



An ALLIED UNIVERSAL Company

THE SECURITY RISKS OF MISINFORMATION & DISINFORMATION

When Digital Narratives Have
Real-World Consequences

Digital eBook

Table of Contents

INTRODUCTION.....03

THE NEW THREAT LANDSCAPE.....04

WHAT MISINFORMATION AND DISINFORMATION ACTUALLY DOES TO ORGANISATIONS.....06

WHY TRADITIONAL SECURITY MODELS ARE NOT ENOUGH.....09

THREE LAYERS OF RISK - CYBER, PHYSICAL, AND NARRATIVE.....11

DETECTION - IDENTIFYING MISINFORMATION AND DISINFORMATION THREATS EARLY.....14

RESPONSE - TURNING INSIGHT INTO ACTION.....16

BUILDING ORGANISATIONAL RESILIENCE.....19

THE ROLE OF TECHNOLOGY AND AI.....21

MISINFORMATION RISK READINESS CHECKLIST.....23

CONCLUSION.....25

Introduction

For years, we have seen misinformation and disinformation as a threat to a company's reputation. Many companies have seen this as a communications issue and have tried to manage it with traditional messaging, media response, and brand protection efforts. The convergence of digital narratives and physical threats has moved misinformation from a PR issue to a core security risk.

The [World Security Report](#) reveals that the way misinformation and disinformation manifest in the real-world is no longer limited to reputation damage, and the level of risk they pose has become serious.

Today, 73% of companies report being targeted by misinformation or disinformation campaigns, with many of these incidents linked directly to real-world disruption, threats, and acts of violence^[1]. 41% of security leaders say these narratives are motivating threat actors.

What does this mean for the future of security?

It means the nature of risk has fundamentally changed. The boundary between digital sentiment and physical action has dissolved; online narratives frequently act as a direct catalyst for real-world disruption. Misinformation and disinformation have become a business-critical security risk that requires a proactive security approach.

Definition: Misinformation vs. Disinformation

Misinformation is false or misleading information shared without the intent to cause harm, often by people who believe it's true.

Disinformation, by contrast, is deliberately created and disseminated with the intent to mislead, manipulate, or cause damage, whether to an organisation, an individual, or a broader audience.

[1] "A staggering 73% of CSOs say their companies have been targeted by a misinformation or disinformation campaign in the last year." - World Security Report- World Security Report

The New Threat Landscape:

From Digital Narratives to Physical Consequences

Misinformation and disinformation are not emerging risks. They are already here and accelerating.

[The World Economic Forum's 2025 Global Risks Report](#) ranks them as the number one global risk by severity over the next two years.

So, what's driving this shift?

It comes down to three interconnected forces: how narratives are created, how they spread, and what happens when they take hold in the real world.

1. ONLINE NARRATIVES

Narratives can form in minutes, often built on incomplete data, speculation, or deliberate manipulation.

Once they take shape, they start to influence how people see the world, shaping perception, shifting sentiment, and changing how events are interpreted.

And importantly, once a narrative takes hold, it becomes difficult to correct.

2. AMPLIFICATION SYSTEMS

Digital platforms accelerate the spread of information at scale.

Social media, online forums, and algorithm-driven systems push narratives across geographies and audiences in real-time. Issues that might once have remained local can now “go viral,” gaining global visibility within hours.

These systems are also designed to reinforce the user's existing beliefs. Narratives are reaffirmed, reactions are intensified, and opposing perspectives are obscured.

3. REAL-WORLD CONSEQUENCES

What begins online can escalate into coordinated, real-world activity.

As narratives spread, they begin to influence behavior. Organisations are seeing the impact in protests, trespassing, targeted threats, and broader operational disruption.

An Unstable Environment Accelerates Risks

These elements aren't new, but what's changed is the speed at which they interact, the scale at which they operate, and the level of integration between them.

Plus, these threats are unfolding in an already unstable environment, which only adds to their volatility.

