THE AGENTIC CRISIS

Safeguarding Brand Integrity Against Synthetic Threats

Powered By:

STRATEGIC INSIGHTS CENTER

POWERED BY ABOVE PROMOTIONS

INNOVATION LAB

POWERED BY ABOVE PROMOTIONS

THE SKILLS DEVELOPMENT HUB

POWERED BY ABOVE PROMOTIONS

THE 2026 LANDSCAPE

The digital age has ushered in unprecedented opportunities for growth alongside a minefield of algorithmic accountability. Rapid technological advancement, mounting demands for data governance, board-level AI oversight, and stringent regulatory mandates create a uniquely challenging environment for organizations of every size. Lawsuits, regulatory sanctions, and lasting reputational damage are constant threats — amplified now by AI-driven breaches and synthetic media attacks.

Over the years, we have worked alongside many organizations and observed a persistent, critical gap: the inability to build a cybersecurity culture that meets evolving regulatory requirements while fostering true operational resilience. A culture that moves far beyond basic phishing tests and compliance checklists — one that embraces data privacy by design and prepares for threats that did not exist even twelve months ago.

Staying compliant and secure amid the EU AI Act, SEC Reg S-P, and a growing roster of US state-level privacy laws is a significant drain on internal resources. Regulators and insurers are no longer satisfied with box-checking. They expect demonstrable preparedness, tested response plans, and a provable commitment to responsible AI governance.

As organizations increasingly deploy autonomous AI agents — not just AI tools — the risk profile has fundamentally shifted. AI now introduces vulnerabilities in the form of hallucinated outputs, compromised agentic workflows, deepfake impersonation, and synthetic disinformation campaigns that can reach viral scale before a human reviewer ever sees them.

Over the last decade, we have assisted organizations in proactive crisis planning and response. In 2026, that mission demands more: equipping your team with the skills to manage autonomous threats, protect narrative integrity, and demonstrate algorithmic sovereignty to every stakeholder who is watching.

GETTING STARTED

This update includes insights on AI-driven threats, the use of generative tools in response planning, and how to communicate organizational AI policies in the wake of rising regulatory and public scrutiny.

At Above Promotions, each team member in our Strategic Insights Center, Innovation Lab, and Skills Development Hub is committed to supporting you in effectively managing unforeseen events, safeguarding your organization, and reducing the impact of crises.

Please review our whitepaper and quiz in this document. They are valuable resources for initiating internal discussions and setting your organization up for success.

Ebony Vaz
Founder and CEO

40%+

of employees struggle to distinguish AI-generated communications from reality.

Source: Proofpoint 2024 Human Factor Report

SECURITY MESSAGING MUST EVOLVE — BECAUSE THE THREATS HAVE.

Cybersecurity training and communication continue to fall short — not because employees don't care, but because the messaging has not kept pace with the threat. In 2026, we have entered the era of the Autonomous Agent, where AI generates not just emails, but real-time voice calls, video appearances, and entire synthetic identities.

Over 40% of employees still struggle to distinguish AI-generated communications from real ones. In 2026, that challenge is compounded by "Vibe-Coding" — AI-written software modules that appear functional but contain concealed backdoors — and interactive deepfakes capable of participating in live meetings.

WHY TRADITIONAL AWARENESS CAMPAIGNS FAIL IN 2026:

- Overly technical language that disengages non-IT staff
- Repetitive messaging that causes "alert fatigue."
- Training that does not reflect real-world agentic AI usage
- Simulations that lag years behind actual attacker capabilities

A MODERN 2026 COMMUNICATION APPROACH INCLUDES:

- Adversarial training: moving beyond simulations to live "Deepfake Drills."
- Psychological framing: training staff to "verify by default" every automated agent interaction
- AI-assisted personalization of training based on individual risk profiles
- Clear, jargon-free guidance on recognizing hallucinated outputs from internal AI tools

Organizations must now train their people not just to spot phishing emails, but to question any content that looks, sounds, or "feels" real — including content generated by systems they already trust.

$21B

Cyber-enabled crimes defrauded Americans of nearly $21 billion in 2025 — a new record — with AI-related complaints generating $893 million in losses. The FBI notes the true figure is likely higher, as most victims never realize AI was involved.

Source: FBI Internet Crime Complaint Center (IC3) 2025 Internet Crime Report

"WHEN" IS CERTAIN — AND NOW, IT'S SMARTER.

