Brighton
You insure, We ensure

INSIGHTS

MARCH 2025

RETHINKING EMERGING RISK ANALYTICS

THE CRITICAL ROLE OF GLOBAL MEDIA INTELLIGENCE IN CAPTIVE STRATEGIES

BROKERS AS RISK ARCHITECTS IN THE NEW RISK ECONOMY

MITIGATING SOCIAL ENGINEERING FRAUD

HEALTH & SAFETY: A TOP CONCERN FOR D&O

Editor's Note

Dear Readers,

The nature of risk is changing, and fast. In this March issue, we take a closer look at how traditional models and mindsets are being tested in a world defined by disruption.

The lead article explores how emerging risks, like global supply chains and reputational threats, exceed traditional insurance methods. It highlights the evolution of captives from niche solutions to strategic resilience tools as historical data becomes less reliable.

The second feature article highlights the importance of foresight and flexibility amidst rising geopolitical instability, cyber incidents, and climate uncertainty. In this new risk economy, brokers are now evolving from mere intermediaries to strategic partners, assisting businesses in navigating uncertainty.

We also examine the changing landscape of cyber risk. Social engineering fraud teaches us that breaches aren't solely the result of harmful code. Often, the most significant vulnerability stems from human trust.

Finally, we examine a major shift in the D&O landscape. Health and safety, once tucked under regulatory compliance, have now emerged as central to corporate governance. For D&O insurance to stay relevant, it must evolve alongside these new expectations.

Together, these articles remind us that resilience in today's environment is not about avoiding risk—it's about understanding it differently. And that begins with asking better questions, challenging assumptions, and being prepared to rethink the fundamentals.

Annie Undikai

Annie Undikai
Managing Editor

Brighton
You insure, We ensure
INSIGHTS

FEBRUARY 2025

IN THIS ISSUE

Brighton
You insure, We ensure

Empowering Your Insurance Journey

You Insure, We Ensure

At Brighton, we don't just provide solutions — we empower your journey to excellence. Our cutting-edge software, business solutions and dedicated technical support are crafted to propel your business forward in the competitive insurance industry.

Our Solutions:

- Licensing & Compliance
- Accounting Services
- Webbie, Cloud-Based Accounting Software
- Payroll Services
- GST Reporting
- Shariah Advisory
- Comprehensive Captive Management
- Run-Off Management
- Serviced Office Facilities

For more information, scan the QR code

Rethinking Emerging Risk Analytics

The Critical Role of Global Media Intelligence in Captive Strategies

Emerging risks today move at the speed of information. From sudden supply chain failures to reputational damage driven by viral headlines, organisations face a more complex and fast-evolving risk landscape than ever before. Traditional risk models are no longer enough. Captives are at the frontlines of confronting this change and must now look beyond structured data sets and historical loss trends.

To stay ahead, they must adopt a more dynamic approach to risk analytics. One that goes beyond conventional actuarial models and one that integrates emerging risk analytics with real-time intelligence from global media sources.

A Shift Toward Global Intelligence

Emerging risk isn't just about probability. It's about perception, timing, and exposure. Increasingly, these dimensions are shaped not in boardrooms, but in headlines, hashtags, and policy briefings. That's where global media intelligence steps in.

By analysing real-time narratives from news outlets, regulatory bulletins, industry reports, and social media; insurers can detect weak signals long before they escalate into financial losses. Traditional datasets often lag. Media, on the other hand, offers a live pulse on how risk is evolving in the real world.

This shift isn't hypothetical. It's already reshaping how advanced insurers and captives think about risk. Media-based risk intelligence provides early warnings on threats that can derail operations, damage brand equity, or erode stakeholder trust. These include geopolitical disruptions, supply chain bottlenecks, cyber threats, and reputational crises—many of which originate far outside the conventional underwriting lens.

For instance, an uptick in civil unrest reported across multiple regions may not show up in claims data until much later. By monitoring media trends, captives can proactively adjust coverage, notify risk managers, or reallocate reserves.

Similarly, any sudden scrutiny over environmental practices that are driven by investigative journalisms or activist campaigns, can signal reputational exposure that actuarial models have yet to capture.