According to the [World Security Report](#), 78% of Chief Security Officers believe geopolitical tensions will compromise supply chain security in the next 12 months.^[2]

While they may not seem related, a misleading narrative about a company can escalate underlying tensions, mobilise activist groups, or influence insider sentiment. From there, the impact can quickly extend to operational disruption, reputational damage, or direct security incidents. And when operations depend on complex, interconnected supply chains, even a small narrative-driven disruption can cascade into delays, shortages, and wider business impact.



[2] "Geopolitical tension will compromise the security of supply chains over the next 12 months, 78% of CSOs said." - World Security Report

What Misinformation and Disinformation Actually Does to Organisations:

From Narrative to Operational Impact

To understand misinformation and disinformation as a security threat, security teams should look beyond abstract risk and focus on what it does to organisations.

Misinformation and disinformation tend to follow a clear pattern. Narratives form, they gain traction, and they begin to influence behavior. As they spread, they shape perception, shift decision-making, and can trigger real-world consequences.



For organisations, this progression appears in four key areas of impact:

I. PHYSICAL SECURITY INCIDENTS

One of the most immediate effects of misinformation and disinformation is its ability to trigger physical-world incidents.

False or misleading narratives can mobilise individuals or groups, leading to protests, trespassing, and targeted disruption at physical sites. In some cases, this escalates into direct threats against people or property.

A well-known example is the [2016 “Pizzagate” conspiracy](#). A false online narrative claimed a Washington, D.C. pizzeria was linked to a child-trafficking ring. As the story spread, it prompted an armed individual to enter the restaurant and fire shots.

It’s a clear illustration of how online narratives can translate into immediate physical risk.

Senior executives are often particularly exposed. As public-facing representatives of the company, they are more likely to become focal points for narrative-driven targeting, increasing the need for protective measures.

2. INSIDER THREATS

Misinformation and disinformation do not just affect external actors. It can also affect people inside the business.

According to the [World Security Report](#), 39% of organisations identify misinformation and external radicalisation as the biggest drivers of intentional insider threats^[3].

Research also shows that misinformation can erode productivity, reduce engagement, and disrupt internal communication. As employees are exposed to conflicting or false narratives, confusion increases and workloads can rise.

Over time, narratives that undermine leadership, challenge organisational values, or spread false claims can shift employee sentiment and behavior. This can lead to disengagement, policy violations, or, in some cases, deliberate harmful actions.

This changes our understanding of insider threat. It's no longer just about access or behavior; it's also influenced by the narratives employees are exposed to outside of the organisation.

For more in-depth insights,
explore our Insider Threat eBook.
[Insider Threat: What You Need To
Know.](#)

3. FINANCIAL AND REPUTATIONAL DAMAGE

Misinformation and disinformation do not stay contained for long. What starts as a seamless innocent narrative quickly shows up in the numbers.

Following security incidents, like misinformation, 26% of organisations report revenue losses, with average losses of at least \$9 million^[4]. At the same time, institutional investors say these events can reduce the value of a publicly listed company by an average of 32%, which is 3% higher than two years ago^[5].

Why This Matters

These incidents have direct financial consequences, and the impact goes beyond individual organisations.

According to the World Economic Forum, the cost of exposure to misinformation is already significant globally. One [2019 study](#) cited in this article found that false information contributed to \$39 billion in stock market losses, along with \$17 billion in poor financial decisions. In total, the estimated annual cost reached \$78 billion worldwide.

Those numbers show that when misinformation escalates, it hits revenue, valuation, and long-term business stability.

[3] "39% say the influence of misinformation or external radicalisation is the biggest driver of intentional insider threats." - World Security Report

[4] "Following an internal or external breach, 26% of CSOs reported revenue losses, and companies on average lost at least \$9 million in revenue." - World Security Report

[5] "On average, an internal or external incident can impact the value of a publicly listed company by 32% according to surveyed institutional investors. That's 3% higher than two years ago." - World Security Report

4. OPERATIONAL DISRUPTION

Misinformation and disinformation can also disrupt day-to-day operations.

Narratives targeting supply chains, workforce practices, or corporate activity can lead to delays, interruptions, or breakdowns in critical processes. This may include disruption at key sites, workforce instability, or interference with logistics and distribution.

