



Establishing a Culture Focused on Preparation, Response, and Restoration in the Age of AI and Evolving Threats

Powered By:

STRATEGIC INSIGHTS CENTER

POWERED BY ABOVE PROMOTIONS



POWERED BY ABOVE PROMOTIONS

THE SKILLS
DEVELOPMENT HUB

POWERED BY ABOVE PROMOTIONS

GETTING STARTED

The digital age has brought unprecedented opportunities for growth and a complex web of regulatory requirements. The speed of technological advancement, coupled with increasing demands for data access, board oversight, and stringent regulatory guidelines, creates a challenging landscape for organizations of all sizes. Lawsuits, hefty regulatory sanctions, and significant reputational damage are constant threats, especially from data breaches and privacy violations.

Over the years, we have worked alongside many organizations and have observed a critical gap. Organizations struggle to build a robust cybersecurity culture that meets regulatory requirements and fosters true resilience while expanding offerings and revenue. A culture that goes beyond basic phishing tests and generic training videos, to one that embraces data privacy by design. Staying compliant and maintaining a strong security posture in the face of evolving regulations, particularly the proliferation of new data privacy laws (such as GDPR, CCPA, and new US state laws like FLDBOR, Delaware, New Jersey, and more), is a significant strain on internal resources.

Regulators and insurance companies want more than just checking boxes. They seek a demonstrable commitment to security and a proven ability to respond effectively. Our approach to outlining communication, decision-making, and resource allocation procedures for crisis management allows the board of directors, insurance companies, and regulators to feel comfortable with your preparedness.

As organizations increasingly adopt AI tools, new risks and opportunities emerge. While AI enhances operational efficiency, it also introduces unique vulnerabilities, such as misinformation, deepfakes, and hallucinated outputs that can amplify crisis communications challenges.

Over the last decade, we have assisted in proactive crisis planning and response. We focus on enhancing your team's problem-solving abilities, teamwork, and risk mitigation readiness. By staying informed about human behaviors, industry trends, and global events that may impact your organization, we enable your team to concentrate on growth and expansion.

GETTING STARTED

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

At Above Promotions, each team member of 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 crisis impacts.

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



Over 40% of employees report difficulty distinguishing real communications from AI-generated phishing attempts.

Source: Proofpoint 2024 Human Factor Report

Cybersecurity training and communication often fall short — not because people don't care, but because the messaging is ineffective in a world of information overload and digital fatigue.

Now, with the emergence of AI-generated content, the risks are no longer just technical; they are also psychological and behavioral. Your audience may not just ignore traditional warnings... they might trust the wrong source entirely.

Why Traditional Awareness Campaigns Fail:

- Overly technical language that disengages non-IT staff
- Repetitive messaging that causes “alert fatigue”
- Pop-ups and policy updates are quickly dismissed
- Lack of real-world relevance in phishing simulations

A Modern Communication Approach Includes:

- Clear, jargon-free messaging tailored to different audiences
- Visual and interactive warnings that cut through digital clutter
- AI-assisted personalization of training based on user behavior
- Psychological framing to make risks memorable and actionable

Organizations must now train their people not just to recognize traditional cyber threats, but to question content that looks, sounds, or feels real — but isn't.

The greatest threat may not be the hacker — it's the fake CEO email, fake product update, or fake data breach notification generated by AI, and sent at the perfect moment to trick your team.

**SECURITY
MESSAGING
MUST EVOLVE
— BECAUSE THE
THREATS HAVE.**

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

3X

AI-generated phishing emails are up to
three times more effective than
traditional ones.

Source: IBM X-Force Threat Intelligence Index 2024

In today's digital environment, a crisis isn't just likely — it's inevitable, and AI is making the fallout swifter, more sophisticated, and more widespread.

The emergence of AI-powered cyber threats means that organizations now face attacks that:

- Mimic internal emails and executive voices through deepfakes
- Manipulate public opinion using synthetic content
- Automate phishing campaigns using natural language generation
- Exploit vulnerabilities in consumer-facing AI tools and bots

Whether it's a deliberate cyberattack, a misused AI chatbot, or a reputational attack from synthetic media, the damage to trust, operations, and reputation can be immense — and fast.

