and trust.
4. Influence	The organisation is regularly invited to contribute to industry conversations and shape opinion.	Expand influence and thought leadership.
5. Authority	The organisation is recognised as a trusted reference point within its market.	Sustain leadership and continue building authority.

6.9 Key questions for leadership teams

Senior leadership teams should periodically ask themselves:

- Are we simply visible, or are we genuinely recognised?
- Is our expertise independently validated, or primarily self-declared?
- Are journalists, analysts and industry peers seeking our perspective?
- Would AI-powered platforms be likely to identify us as an authoritative source?
- If our organisation faced a significant reputational challenge tomorrow, have we already built the trust needed to withstand it?
- Which stage of the Authority Model best describes our organisation today?
- What would it take to move to the next stage?



7. The future role of cybersecurity PR: from communications function to strategic business capability

The previous chapters explored how artificial intelligence is reshaping communications, intensifying market competition, changing the nature of discoverability and increasing the strategic importance of authority, reputation and trust. Considered individually, each of these developments presents a significant challenge for cybersecurity organisations. Taken together, they fundamentally redefine the role that strategic communications can play in organisational success.

The implications for public relations are profound.

For many years, PR has been viewed primarily as a communications discipline responsible for media relations, messaging, brand awareness and reputation management. These responsibilities are important, but they do not fully reflect the contribution that strategic communications makes to business performance.

As AI transforms both the creation and discovery of information, the role of PR is expanding beyond communications support to become a strategic business capability. Its value lies in helping organisations build the authority, trust and external validation that influence how they are perceived, discovered and ultimately selected.

This evolution is a fundamental change in the challenges organisations need communications to solve. The objective is not just to become visible. It is to become recognised as a credible, authoritative voice within an increasingly competitive and AI-driven marketplace.

The evolution of cybersecurity PR

Traditional Role	Strategic Business Capability
Media relations	Authority building
Brand awareness	Market influence
Product messaging	Executive positioning
Share of voice	Share of trust
Communications support	Strategic business capability
Visibility	AI discoverability
Campaigns	Reputation capital

This evolution also changes how communications should be evaluated.

Historically, communications programmes have been measured through activity-based metrics such as media coverage, impressions, social engagement and website traffic. While these are useful indicators, they reveal relatively little about the long-term value communications creates for an organisation.

Future communications programmes should be judged by what they enable. Questions such as these become increasingly important:

- Is the organisation recognised as an authority within its market?
- Are its executives and subject matter experts regularly sought out by journalists, analysts and policymakers?
- Does its research influence industry conversations?
- Is the organisation consistently represented within AI-driven search and recommendation platforms?
- Can it maintain stakeholder confidence during periods of uncertainty?
- Does its reputation contribute directly to growth, resilience and long-term competitive advantage?

These questions shift communications away from measuring activity and towards measuring strategic influence.

This is particularly important within cybersecurity, where market leadership depends on more than technological capability alone. The organisations that consistently shape the industry combine technical excellence with recognised expertise, influential executives, respected research programmes and sustained participation in wider industry conversations. Their competitive advantage extends beyond the products and services they offer. It is reinforced by their ability to explain emerging risks, contribute meaningful insight and become recognised sources of expertise.

Rather than simply amplifying organisational messages, PR creates assets that strengthen long-term competitive position. Thought leadership establishes recognised expertise. Original research builds authority. Executive profiling develops influence. Media engagement creates independent validation. Analyst relationships reinforce credibility, while consistent storytelling strengthens reputation over time.

PR creates strategic business assets

PR Activity	Strategic Asset Created
Thought leadership	Recognised expertise
Original research	Authority
Media engagement	Independent validation
Executive profiling	Market influence
Analyst engagement	External credibility
Speaking opportunities	Industry recognition
Crisis communications	Reputation resilience
Consistent storytelling	Reputation capital

Unlike campaign outputs, these assets compound over time. Every piece of original research reinforces credibility. Every executive interview strengthens market recognition. Every conference presentation extends influence. Every independent media citation contributes to broader perceptions of expertise. Collectively, these activities build reputation capital that supports commercial growth, strengthens organisational resilience and improves long-term market position.