In an already volatile environment, shaped by geopolitical tension and supply chain pressure, misinformation and disinformation adds another layer of instability.

Why This Matters

Misinformation and disinformation can affect physical security, workforce stability, financial performance, and operational continuity. Yet many companies still address these impacts separately, treating them as disconnected issues instead of symptoms of the same underlying threat.

If your security approach is not designed to detect narrative-driven threats early and respond quickly, it will fall short.



Why Traditional Security Models Are Not Enough:

A Structural Mismatch Between Risk and Response

Misinformation and disinformation are not just creating reputational noise. Whether a narrative spreads unintentionally (misinformation) or is deliberately engineered (disinformation), it exposes a deeper problem: most organisations are not structured to manage a threat that moves from narrative to digital amplification to real-world disruption.

These threats do not stay in one lane. They begin as narratives, spread through digital channels and can quickly create real-world consequences — yet most organisations still respond in silos.

In practice, responsibility is divided: communications teams manage messaging, while security teams tend to engage only once a situation escalates. By then, the narrative has already gained momentum.

This creates three critical gaps:

I. SILOED TEAMS

In many organisations, risk is managed in silos — security focuses on physical protection and incident response, communications manage reputation and external messaging, and digital and cybersecurity monitor online environments — with limited coordination and shared visibility.

So, what happens in practice?

Early signals are missed, or they are identified but not escalated. An emerging narrative may be picked up in one part of the organisation without triggering a broader response. At the same time, security teams may be required to respond to incidents without understanding what is driving them.

The result is slower decision-making and a fragmented response.

2. REACTIVE RATHER THAN PROACTIVE POSTURE

Most security models are built to respond after an incident has occurred.

In the context of misinformation and disinformation, that creates a disadvantage. By the time a narrative escalates into a protest, threat, or disruption, the organisation is already reacting.

So, what needs to change? Attention must shift earlier.

That means identifying emerging narratives, assessing their potential impact, and taking action before they escalate into physical incidents. Without a proactive model, response times often lag behind the speed of digital amplification.

3. LACK OF REAL-TIME MONITORING

Misinformation and disinformation evolve quickly.

Narratives can gain traction within hours, driven by amplification across digital platforms. Many organisations lack continuous, real-time visibility into how these narratives are developing. Monitoring efforts are often limited in scope or disconnected from broader security intelligence. This creates a blind spot.

Without early visibility, it becomes difficult to detect when a narrative is gaining momentum, being coordinated, or starting to influence behaviour.

And when that visibility is missing, the opportunity to act early is lost.

Expanding the Role of Security

These gaps are emerging at a time when the role of security is already evolving.

According to the [World Security Report](#), security leaders are increasingly expected to engage with technology, data, and communications. The scope of security is expanding in response to a more complex and interconnected risk environment.

But often, operating models have not yet caught up.

A Need for an Integrated Approach

Current models are not well suited to a threat that begins with a narrative, scales through digital systems, and leads to real-world consequences.

A more integrated approach is required.

One that connects teams, enables real-time visibility, and supports earlier intervention across the full lifecycle of a threat. Without that shift, the same challenges persist: delayed detection, limited coordination, and increased exposure to fast-moving risks.

Three Layers of Risk - Cyber, Physical, and Narrative:

A Framework for Understanding and Managing Misinformation and Disinformation Threats

Managing misinformation and disinformation as a security risk requires a clear way to see how it moves and how different types of risk connect.

Traditional security models separate cyber and physical domains. Misinformation and disinformation ignore those boundaries. They travel across them, evolving as they spread and growing in impact along the way.

A more effective approach is to view misinformation and disinformation risk through three interconnected layers: narrative, digital, and physical.



I. NARRATIVE LAYER

Where Risk Originates

This is where misinformation and disinformation begin.

False, misleading, or manipulated information shapes how events, organisations, or individuals are perceived. These narratives may arise organically, through misunderstanding or incomplete information, or be deliberately constructed to influence opinion or behavior.