The stakes are no longer just technical — they're narrative. In this new era, your ability to respond to manipulated realities and protect your credibility in real time is what sets resilient organizations apart.

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.



\$1.1 b

Deepfake scams cost global businesses over \$1.1 billion in 2023 alone, with many executives unaware until after the damage was done.

Source: Trend Micro + Deeptrace Labs



BUILDING A THREE-PILLAR AI-AWARE CRISIS STRATEGY

Cybersecurity is no longer just about firewalls — it's about communication, trust, and adaptability in the face of increasingly intelligent threats. Above Promotions' Preparation, Response, and Restoration framework is designed to help you do just that — with or without a technical SOC team.

[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.

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

<https://www.ibm.com/reports/data-breach>



PREPARATION

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

Being prepared calls for an initial cyber communications risk assessment and evaluation of training materials.

This assessment includes reviewing current communications for processes, protocols, teams, and roles during a crisis.

We then:

- Audit preparedness for AI-generated misinformation
- Create pre-approved messaging for potential AI crises
- Incorporate AI tools in crisis simulations (e.g., auto-generated fake news or deepfake drills)
- Map out an action plan with timelines,
- Create templates for simple verbal and written communications,
- Begin online reputation management,
- Conduct media training,
- Develop and run cyber event response simulations,
- Identify and network with influencers in your space with active social media and news presence to develop a positive relationship.



RESPONSE

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

<https://www.ibm.com/reports/data-breach>

Creating and deploying a rapid response team to support cyber crises is essential.

We work with rapid response teams to:

- Rapid content review of AI-generated responses to ensure accuracy
- Create response kits for addressing deepfakes or chatbot hallucinations
- Use AI to analyze real-time media sentiment and disinformation spread
- Create content for messaging
- Develop answers to FAQs
- Prepare spokespersons
- Monitor media and social media platforms
- Social media messaging within hours
- Media relations execution or preparation
- Help execute the plan of action
- Manage online reputation
- Executive articles and blog posts created
- Draft notifications to internal and external stakeholders, including vendors, personnel, and customers.

RESTORATION

Restoration

We help move clients from crisis fatigue to building a stronger brand presence.

We provide:

- AI-powered sentiment analysis for brand recovery
- Transparency communications around internal AI use and future protections
- Post-crisis content development clarifying organizational values in responsible AI usage
- post-crisis action items
- communications reports
- reputation audit
- adjustments to the response plan and corporate policies
- continued monitoring of online reputation
- thought leader content
- build new influencer relationships
- update response simulations
- communications for internal and external stakeholders or litigation communications.

**Regain trust and
Reset the brand.**



CRISIS READY QUIZ

No one can predict when a threat may arise, but having a strategy in place can help prevent organizations from suffering long-lasting damage.

Executives and department leaders striving to protect their organizations from cyber incidents can help detect and respond to risks promptly.