Media-based risk intelligence provides early warnings on threats that can derail operations, damage brand equity, or erode stakeholder trust.

What Is Media-Based Intelligence?

Media-based intelligence is the systematic use of global media sources to identify, monitor, and assess emerging risks. Media monitoring provides risk assessors with a wealth of publicly available information, from which intelligent insights, trends, and analyses can be drawn. This includes news reports, social media signals, expert commentary, and industry updates.

Unlike traditional risk data, which often lags behind events, media intelligence captures sentiment and signals in real time. It allows insurers to see not just what is happening, but how the world is reacting. That's a crucial distinction in an age where perception can shape markets and reputation is the new currency.

Captives as Risk Labs

Once considered mere cost-saving tools, captives are rapidly becoming innovation hubs. Forward-looking organisations are using them to pilot cutting-edge risk technologies in a controlled environment. For instance, several large multinationals now run climate stress-testing models within their captives, using satellite data and AI-driven weather analytics to better anticipate natural catastrophe exposures.

Others are leveraging captives to experiment with cyber risk quantification models. They are refining cyber exposure pricing through the integration of threat intelligence feeds, dark web monitoring, and behavioural data, often achieving greater accuracy than traditional commercial markets.

Supply chain visibility is another frontier. Some captives are testing blockchain-based tools to track logistics and supplier risks in real time. This allows for more agile underwriting of contingent business interruption coverage, especially in volatile sectors like manufacturing and pharmaceuticals.

A prominent example is RiskStream Collaborative, which teamed up with ChainThat to introduce a blockchain-based tool designed to enhance supply chain risk management.

But intelligence alone is not enough. To extract true value, captives must connect these insights with their actuarial, capital optimisation, and exposure management strategies. Tools exist to simulate future scenarios, quantify hard-to-measure exposures, and model capital requirements accordingly. The question is: are they being used well?

From Insight to Action

Too often, insurers collect data but fail to act on it. Emerging risk analytics must move from static reports to strategic decision-making. This means integrating media intelligence with underwriting, pricing, and capital allocation. It also means training teams to understand the nuance behind qualitative signals.

For example, a sudden spike in media attention around a supplier's labour practices might not yet affect financials—but could soon trigger regulatory scrutiny or consumer backlash. Captives equipped to model this exposure in real time can respond faster, adjust their coverage structures, or ring fence the risk entirely.

Media analytics empowers organisations to distinguish between noise and meaningful signals. This enables them to evaluate not only what is occurring but also how it is perceived, who it impacts, and what potential outcomes it may lead to. This type of insight is valuable not only for managing crises but also for improving long-term strategic planning.

Incorporating media signals into current exposure models allows captives to obtain a more dynamic perspective on potential vulnerabilities, shifts in sentiment, and the timing of necessary interventions.

Noise and Misinformation

As captives embrace media-based intelligence, one critical challenge stands out: not all information is accurate. The rise of fake news where misinformation disguised as fact, can distort perceptions, trigger false alarms, and lead to misguided decisions. In the context of emerging risk, reacting to inaccurate narratives can be just as damaging as missing real threats.

This risk is especially acute when decisions are made quickly. An overhyped media story about a regulatory crackdown, for example, might prompt unnecessary adjustments to risk models or capital reserves. Conversely, dismissing early coverage of a legitimate threat because it seems speculative can leave captives exposed.

That's why the quality of media intelligence matters as much as the quantity. Filtering noise from signal requires more than keyword tracking. It demands advanced tools, human oversight, and contextual understanding.

Modern media analytics platforms use AI to assess source credibility, sentiment trends, and cross-platform consistency. But technology alone isn't enough. Risk managers must apply judgment. They must understand the difference between viral panic and verifiable risk.

Ultimately, the goal isn't just to gather data. It's to generate insight. And that requires a disciplined approach—one that accounts for misinformation, validates sources, and anchors intelligence in a wider strategic context.

In a world where perception often moves faster than truth, the ability to navigate misinformation is not a nice-to-have. It's a core skill for future-ready captives.