At this stage, the impact is mostly on perception and intent. Narratives change how audiences interpret reality, create distrust, and frame organisations in ways that make escalation more likely.

2. DIGITAL LAYER

Where Risk Is Amplified

The digital layer is where narratives gain scale. Social media platforms, online forums, and algorithm-driven systems act as accelerators. They spread narratives quickly, reach targeted audiences, and reinforce beliefs through interaction.

This layer controls speed, reach, and intensity. A narrative that gains traction here can move fast from a niche concern to a widespread issue, raising the odds of real-world consequences.

It's also where coordinated activity, like organised campaigns or targeted dissemination, can push escalation further and faster.

3. PHYSICAL LAYER

Where Impact Occurs

Finally, this is where narratives turn into action.

As misinformation and disinformation influence behaviour, they can trigger protests, trespassing, threats, and operational disruption. Physical security teams respond most visibly at this stage, but by the time they act, the threat is already in motion and often intensified.

How Risk Moves Across Layers

Misinformation and disinformation won't stay in one layer for long. They move from:



A single misleading claim can gain visibility online and ultimately shape real-world actions.

A [2018 MIT study](#) found that false news reports were 70% more likely to be retweeted than true stories, reaching the first 1,500 people 6x faster.

The further it moves, the faster it escalates, and the harder, costlier, and riskier it becomes to intervene.

Implications for Security Strategy

The [World Security Report](#) highlights the growing convergence of cyber and physical security, and the need for integrated, cross-domain risk management.

This layered framework reinforces that shift.

Focusing only on physical response means reacting to outcomes rather than managing risk at its source. Effective security begins earlier: at the narrative and digital layers, where threats can be detected, assessed, and mitigated before they escalate.

That requires two changes:

1. **Earlier detection** – visibility into emerging narratives and digital amplification patterns.
2. **Coordinated response** – linking insight from digital environments to action in the physical world.

By adopting this layered view, organisations can move from reactive incident response to a proactive, intelligence-led approach to security.



Detection - Identifying Misinformation and Disinformation Threats Early

From Visibility to Early Intervention

Misinformation and disinformation become dangerous when they reach the physical world. Security depends on spotting them long before that point. The challenge is not just recognising false narratives. It's detecting them early, while they are forming, before they spread, and before they trigger real-world consequences. Traditional monitoring is not enough. Organisations need intelligence-led detection that links signals across platforms, channels, and behaviors.

Disinformation adds another layer of complexity. Because it is intentional, detection must look beyond whether a claim is false and focus on how it is being pushed: signs of coordination, impersonation, repeated seeding across platforms, and abnormal amplification patterns. Identifying these signals early helps teams distinguish organic confusion from engineered campaigns and prioritise response accordingly.

Insights from the [World Security Report](#) show that 44% of organisations already use online monitoring as a mitigation tactic^[6]. Visibility matters, but monitoring alone is not enough. Signals must be interpreted, risks assessed, and patterns of escalation identified.

There are four main ways to pay attention to these signals so we can spot threats early:

I. SOCIAL MEDIA MONITORING

Social media is where most narratives start. Tracking platforms, forums, and trending topics reveals emerging stories, sudden spikes in attention, and high-risk actors driving content. Monitoring shows not only what is being said, but how it is evolving, and whether it could escalate.

For example, a sudden surge of coordinated posts questioning company practices can indicate a narrative ready to spill into protests or targeted threats.

[6] "Adopting enhanced security measures is the top tactic taken by companies to mitigate the threat of violence to leaders, 49% of CSOs say. This is followed by risk assessment and the monitoring of online threats at 45% and 44%, respectively." - World Security Report

2. DARK WEB SIGNALS

Not all threats appear publicly — encrypted chats, closed forums, and dark web spaces often reveal early intent. Discussions about specific companies, plans for action, or harmful narratives may appear there before reaching mainstream channels.

3. THREAT INTELLIGENCE INTEGRATION

Misinformation and disinformation intersect with broader risks, geopolitics, activism, and known threat actors. Connecting narrative monitoring with threat intelligence builds a complete picture. Correlating online activity with past incidents, known actors, or risk trends turns scattered alerts into actionable insight.