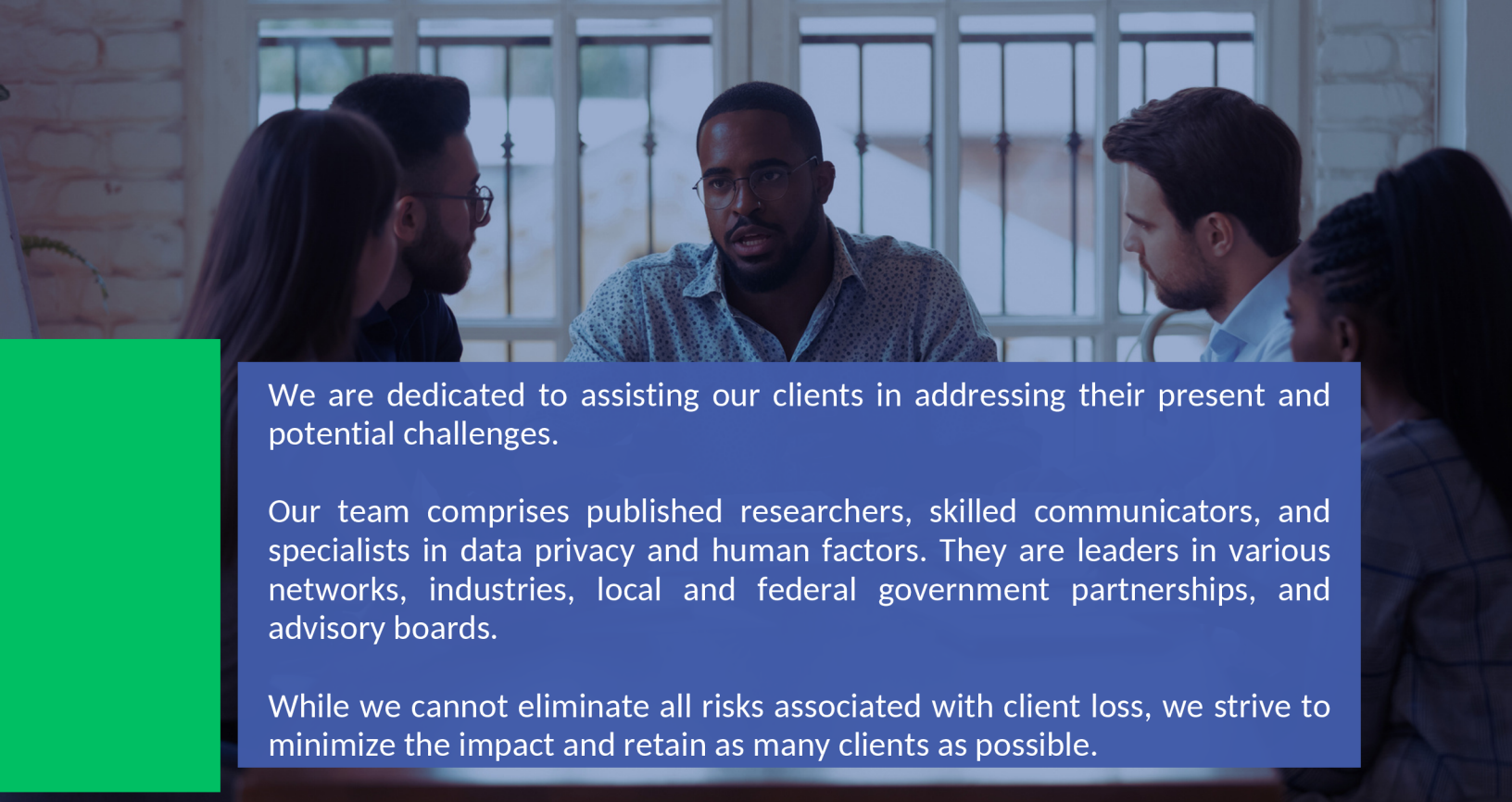
To assess your crisis readiness, take our Crisis Ready Quiz and consider the following questions with your team:

- ☐ YES or ☐ NO Do you possess an official crisis playbook?
- ☐ YES or ☐ NO Has the crisis playbook been updated within the last three months?
- ☐ YES or ☐ NO Does your policy cover internal and external threat communications?
- ☐ YES or ☐ NO Are basic messaging templates readily available for immediate use?
- ☐ YES or ☐ NO Is there a designated hierarchy of spokespersons for different crises?
- ☐ YES or ☐ NO Have you identified external roles to fill gaps during emergencies?
- ☐ YES or ☐ NO Have you conducted a crisis simulation in the past five months?
- ☐ YES or ☐ NO Do you have messaging ready for misuse of your brand by deepfake content?
- ☐ YES or ☐ NO Are your internal tools equipped for online reputation management?
- ☐ YES or ☐ NO Has your organization prepared public-facing messaging about how AI is used responsibly in your operations?
- ☐ YES or ☐ NO Is your team trained to respond to synthetic disinformation?
- ☐ YES or ☐ NO Do employees report triggering events within 10 minutes of occurrence?

Answering "No" to two or more questions suggests that your organization may not be crisis-ready, leading to a prolonged and costly recovery process in case of an incident.

Start your journey towards a prepared, responsive, and restorative process 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.

Problems with:

Data Breach
Cyber Hacking
Phishing Attacks
Investigative Reports
Theft
Audits
Litigation

Contact us today.

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

Above Promotions provides strategic consulting services to individuals and companies across the globe through complex business challenges.

This document is for general information and should not be construed as professional advice or services. When making decisions, you must consult a qualified professional adviser directly for assistance.

Above Promotions is not liable for any action taken with this document.

2025 Copyright