The Future Is Proactive

The role of captives is evolving. No longer just passive holders of risk, they are becoming active enablers of resilience. To fulfill this role, they must widen their lens and embrace more dynamic sources of intelligence.

Emerging risks don't wait for quarterly reports or spreadsheet models. They unfold in real time and often in headlines, markets, or public sentiment. Captives can't afford to lag behind. Neither can their strategies.

In today's volatile risk environment, foresight isn't optional. It's essential. The cost of missing an early signal is steep. But the value of responding ahead of the curve is even greater. Captives that embed global intelligence into their frameworks gain a meaningful edge. They don't merely react to change—they anticipate it. And in doing so, they transition from insurers of risk to architects of resilience.

With the right analytics guided by modern platforms, and interpreted with precision, captives can evolve from compliance-driven entities to strategic instruments for long-term value creation. In a world defined by constant disruption, advantage belongs to the best-informed.

In a world where perception often moves faster than truth, the ability to navigate misinformation is not a nice-to-have. It's a core skill for future-ready captives.

BROKERS

AS RISK ARCHITECTS *in the* NEW RISK ECONOMY

In today's volatile environment, risks are more complex, interconnected, and less predictable than ever. From geopolitical unrest and cyber attacks to climate change and global pandemics, the limitations of traditional insurance are becoming clear. Businesses now require more than protection, they need foresight, strategy, and adaptability. That's where brokers come in.

The role of brokers is evolving. No longer mere intermediaries, they are stepping up as risk architects. They craft bespoke solutions, embed alternative risk strategies, and serve as trusted advisors. In this new risk economy, brokers are the vital link between uncertainty and resilience.

Rise of the New Risk Economy

The global risk landscape is undergoing a profound transformation. The traditional insurance model—built on historical loss data, standardised coverage, and stable risk pools—is struggling to keep pace with a world defined by volatility, complexity, and rapid change. As risks evolve, so too must the mechanisms used to manage and transfer them.

Today's economy is shaped by a mix of known and emerging threats: climate change, cybercrime, geopolitical instability, supply chain fragility, and social unrest. These risks are no longer isolated events. They interact, amplify one another, and create cascading consequences that conventional insurance products are often ill-equipped to address.

At the same time, the insurance industry faces internal pressures. Capital constraints, rising reinsurance costs, and tighter underwriting are contributing to hard market conditions across many lines. In 2024, global insured losses from natural catastrophes exceeded $100 billion for the fifth consecutive year—well above the 10-year average of $89 billion.

This is driven in large part by secondary perils such as floods, wildfires, and severe storms with losses remained significant at $136 billion in total. Of this, around $67 billion was covered by insurance. However, these events are increasing in both frequency and severity, challenging traditional actuarial assumptions and pricing models.

Meanwhile, businesses are shifting their expectations. They want more than coverage—they want insight, agility, and strategic value. A growing number of risk managers are demanding tailored, data-informed solutions that align with enterprise risk management goals. In an Aon survey, 84% of global executives said their risk exposure had increased over the past three years, yet only 42% felt they were adequately prepared to manage it. The gap between risk and readiness is widening.

At the same time, intangible risks, i.e. those that are harder to quantify, model, and insure; are becoming more prominent and threatening to business continuity. Cyberattacks are a prime example. Once considered an IT issue, cyber risk has now escalated into a board-level concern with far-reaching implications for operations, customer trust, as well as regulatory compliance.

Environmental, Social, and Governance (ESG)-related exposures are also gaining urgency. Companies are under increasing scrutiny from regulators, investors, and the public to demonstrate sustainable and ethical practices. Failure to meet ESG expectations can result in legal action, loss of capital, or reputational damage. A misstep in governance, a poorly handled environmental incident, or social backlash from stakeholders can have swift and lasting financial consequences.

Reputational risk, which is closely linked to both cyber and ESG factors, is now a critical concern for C-suites. In the digital age, a single incident can go viral and cause significant brand damage overnight. According to a Deloitte survey, 87% of executives rated reputation risk as more important or much more important than other strategic risks, yet fewer than half felt adequately prepared to manage it.

These intangible risks are particularly challenging because they often fall outside the boundaries of traditional insurance policies. They are fast-moving, difficult to predict, and require a different kind of response; one that blends advisory services, real-time data, and non-traditional risk transfer tools.