In today's digital environment, a crisis is no longer a matter of if — it is a matter of when, how fast, and how autonomously. AI is making the fallout from breaches swifter, more sophisticated, and more difficult to contain through human oversight alone.

Anthropic's Project Glasswing — launched in April 2026 — shows how fast threats change. Its latest AI found thousands of new security problems in all main computer systems and web browsers within weeks. Anthropic admits that attackers can use the same AI abilities that help protect computers, and these skills will soon spread. The best-prepared organizations are getting ready now.

The emergence of Agentic AI means that organizations now face threats that operate without human instruction:

Agentic attacks
Malicious AI agents that navigate internal networks independently, escalating access before any alert is triggered

Interactive deepfakes
Real-time video and audio that can appear in live board meetings to authorize fraudulent transactions

Hallucinated liability
Consumer-facing AI bots that make legally binding promise the organization never sanctioned

Synthetic disinformation
AI-generated misinformation campaigns that can outpace your official communications by hours

Whether it is a deliberate cyberattack, a rogue agentic workflow, or a reputational assault from synthetic media, the damage to trust, operations, and brand equity can be immense — and viral. Protecting the story is as vital as safeguarding data; clear, credible communication during crises reassures stakeholders and rebuilds trust effectively.

FROM IT TO AI: EXPANDING THE CRISIS TEAM TRUST TAKES A TEAM — AND A STRATEGY BEYOND IT.

Traditionally, cyber crises were seen as a job for IT. But in the age of intelligent attacks and algorithmic errors, communications, privacy, legal, and brand leaders must be equally equipped.

A modern crisis team should now include:

- Cybersecurity and compliance professionals
- Communications leaders and PR advisors
- Privacy and AI governance officers
- Legal counsel (especially with AI liability concerns)
- Marketing and customer experience leads

Additionally, organizations should designate:

- An executive responsible for AI use policy communications
- A spokesperson trained to address deepfake or misinformation events

Outsourcing parts of your response strategy is also vital. External partners should assist with:

- Media narrative management
- Internal stakeholder messaging
- Misinformation tracking and takedowns
- Post-crisis sentiment monitoring

Even one delayed or unclear message in the AI age can cascade into viral reputational damage.

The damage from cyber and AI-related incidents doesn't just show up on balance sheets. The losses are emotional, cultural, reputational — and lasting.

What's at Stake:

- Customer trust: AI-generated misinformation can lead to mistaken beliefs in false narratives, resulting in customer churn.
- Revenue: Downtime from attacks or containment measures causes lost sales and operational disruption.
- Brand equity: Your brand becomes linked to mishandled crises or controversial AI usage.
- Employee morale: Internal confidence erodes when teams feel unprepared or misrepresented during public-facing incidents.

Even companies that weren't breached, but were impersonated or misrepresented, still faced:

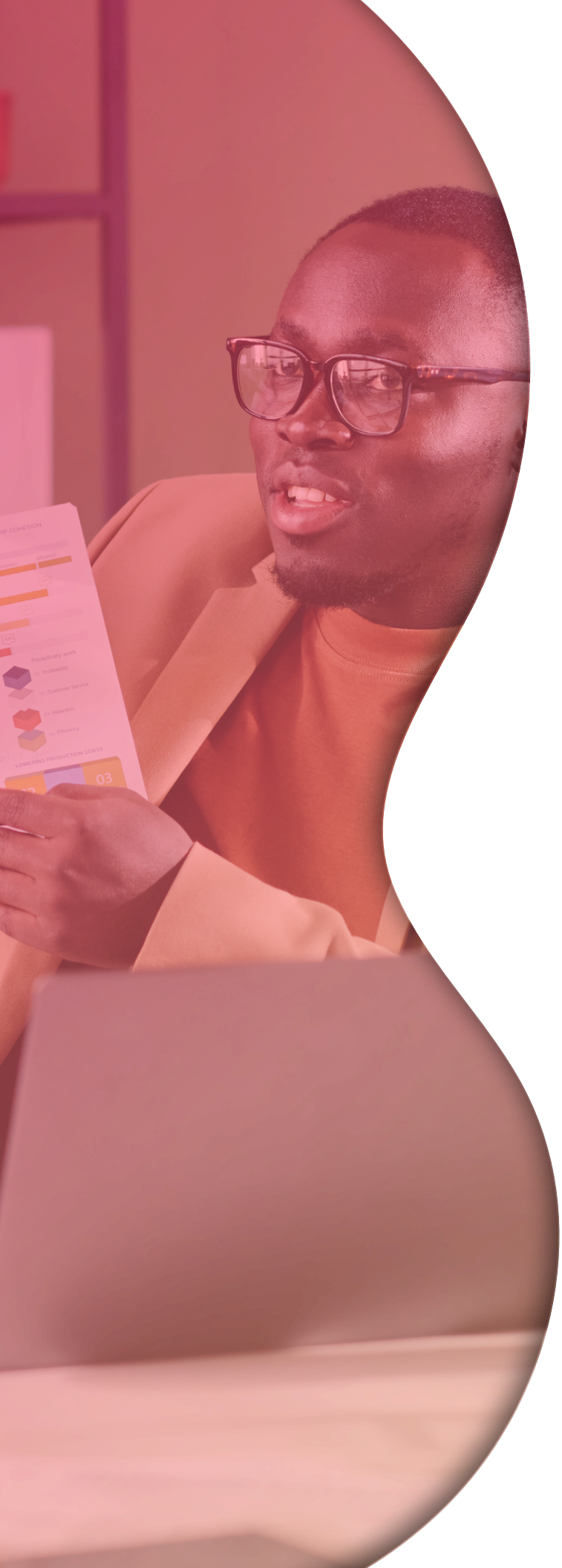
- Negative headlines
- Lawsuits
- Social media boycotts
- Government scrutiny