Without this integration, early warning signals remain fragmented and easy to miss.

4. PATTERN RECOGNITION AND THE ROLE OF AI

The speed and volume of online content make human monitoring alone impossible. AI identifies unusual activity, coordinated campaigns, and narratives gaining momentum. It flags spikes in attention, networks of accounts acting together, and emerging escalation patterns.

From Signals to Insight

Data is meaningless without context. Teams must filter noise, assess risk, and decide what to act on. Early detection gives time to intervene before a narrative triggers a physical incident, helps protect people, and limits operational disruption.

Organisations with strong detection capabilities see threats first. They respond first, prevent escalation, and intervene before disruption occurs.



Social Media
Monitoring



Dark Web
Signals



Threat Intelligence
Integration



Pattern Recognition
& Role of AI

Response - Turning Insight Into Action:

From Detection to Coordinated Security Response

Early detection gives organisations an advantage, but insight alone does not stop threats. Action is what reduces risk.

Preventing escalation means translating intelligence into coordinated, timely responses. That requires a structured model that aligns teams, prioritises security outcomes, and keeps pace with fast-moving narratives.

Response is not primarily a communications function. Messaging may play a role, but the main goal is to help protect people, assets, and operations as risk moves toward the physical domain.

Disinformation also changes how you respond. Because some campaigns are designed to provoke engagement and generate more buzz, the right move is not always to correct publicly. A disciplined response model evaluates intent, likely amplification effects, and potential harm, then selects the least escalatory action that protects people and operations—ranging from quiet monitoring and internal readiness to targeted countermeasures and public messaging when necessary.



Cross-Functional Coordination

Effective organisations establish clear coordination between security, communications, and leadership teams. Roles and responsibilities are defined in advance. Escalation protocols are ready when narratives start to gain traction.

Without alignment, responses become fragmented. Delays multiply risk and reduce the chance of containing escalation.

Executive Protection Protocols

Organisations must adapt executive protection in real-time. This can mean adjusting travel plans, increasing monitoring, boosting close protection, or adding security measures around public appearances.

The [World Security Report](#) underscores this risk: 97% of institutional investors say executive protection is a priority^[7]. This reflects both the seriousness of narrative-driven threats and the expectation that organisations actively manage them.

Site-Level Preparedness

Organisations must prepare sites for protests, trespassing, or coordinated disruption. This includes training staff, reinforcing access controls, and aligning incident response plans with real-time intelligence.

Prepared sites enable faster, controlled responses and reduce the chance of escalation.

Scenario Planning

Teams must plan for multiple outcomes, from minor reputational issues to significant physical disruption. Scenario planning maps how narratives could evolve, identifies trigger points, and rehearses coordinated responses across functions.

Being prepared allows organisations to act decisively under pressure, rather than reacting after the damage has started.