The confluence of external pressures and rising client expectations is giving rise to what many are calling the “new risk economy”—a system where risk is not just transferred but actively managed, mitigated, and reimagined. It is an economy that demands creativity, adaptability, and forward-looking solutions.

In this evolving landscape, conventional methods are insufficient. The insurance industry needs to broaden its range of tools. Central to this transformation is the broker, who has transitioned from a transactional role to becoming a strategic partner, assisting organisations in developing resilience and gaining a competitive edge.

Brokers as Risk Architects

In this new risk economy, brokers are transforming from just placing insurance to becoming true risk architects. They are now experts who design, structure, and manage comprehensive risk strategies that reflect the complex nature of a business's operations.

Modern brokers are progressively taking on the role of consultants, actively engaging with clients to comprehend not only what can be insured, but also what should be prevented, retained, mitigated, or transferred through alternative strategies. This transition marks a significant transformation in their role, evolving from intermediaries to strategic advisors positioned at the crossroads of risk, finance, and business strategy.

In the new risk economy, brokers are transforming from just placing insurance to becoming true risk architects.

Consider Marsh's Strategic Risk Consulting division as an example. It provides clients with various services such as geopolitical risk modelling, cyber preparedness assessments, ESG exposure mapping, and supply chain stress testing. These offerings extend well beyond conventional placement; they are proactive and insight-focused, designed to assist organisations in anticipating emerging threats and responding with agility.

Marsh's geopolitical risk intelligence, for example, has been instrumental in advising multinational clients on how to navigate the repercussions of the Russia-Ukraine conflict. This underscores the importance of scenario planning, implementing crisis response protocols, and maintaining diversified supply chains.

This advisory-led approach is gaining significant traction. As highlighted in the 2023 Deloitte Global Insurance Outlook, 62% of corporate clients anticipate their brokers to offer not just insurance placement, but also data analytics, benchmarking, and enterprise risk consulting. The market is clearly indicating a transition toward value-added services and enhanced engagement throughout the risk lifecycle.

Risk architects distinguish themselves by dismantling risk silos and integrating cyber, operational, environmental, and reputational risks. They evaluate how one risk can trigger or intensify another, such as a cyberattack disrupting supply chains and damaging customer trust. Consequently, they recommend a comprehensive risk strategy that includes insurance, self-insurance, risk mitigation, and alternative financing options.

This new mindset is especially valuable to mid-sized and large firms navigating global uncertainty. Risk doesn't respect industry boundaries or national borders. As such, brokers who can provide cross-sector insights and global perspectives are becoming essential to boardroom decision-making.

In this evolved role, brokers bring a unique blend of technical knowledge, analytical tools, and commercial insight. They help clients quantify exposures, evaluate risk appetite, and align insurance strategies with business objectives. In doing so, they don't just transfer risk, they help businesses transform it.

Mitigating SOCIAL ENGINEERING FRAUD RISK

The current digital landscape reveals that the most damaging breaches often don't originate from viruses or compromised firewalls; they start with deception. A meticulously crafted email, a convincing voice on the phone, or an urgent request that seems ordinary and completely credible—these are the tools of social engineering fraud. This subtle yet alarming threat is quickly emerging as one of the most perilous and expensive challenges confronting modern businesses.

In contrast to conventional cyberattacks that target system vulnerabilities, social engineering sidesteps technology altogether. Instead, it capitalises on human behaviour—exploiting instincts such as trust, fear, and the urgency to respond swiftly.

In 2024, the FBI's Internet Crime Complaint Center (IC3) reported over $2.9 billion in adjusted losses due to Business Email Compromise (BEC)—a refined form of social engineering that impersonates trusted contacts to manipulate employees into transferring funds or disclosing sensitive information. That's more than the total losses from ransomware and data breaches combined.

Businesses are losing nearly $8 million daily, often without any code breaches. Despite the increasing losses, many organisations remain unprepared, facing not just technical but also psychological threats that are often overlooked.