They also strengthen discoverability. As discussed in the previous chapter, AI-powered search and recommendation platforms increasingly rely on external authority signals when identifying credible sources of information. The same investments that build reputation also improve an organisation's ability to be discovered and recommended within AI-driven information environments.

This is a significant departure from traditional approaches to digital visibility. Search optimisation, advertising and content production remain important, but they are becoming less effective when pursued in isolation. Organisations that consistently appear within AI-generated recommendations are unlikely to achieve that position through content volume or advertising spend alone. More often, they have built a broad ecosystem of recognised expertise, independent validation and trusted relationships that reinforce their authority across multiple channels.

This is one of the defining paradoxes of the AI era. AI has dramatically reduced the effort required to create content while simultaneously increasing the value of the qualities that are most difficult to automate. Expertise cannot be generated through a prompt. Credibility cannot be manufactured overnight. Independent validation cannot simply be purchased, and recognised authority is earned only through sustained demonstration of expertise, meaningful contribution to industry conversations and trusted relationships built over time.

7.1 Communications as a competitive advantage

For cybersecurity organisations, this changes how strategic communications should be viewed. Communications is a long-term investment in competitive advantage.

Just as organisations invest in technology, innovation, talent and intellectual property, they must also invest in building recognised authority. Authority influences how organisations are perceived, how their expertise is evaluated, how readily they are discovered and, ultimately, how successfully they compete.

This is particularly important because cybersecurity purchasing decisions are rarely based solely on product functionality. Buyers are making decisions that involve financial investment, operational risk and long-term partnership. They evaluate not only the capabilities of a product but also the credibility of the organisation behind it. They seek evidence that providers understand emerging threats, possess recognised expertise and can be relied upon when complex challenges arise.

Those same signals influence not only human decision-makers but also the AI platforms that are becoming an integral part of the research and evaluation process.

The organisations that recognise this shift now are likely to establish a significant competitive advantage over the coming decade. They will understand that market leadership is no longer determined solely by technological innovation or marketing reach. It is increasingly shaped by recognised expertise, independent validation and the ability to influence conversations across an AI-driven information ecosystem.

In many respects, this represents the future of cybersecurity PR. Its role is no longer defined just by media relations, content production or awareness generation. Its strategic value lies in helping organisations build recognised authority—an asset that strengthens discoverability, supports resilience, builds stakeholder confidence and contributes directly to long-term competitive advantage.

As AI reshapes how information is created, discovered and evaluated, organisations that consistently invest in expertise, original research, executive visibility and trusted third-party relationships will not simply communicate more effectively. They will be better positioned to earn trust, influence decisions and compete successfully within an increasingly complex marketplace.

Ultimately, the future of cybersecurity PR is not simply about communications.

It is about building the authority that underpins sustainable business growth.

7.2 From authority to action

We have established that AI discoverability is not only a question of technical optimisation. AI systems form their understanding of organisations from a much wider set of signals and building authority needs a sustained approach.

The following 12 principles bring those ideas together.

12 Best practices for building AI authority

Proven principles that strengthen visibility, credibility and authority in AI-driven environments.



1. FOCUS ON RELEVANCE

- Understand your audience, their challenges and priorities.
- Align your content and messaging to what matters.



2. CREATE ORIGINAL INSIGHTS

- Produce research, data and analysis that advance thinking.
- Offer a unique perspective that others can reference.



3. BUILD CREDIBILITY

- Back claims with evidence and real-world examples.
- Be accurate, transparent and consistent



4. EARN INDEPENDENT VALIDATION

- Secure third-party reviews, analyst mentions and citations.
- Let others validate your expertise.



5. AMPLIFY EXECUTIVE VOICE

- Position leaders as visible experts and spokespeople.
- Share insights at events, in media and online.



6. ENGAGE IN INDUSTRY CONVERSATIONS

- Contribute to key discussions, debates and communities.
- Add value and build relationships.