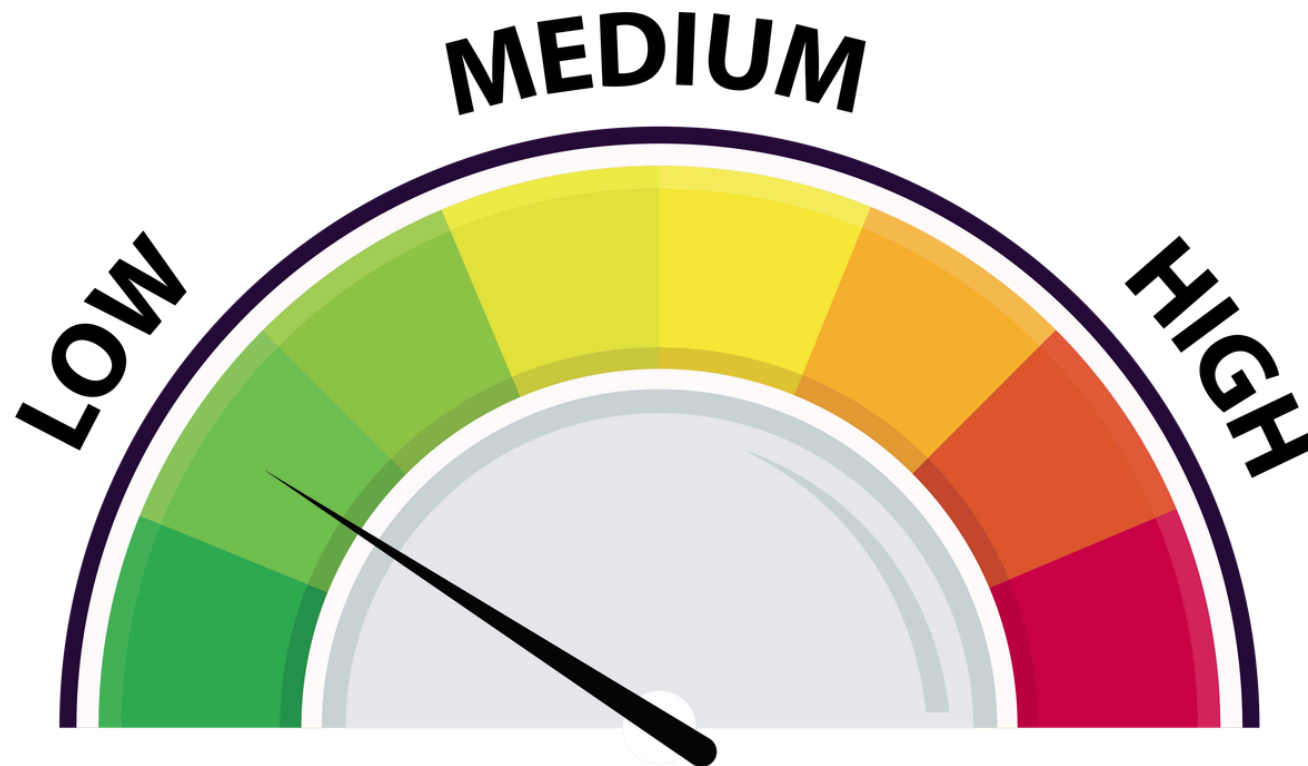
[7] "97% of institutional investors state that it is important for companies they invest in to provide physical protection for executives" - World Security Report

From Insight to Intervention: Embedding Response into Your Operations

A response is only as effective as the organisation's ability to act on intelligence.

Delayed or uncoordinated actions let narratives grow, increasing both scale and severity. Timely, aligned intervention reduces risk before it reaches the physical domain.

Effective response is not a one-time effort. It must be integrated into teams, processes, and decision-making structures. This builds resilience, not just for a single incident, but for adapting continuously to an evolving threat landscape.



Building Organisational Resilience:

Strengthening the Ability to Withstand and Adapt

Responding to individual misinformation or disinformation incidents is necessary, but not enough.

As misinformation and disinformation become persistent and evolving, organisations need to move from reactive response to long-term resilience: the ability to anticipate, withstand, and adapt to narrative-driven risk.

Resilience depends on more than tools or isolated processes. It relies on how security is embedded across people, culture, and strategy.

Building this capability requires work in the following areas:

WORKFORCE AWARENESS AND TRAINING

Employees are both potential targets and amplifiers of misinformation and disinformation.

Without awareness, staff may unintentionally spread false narratives or miss early warning signs. With proper training, the workforce becomes an additional layer of defense. Teach employees to identify misinformation and disinformation, understand its potential impact, and respond appropriately.

This includes spotting suspicious content, escalating concerns through proper channels, and following security protocols during periods of heightened risk. Over time, this builds a security-aware culture where narrative-driven threats are recognised and mitigated as part of day-to-day behaviour.

LEADERSHIP ALIGNMENT

Resilience depends on alignment between security leaders and executive decision-makers.

Misinformation and disinformation-driven risks evolve rapidly and require coordinated action. Misaligned priorities, unclear escalation thresholds, or inconsistent strategies create delays and increase exposure.