The Many Faces of Social Engineering

Social engineering is not a single tactic, but an evolving playbook of psychological manipulation. Fraudsters adapt their approach to the target, the moment, and the medium. And they're getting better. Let's break down the most common and dangerous forms.

Business Email Compromise (BEC)

Also called "CEO fraud," BEC involves impersonating a senior executive—often via a spoofed or hacked email account—and instructing an employee to urgently transfer funds or send sensitive data.

In one case, a US tech company was tricked into wiring $46.7 million to fraudsters posing as a trusted vendor. The email looked authentic. The invoice matched. The tone mirrored the real executive's. It took hours to realise the deception, and by then, the money had vanished into overseas accounts. According to the IC3, BEC scams caused more losses in 2024 than any other cybercrime category.

Phishing

Phishing remains the most widespread form of social engineering. Fake emails, texts, or messages appear to come from trusted institutions such as banks, cloud providers, HR departments; urging recipients to click a link, reset a password, or verify an account

These links lead to credential harvesting sites or trigger malware downloads. Even cybersecurity-savvy employees fall for them. Verizon's 2023 Data Breach Investigations Report found that 36% of breaches involved phishing, and 74% of organisations experienced at least one successful phishing attack in the past year.

Vishing and Smishing

Social engineering has moved beyond the inbox. Vishing (voice phishing) uses phone calls, often spoofed to appear local or from a known company. Attackers impersonate IT support, government officials, or fraud investigators, convincing employees to reveal confidential access credentials.

Smishing utilises SMS messaging. A common example involves a text that appears to be from a bank, alerting the recipient about unusual activity and urging them to "click here to resolve it." That click can lead to serious consequences. These methods are particularly perilous in hybrid or remote work settings, where verification becomes more challenging and the sense of urgency is heightened.

Pretexting

Pretexting involves constructing a detailed and believable story, which often based on publicly available data, to manipulate targets.

Consider this: An attacker poses as an external auditor working with the CFO. They know the company's fiscal year-end. They reference a recent press release. They even use correct names and titles scraped from LinkedIn. The result? An employee shares financial statements, or worse, access credentials—believing it's all above board.

As reported in IBM's 2023 Cost of a Data Breach Report, it takes an average of 270 days to detect and contain a breach resulting from social engineering. This lengthy duration is often leveraged by attackers to enhance their access and increase the overall damage.

Tailgating and Physical Social Engineering

Not every attack happens in the digital realm. Tailgating, the act of trailing an authorised individual into a secure facility without the necessary credentials, continues to be an unexpectedly effective strategy. A quick display of a counterfeit badge or a courteous remark like, "I forgot my keycard," can compromise security—not through technology, but through simple human politeness.

In 2022, a security audit conducted at a prominent financial institution revealed that 83% of employees permitted unauthorised individuals to access secure areas without hesitation. The most significant vulnerability? Human behaviour.

Deepfakes

This AI-generated synthetic media are becoming a chilling tool in the social engineering arsenal. Cybercriminals can now create realistic videos or audio recordings that appear to show a CEO authorising a wire transfer, or a senior executive instructing staff to share confidential files.

The technology has already been used to devastating effect. In 2023, a multinational firm in Hong Kong was defrauded of $25 million after a finance worker received what appeared to be a live video call from the CFO instructing them to transfer funds. It wasn't real. The executive's likeness had been faked using AI and stitched into a real-time video stream. The employee, believing it genuine, complied without hesitation.

As generative AI tools become more accessible, the barrier to creating convincing deepfakes continues to drop. According to a report by Gartner, 90% of video content may be synthetically generated by 2030, blurring the line between reality and deception.

In 2022, a security audit conducted at a prominent financial institution revealed that 83% of employees permitted unauthorised individuals to access secure areas without hesitation.

Strategies to Mitigate

No organisation is exempt from risk. However, every organisation can take steps to be ready. Mitigating social engineering fraud doesn't necessitate advanced technology; it demands a well-coordinated strategy that includes human vigilance, strict adherence to procedures, and fostering a culture of zero trust until verification is achieved. Here are several ways to build that defence.

Implement Multi-Factor Authentication (MFA)

Passwords alone are no longer enough. Even if credentials are stolen, MFA adds a critical layer. It requires users to verify their identity through a second factor, usually a mobile app, hardware token, or biometric scan.