7. PUBLISH CONSISTENTLY

- Maintain a steady flow of high-quality, valuable content.
- Show up regularly across the right channels.



8. OPTIMISE FOR DISCOVERABILITY

- Ensure your content is easy to find and understand.
- Optimise for AI platforms, search and answer engines.



9. BUILD STRATEGIC RELATIONSHIPS

- Partner with credible brands, analysts and organisations.
- Collaborate to expand reach and credibility.



10. SEEK RECOGNITION

- Pursue awards, listings and industry acknowledgements.
- Use recognition to reinforce your authority.



11. MEASURE AND LEARN

- Track visibility, mentions, traffic and engagement.
- Use insights to refine and improve your approach.



12. STAY ADAPTIVE

- AI and buyer behaviour are evolving.
- Continuously adapt, innovate and stay ahead.

Authority is built through consistent expertise, meaningful contribution and external validation.

- Put your audience at the centre
- Deliver value consistently
- Build trust through relationships
- Stay focused on impact
- Innovate and evolve
- Follow these best practices and authority will follow.

8. Conclusion

AI is reshaping far more than cybersecurity technology. It is changing how organisations communicate, how expertise is evaluated, how information is discovered and, ultimately, how competitive advantage is established.

Throughout this paper we have explored how generative AI is transforming content creation, intensifying market competition, increasing the importance of recognised expertise and changing the relationship between communications, reputation and resilience. Individually, each of these developments presents a challenge. Collectively, they point to a fundamental shift in how cybersecurity organisations compete and how market leadership will be determined.

Historically, organisations sought competitive advantage by increasing visibility. Marketing and communications focused on generating awareness, improving search rankings and producing more content. Those objectives are important, but they are no longer enough.

As AI dramatically increases the volume of available information, visibility alone is less valuable. Content can now be created quickly and at scale by almost any organisation. What will be scarce is recognised expertise, not information. Buyers, journalists, analysts and AI-driven discovery platforms are looking beyond content itself towards the external signals that demonstrate authority, credibility and trust.

This changes the role of public relations. PR is no longer only responsible for generating awareness or supporting marketing campaigns. It helps organisations build strategic business assets that contribute to commercial growth, organisational resilience, AI discoverability and long-term competitive advantage. In doing so, communications is a contributor not only to reputation, but to business performance.

As the PRPR Authority Model demonstrates, organisations do not become market leaders through visibility alone. They progress from awareness to recognition, from credibility to influence and ultimately to recognised authority. That journey cannot be accelerated through content volume or advertising spend alone. It is built through the consistent demonstration of expertise, meaningful contribution to industry conversations and the accumulation of independent validation over time.

Perhaps the greatest paradox of the AI era is that the qualities becoming most valuable are also those that AI cannot easily replicate. AI can generate content, draft articles and summarise knowledge. It cannot independently earn credibility, establish trusted relationships or build recognised authority. Those assets are fundamentally human. They are developed through experience, expertise, original thinking and the confidence built through sustained engagement with customers, journalists, analysts, policymakers and the wider cybersecurity community.

For cybersecurity organisations, technology leadership will always be essential. Innovation will continue to matter and technical excellence will always provide the foundation for success. Increasingly, however, these strengths must be matched by recognised expertise, independent validation and the ability to influence the conversations that shape markets.

The organisations that thrive over the next decade will not just build better technology. They will build stronger authority. They will become trusted sources of expertise for customers, analysts, journalists, policymakers and the AI systems that increasingly influence how information is discovered and how decisions are made.

Public relations is entering a new era. No longer defined primarily by media relations, publicity or content production, it is a strategic business capability that helps organisations build sustainable competitive advantage through authority, influence and reputation.

Ultimately, the future of cybersecurity PR is about helping organisations earn the trust, recognition and authority that enable them to compete, grow and lead in the age of AI.



Passionate. Resourceful. Professional. Results-driven.

62 Ashwell Street Leighton Buzzard Bedfordshire LU7 1BG | Telephone: +44 (0)1442 245030 | Email: info@prpr.co.uk | www.prpr.co.uk