Leaders must understand the security implications of misinformation and disinformation and act on that understanding. Narrative risk should be integrated into existing risk frameworks and considered alongside other strategic threats. The [World Security Report](#) highlights this need: 92% of institutional investors say physical security should be elevated within business strategy, compared with 82% of Chief Security Officers^[8].

[8] "In fact, 92% of institutional investors surveyed said physical security should be a higher strategic priority for businesses, compared to 82% of CSOs." - World Security Report

EMBEDDING SECURITY INTO BUSINESS STRATEGY

Security cannot operate in isolation, it must influence how you plan, operate, and make decisions.

This means incorporating security considerations into site operations, supply chain management, communications, and crisis planning. Embedding security at this level helps build responses into the organisation's operating model, not improvised under pressure.

FROM CAPABILITY TO RESILIENCE: A CONTINUOUS EFFORT

It's time to move beyond responding to incidents. Instead, we need to anticipate threats, adapt to changing conditions, and maintain continuity under pressure.

Managing misinformation and disinformation requires sustained investment in people, processes, and alignment across the organisation. The challenges will continue to evolve with technology, geopolitics, and social dynamics.

If you treat resilience as a one-time project, you will fall behind. If you embed it into structures, culture, and strategy, you will gain the ability to manage uncertainty and reduce the impact of future incidents.

And importantly, response does not always mean engagement. In some cases, disinformation campaigns are designed to provoke a public reaction and generate more attention.

A resilient organisation has a strategic, methodical way to evaluate each incident, decide whether to act, counter, or monitor, and choose the next step that reduces risk without amplifying the narrative.



The Role of Technology and AI:

Scaling Detection, Enhancing Decision-Making

The speed and scale of misinformation and disinformation create a challenge that manual processes alone cannot meet. Narratives emerge, evolve, and spread across multiple platforms in hours, generating more volumes of data than humans can track.

Technology, and increasingly artificial intelligence, enables organisations to detect, monitor, and respond to these threats more effectively. AI is not a replacement for human judgment. Its purpose is to amplify the capabilities of security teams, helping them operate with greater speed, precision, and insight.

The [World Security Report](#) reflects this shift: 93% of organisations plan to use technology to reduce security threats, and nearly half are specifically investing in tools to enhance human capabilities in threat detection and prevention^[9].

Three use cases illustrate how technology strengthens security:

THREAT DETECTION

AI can identify emerging risks earlier and more accurately than manual monitoring alone. By analysing data across platforms, AI can detect anomalies, unusual activity patterns, and signs of coordinated campaigns. This includes spikes in narrative traction, networks of related accounts, or patterns that signal potential escalation.

These capabilities create stronger early warning systems, enabling organisations to act before narratives fully develop.

MONITORING AT SCALE

Comprehensive visibility is impossible without technological support.

AI-powered tools track narratives, sentiment, and activity across multiple platforms in real time. This extends beyond public social media to forums, niche platforms, and hidden digital environments where narratives often originate or evolve. By scaling monitoring, organisations maintain a consistent, detailed view of the threat landscape, reducing blind spots and increasing readiness.

[9] "Unsurprisingly, security decision makers are planning to use technology to reduce the likelihood of security threats (93%) and nearly half (49%) said they plan to use technology to enhance human capabilities to improve threat detection and help prevent incidents." - World Security Report

RISK ANALYSIS AND DETECTION SUPPORT

Data alone does not reduce risk. Security teams need actionable insight. AI helps by aggregating, correlating, and prioritising information, linking narrative trends to known threat actors, historical patterns, and external risk factors.

This transforms fragmented signals into structured intelligence, enabling faster, more targeted decision-making.

AUGMENTING HUMAN JUDGEMENT

AI expands speed and scale but can't replace human expertise. Assessing intent, context, and operational priorities requires judgement, experience, and organisational understanding.

The most effective organisations combine advanced technology with skilled security teams, helping to ensure that insights are accurate and actionable.

ENABLING A MORE ADAPTIVE SECURITY MODEL

Misinformation and disinformation evolve continuously. Integrating AI into detection, monitoring, and analysis allows organisations to operate in real-time and adjust to changing conditions.