Microsoft reported that MFA can prevent over 99% of account compromise attempts. However, its adoption continues to be uneven, particularly among mid-sized and legacy organisations.

Implement Robust Verification Protocols

Adopt the mantra: "Don't trust, verify." Every financial transaction, particularly those involving modifications to payment details or unusual requests, must adhere to stringent internal verification processes. For instance, any wire transfer exceeding a specified limit should necessitate dual authorisation.

Requests sent through email or phone must always be confirmed through a different, secure method. Ideally, this verification should occur in person or through a recognised phone number, rather than by replying to the original message. This straightforward guideline, referred to as "out-of-band verification," could have averted millions in losses related to business email compromise (BEC).

Invest in Ongoing Training and Simulation

Relying on just one training session each year is insufficient. Social engineering tactics are always changing, and your defences must adapt as well.

Organisations ought to carry out quarterly simulations that incorporate fake phishing emails, spoofed calls, and deepfake audio tests. It's crucial for employees to encounter the realistic nature of these attacks firsthand. Training should extend beyond simply identifying threats; it must foster reflexes: Stop. Question. Verify.

Monitor for Behavioural Anomalies

Leverage technology to your advantage. AI-driven fraud detection tools can flag unusual access patterns, sudden fund transfers, or abnormal login behaviour; signals that a user may be compromised or coerced.

For example, if an employee suddenly logs in from a foreign IP or requests multiple password resets, the system can automatically freeze access until a human review clears it. IBM reports that AI-enhanced threat detection shortens the average breach lifecycle by 108 days—a powerful advantage in stopping escalation.

Strengthen Vendor and Third-Party Due Diligence

Social engineering often starts outside the organisation. Attackers may target vendors or partners to gain access to internal systems or impersonate trusted third parties. That's why organisations must assess their partners' cybersecurity posture just as rigorously as their own.

Incorporate social engineering risks into vendor risk assessments. Ensure that you obtain proof of security measures, staff training, and disclosures regarding breach history.

Prepare for Deepfakes

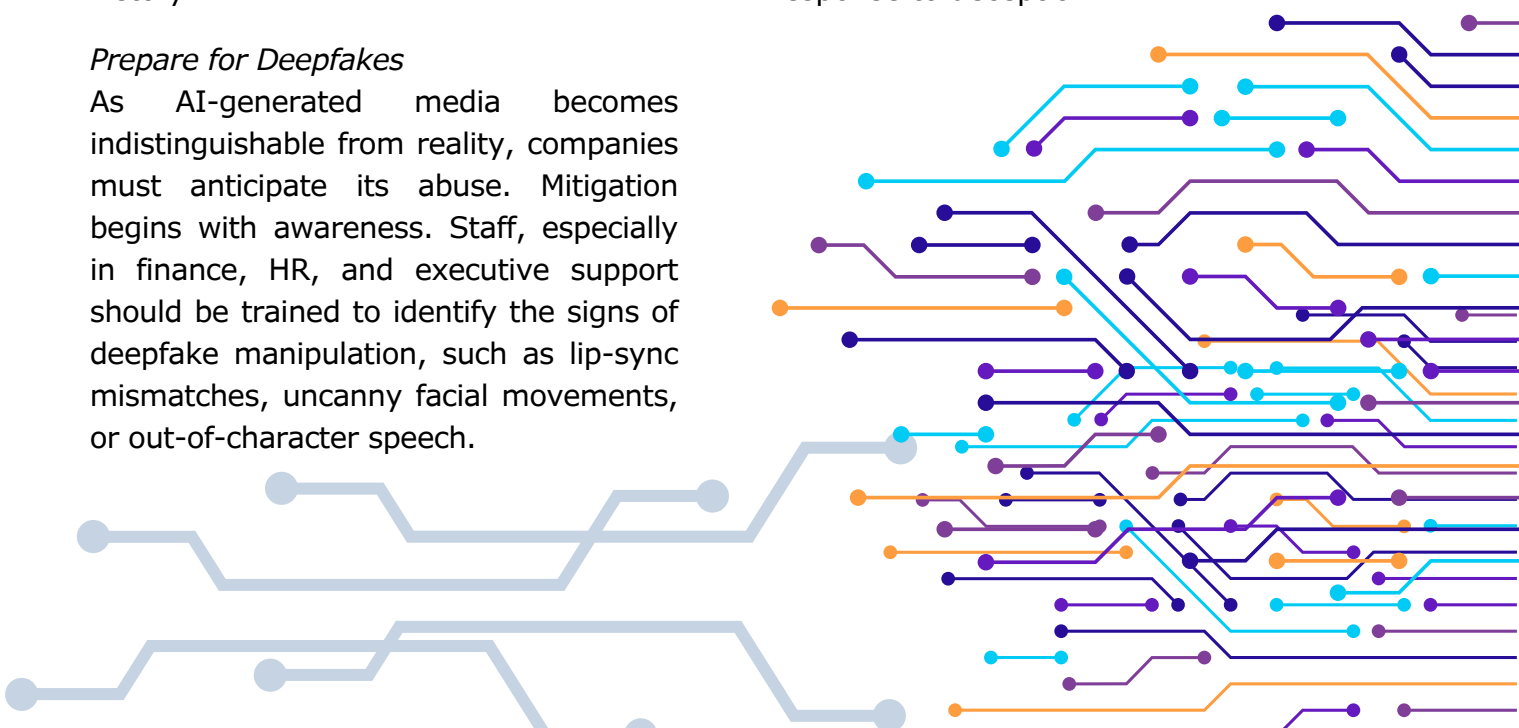
As AI-generated media becomes indistinguishable from reality, companies must anticipate its abuse. Mitigation begins with awareness. Staff, especially in finance, HR, and executive support should be trained to identify the signs of deepfake manipulation, such as lip-sync mismatches, uncanny facial movements, or out-of-character speech.