Being caught off guard is no longer an excuse — AI amplifies speed and scale, and response readiness is now a reputational currency.

$893M

The FBI received over 22,000 AI-related cybercrime complaints in 2025, resulting in $893 million in losses. The true number is likely higher, as most victims do not recognize AI involvement.

Source: FBI Internet Crime Complaint Center (IC3) 2025 Internet Crime Report



BUILDING A THREE-PILLAR AI-AWARE CRISIS STRATEGY

Cybersecurity in 2026 is no longer just about firewalls; it is about communication, trust, and adaptability in the face of increasingly autonomous threats. To address these realities, Above Promotions has developed a Preparation, Response, and Restoration framework that is your first line of defense against the Agentic Crisis, whether or not you have a technical SOC team on staff.

Strategic Communications is Your First Line of Defense

As a communications agency, Above Promotions supports clients in crafting messages that empower employees, build public trust, and respond with clarity and confidence — even in the face of manipulated or misleading digital content.

We provide the strategic communications infrastructure needed to maintain narrative control, demonstrate algorithmic sovereignty, and restore stakeholder confidence when it matters most.

Organizations that had an Incident Response plan and tested it saved an average of $1.3 million on data breach costs.

Source: IBM COst of a Data Breach Report

PREPARATION

The cost to prepare for any organization is significantly less than the cost of being caught unprepared.

- Conduct Algorithmic Audits: auditing internal and external AI agents for hallucination risk and unauthorized data access.
- Build an Agent Inventory: mapping every autonomous tool your organization uses to ensure a documented Kill-Switch protocol exists for each.
- Run Deepfake Drills: simulations where an executive is impersonated in a live video call to test detection and response.
- Create pre-approved messaging templates for potential AI crises, including hallucinated promises and rogue agent incidents.
- Map out action plans with timelines for regulatory notification windows.
- Conduct media training with a specific focus on debunking synthetic media.
- Begin proactive online reputation management and influencer relationship building.
- Develop and run agentic event response simulations across departments.

23%

Breaches identified and contained within 200 days cost 23% less to resolve.

Source: IBM COst of a Data Breach Report

RESPONSE

Creating and deploying a rapid response team to support cyber and AI crises is not optional: it is essential.
In 2026, response timelines are compressed by new regulatory mandates, including the SEC's Reg S-P 30-day notification requirements.

We work with rapid response teams to:

- Perform Agent Override: rapidly shutting down compromised bots and agentic workflows while maintaining business continuity.
- Deploy Sentiment Tracking: using AI to monitor how quickly a deepfake or hallucinated policy is spreading across media and social platforms.
- Issue Transparency Kits: pre-drafted stakeholder notifications that explain technical AI failures in accessible, non-technical language
- Conduct a rapid content review of AI-generated responses to ensure accuracy before publication.
- Create response kits specifically for deepfake incidents and chatbot hallucination events.
- Develop answers to likely FAQs from customers, regulators, and media.
- Prepare and coach designated spokespersons for real-time deepfake scenarios.
- Monitor media and social platforms for the spread of disinformation and narrative drift.
- Execute social media messaging within hours of a triggering event.
- Draft notifications to all internal and external stakeholders, including vendors, personnel, and customers

RESTORATION

Regain trust and Reset the brand.