Without these capabilities, maintaining visibility and control in a rapidly shifting information environment becomes significantly more difficult. Advanced technology, paired with human intelligence, provides the scale required to monitor and mitigate these high-velocity threats.



Misinformation & Disinformation Risk Readiness Checklist

Understanding misinformation and disinformation risk is just the first step. The next is asking: how prepared is your organisation to manage it?

Misinformation and disinformation-driven threats move fast and cut across multiple functions. Organisations that respond effectively do not scramble, they already have visibility, defined responsibilities, and coordinated response mechanisms in place.

Use this checklist to evaluate readiness and identify gaps before a narrative escalates into real-world impact.



Detection and Monitoring



Intelligence and Analysis



Coordination and Response



Protection and Preparedness



Strategy and Resilience

MISINFORMATION AND DISINFORMATION RISK READINESS CHECKLIST

Detection and Monitoring

- ☐ Do you have real-time visibility into emerging narratives across social media and digital platforms?
- ☐ Are you tracking shifts in sentiment, coordinated activity, and early escalation signals?
- ☐ Do you include dark web and closed-channel intelligence in your monitoring?

Intelligence and Analysis

- ☐ Are narrative insights integrated with broader threat intelligence?
- ☐ Can you separate low-level noise from high-risk signals that require immediate action?
- ☐ Are technology and AI tools in place to support pattern recognition and early detection?

Coordination and Response

- ☐ Are security, communications, and leadership teams aligned on roles and responsibilities?
- ☐ Do clear escalation protocols exist for misinformation- and disinformation-driven threats?

Protection and Preparedness

- ☐ Are executive protection measures adaptable to emerging narrative-driven risks?
- ☐ Are physical sites prepared to handle protests, trespassing, or coordinated disruption?
- ☐ Do you regularly conduct scenario planning for potential misinformation incidents?

Strategy and Resilience

- ☐ Is misinformation and disinformation risk integrated into broader security and business strategy?
- ☐ Are employees trained to identify and respond to misinformation?
- ☐ Do leadership teams treat narrative-driven threats as a strategic security priority?

Interpreting Your Results

If you can confidently answer “yes” across these areas, you are better equipped to detect, respond to, and mitigate misinformation and disinformation risks.

Next Steps

Close gaps by improving structure, intelligence sharing, and coordination, with external expertise helping strengthen capabilities and prevent issues before they escalate.

Conclusion:

Moving from Intelligence to Action

Misinformation no longer stays confined to a screen; it travels across domains to create real-world consequences for your people and operations. Managing these risks requires more than just awareness—it requires a partner who can connect the dots between an emerging digital narrative and a physical response.

At G4S, we support organisations at every stage of this journey. Whether it's leveraging our Global Security Operations Centres (GSOC) to monitor emerging threats or deploying specialised protection to a high-risk site, we provide the tools to help you build a resilient, proactive programme. By integrating monitoring, technology, planning, and on-the-ground expertise, we help you stay ahead of misinformation risk before it becomes a physical reality.

Disclaimer

This eBook was written by G4S. This guide may contain forward-looking statements including statements regarding our intent, belief or current expectations with respect to the physical and technology security services businesses and operations. Readers are cautioned not to place undue reliance on these forward-looking statements.

The intention of this eBook is not to present a complete and all-encompassing view on the topic, but to elaborate and provide qualitative insights from G4S experts as a thought-starter for the creation of the security future of your organisation.

The information provided by G4S in this eBook is for general informational purposes only. We make no representation or warranty of any kind, express or implied, regarding the accuracy, adequacy, validity, reliability, availability or completeness of any information. Under no circumstance shall we have any liability to you for any loss or damage of any kind incurred as a result of the use of or reliance on any information provided in this presentation.

This eBook and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the law of England and Wales. The courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with this eBook or its subject matter or formation.



An ALLIED UNIVERSAL Company

THE SECURITY RISKS OF MISINFORMATION & DISINFORMATION

When Digital Narratives Have
Real-World Consequences

g4s.com