In high-risk environments, video calls involving financial approvals should be backed by secure voice verification protocols or digital signatures. Some firms now use watermarked "trusted video" technology to authenticate executive communications.

Strategies to Mitigate

In a digital age, trust is essential yet vulnerable. Social engineering fraud targets belief systems rather than machines, exploiting fear and goodwill. However, organisations that prioritise awareness and vigilance can empower individuals to become defenders against such threats.

Although social engineering risks persist, effective systems and a strong culture can reduce its success. Cybersecurity is now a leadership and cultural issue, with clarity being the best response to deception.



health &safety

A TOP CONCERN FOR D&O

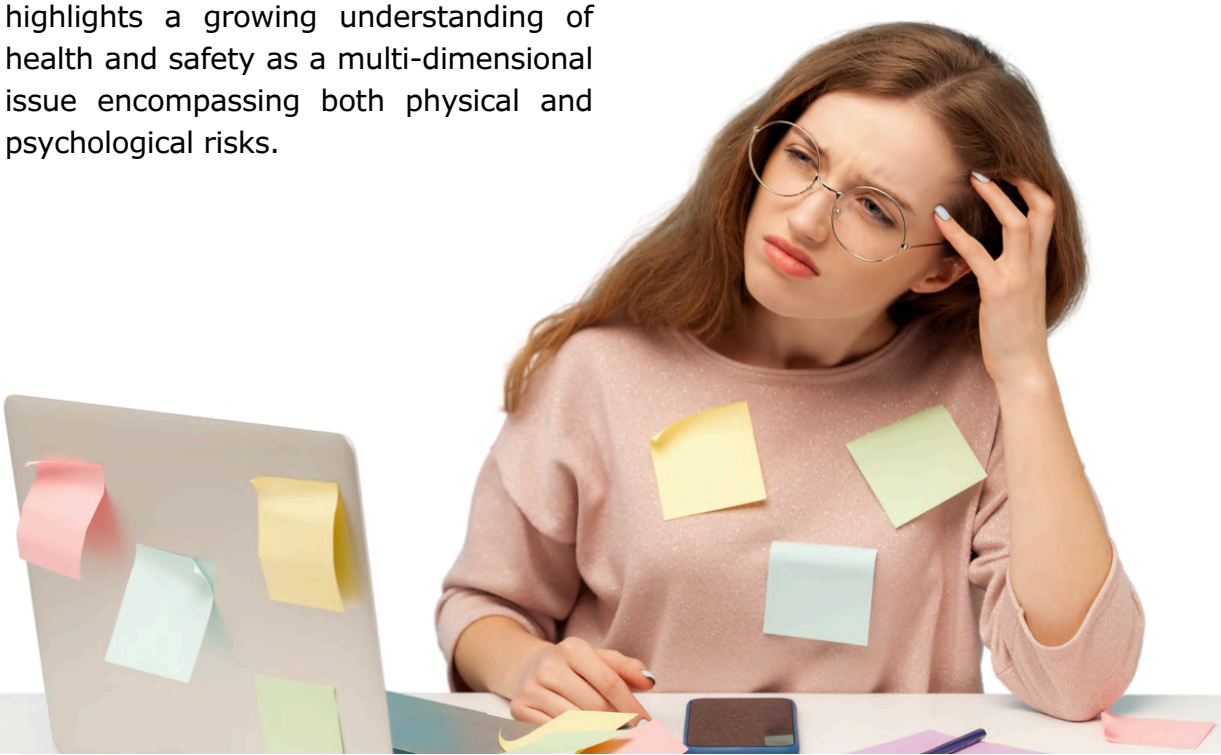
A recent joint survey by Willis Towers Watson and global law firm Clyde & Co. has spotlighted a significant shift in the risk landscape for directors and officers (D&Os). Health and safety has emerged as the top concern among D&O risks, overtaking traditional worries like regulatory investigations and shareholder litigation.

The survey, which canvassed risk professionals, senior executives, and board members across various sectors, indicates a growing awareness of the personal liability D&Os face regarding workplace safety, employee wellbeing, and corporate responsibility.

Among health and safety concerns, physical workplace risks were cited as the most significant by 43% of respondents, followed by mental health and wellbeing issues tied to work (28%) and personal matters (12%). This split highlights a growing understanding of health and safety as a multi-dimensional issue encompassing both physical and psychological risks.

Boards are now expected to proactively foster a culture of care, going beyond mere compliance with safety regulations. In light of pandemic-related changes and mental health challenges in high-pressure sectors, directors face pressure to show effective oversight and accountability.