Restoration in 2026 is about proving you have regained Algorithmic Sovereignty — that your AI systems are once again under appropriate human oversight, and that your organization has drawn meaningful lessons from the incident.

We help clients move from crisis fatigue to building a stronger, more credible brand presence. We provide:

- AI-powered sentiment analysis for brand recovery and ongoing perception monitoring
- Transparency Reports: publicly clarifying how the AI error or agentic failure occurred and what Responsible AI protections are now in place
- Reputation Audits: assessing the “hallucination hangover” — identifying and correcting false information that remains in the public’s perception of your brand
- Post-crisis content development to clarify organizational values around responsible AI use.
- Post-crisis action items and communications reports
  Adjustments to response plans and corporate AI policies
- Continued monitoring of online reputation and narrative trends
- Thought leader content to reestablish expertise and credibility
- Updated response simulations incorporating lessons learned
- Communications for internal and external stakeholders, including litigation support communications

CRISIS READY QUIZ

Assess Your Agentic Readiness

No one can predict when a threat will arise, but having a tested strategy in place can prevent organizations from suffering long-lasting damage. Executives and department

leaders can use this quiz to assess crisis readiness and identify gaps before an incident does it for them.

Answer YES or NO to the following with your team:

YES OR NO Do you have an official AI Use and Agentic Safety playbook?

YES OR NO Has your playbook been updated within the last three months to reflect the 2026 EU AI Act or applicable US state laws?

YES OR NO Does your policy cover both internal and external threat communications, including AI-originated incidents?

YES OR NO Do you have a designated Kill-Switch protocol for every autonomous agent in your organization?

YES OR NO Are messaging templates ready to address “hallucinated” promises made by your chatbots or AI agents?

YES OR NO Is there a designated hierarchy of spokespersons trained for different types of crises, including synthetic media events?

CRISIS READY QUIZ

YES OR NO Do you have a spokesperson specifically trained to handle real-time deepfake video crises?

YES OR NO Have you conducted an adversarial “Red-Team” or Deepfake Drill simulation in the past three months?

YES OR NO Do you have an AI Transparency Statement ready for public-facing operations?

YES OR NO Are your internal tools equipped to monitor online reputation and track disinformation?

YES OR NO Has your organization prepared public-facing messaging about how AI is used responsibly in your operations?

YES OR NO Can your team detect and report an AI-triggering event within 10 minutes of occurrence?

Score: Answering “No” to two or more questions indicates your organization is vulnerable to the Agentic Crisis. Start your journey toward a prepared, responsive, and restorative strategy today.

Preparation Response Restoration

We are dedicated to assisting our clients in addressing their present and potential challenges.

Our team comprises published researchers, skilled communicators, and specialists in data privacy and human factors. They are leaders in various networks, industries, local and federal government partnerships, and advisory boards.

While we cannot eliminate all risks associated with client loss, we strive to minimize the impact and retain as many clients as possible.

We help organizations navigate problems, including:

Data Breach & Agentic AI Failures

Cyber Hacking & Network Intrusion

Phishing & Synthetic Disinformation Attacks

Deepfake Impersonation Incidents

Investigative Reports & Regulatory Audits

Litigation Communications

Contact us today for an AI Sovereignty Audit.

(813) 383-1914 office
www.abovepromotions.com

FBI Internet Crime Complaint Center (IC3) 2025 Internet Crime Report https://www.fbi.gov/news/press-releases/cryptocurrency-and-ai-scams-bilk- americans-of-billions (Full report: https://ic3.gov)
Anthropic Project Glasswing https://www.anthropic.com/glasswing

IBM Cost of a Data Breach Report (used for the $1.3M tested IR plan stat and the 23% faster containment stat — these carried over from the original 2025 whitepaper) https://www.ibm.com/reports/data-breach
Proofpoint 2024 Human Factor Report (used for the 40%+ employees stat on Page 4 — also carried over from the original) https://www.proofpoint.com/us/resources/threat-reports/human-factor