For insurers and brokers, the rising prominence of health and safety as a D&O risk necessitates a recalibration of underwriting frameworks. Traditionally, D&O insurance has been primarily concerned with financial mismanagement, shareholder litigation, and regulatory investigations. However, the increasing focus on workplace safety means insurers must assess the governance and risk management culture of an organisation more holistically.



In practical terms, this means insurers are likely to apply stricter underwriting scrutiny. There will be heightened attention on a company's health and safety protocols, training programs, governance structures, and historical claims. Organisations with inadequate safety oversight or a poor track record may face higher premiums or more restrictive coverage terms.

Policy wordings are also expected to evolve. D&O policies may begin to more explicitly address liabilities stemming from failures in workplace safety, including those related to employee mental health and breaches of duty of care. Insurers could also consider expanding coverage for regulatory investigations tied specifically to non-compliance with health and safety regulations.

There is also a growing convergence between health and safety risk and broader Environmental, Social, and Governance (ESG) concerns. As investor and regulatory scrutiny of employee wellbeing intensifies, insurers may begin integrating ESG assessments into D&O underwriting. This would ensure companies demonstrate meaningful and measurable actions to mitigate workplace risks as part of their overall governance strategy.

In response to this changing environment, insurers and brokers are anticipated to take on a more advisory position, working closely with boards to improve their risk management strategies. This could involve offering risk engineering support, developing tailored training programs for directors, or encouraging proactive governance through favorable terms.

Ultimately, the changing risk landscape necessitates a more collaborative strategy among insurers, brokers, and corporate leaders. In a time when health and safety have transcended mere compliance to become foundational aspects of corporate governance, D&O insurance must evolve to stay relevant and robust.

In light of this evolving landscape, insurers and brokers are expected to adopt a more advisory role, collaborating closely with boards to enhance their risk management strategies.