

# 2024



## **ESTABLISHING A CULTURE FOCUSED ON PREPARATION RESPONSE RESTORATION**

# BEFORE WE BEGIN

---

Strategic planning for crises is a crucial duty for leaders.

Aiding organizations in navigating challenges is more critical now than ever before. Lawsuits, regulatory sanctions, and more are just around the corner. While collaborating with various companies and leaders, we identified a significant gap in fostering an organization's positive cybersecurity culture. Those organizations focused on collaborative approaches to preparation, response, and restoration and had leaders who focused on people first instead of solely technology tools.

Successful, influential leaders assess potential risks such as natural disasters, cyber-attacks, economic downturns, and reputational harm. They understand the value of planning and implementing strategies to steer their organizations toward favorable outcomes during tough times.

Data proves that preparedness instills team confidence and readiness, leading to a successful response to risks and immediate rewards during crises. As solution providers, we craft tailored crisis management plans, particularly for cybersecurity incidents. Collaborating with outstanding leaders across different disciplines and departments, we outline communication, decision-making, and resource allocation procedures for crisis management. Insurance companies approve our plans for your coverage policies and help even the most inexperienced leader navigate media and board inquiries. Through neuroscience-based training, we promote a cybersecurity-conscious culture among your teams.

We are dedicated to assisting you in proactive crisis planning and response. Our focus is 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.

At Above Promotions, we are committed to supporting you in effectively managing unforeseen events, safeguarding your organization, and reducing crisis impacts. Our whitepaper and quiz serve as valuable resources for initiating internal discussions and setting your organization on a path to success.

Ebony Vaz  
Founder and CEO



**Users become  
overwhelmed  
or frustrated  
when faced with  
overly complex  
or technical  
security warnings**

The Encyclopedia of Human-Computer Interaction, 2nd Ed.  
Authors: Mads Soegaard and Rikke Friis Dam

Effective communication is essential for addressing issues in any organization, especially when it comes to discussing complex cybersecurity topics.

Simply warning users about potential threats often fails to create lasting positive behavior changes.

Users may struggle with understanding technical terms and become overwhelmed by notifications, leading to desensitization or disregard for warnings, leaving them vulnerable to cyber-attacks. Hence, it's crucial to consider how people process warnings during training to enhance their effectiveness and lower cybersecurity risks.

To achieve this, it's important to use clear language without technical jargon.

Warnings should be visually striking and engaging to grab users' attention.

They should be used sparingly to prevent alert fatigue and ensure users pay attention.

By focusing on simplicity and user-friendliness in cybersecurity warnings and training, it is possible to reduce risks and enhance security for individuals and organizations.

# "WHEN" IS CERTAIN, IT'S JUST A MATTER OF TIME.

## 3,205

is the number of data breaches in the  
U.S. with over 353 million individuals  
affected by data exposures.

<https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/>

An organization will inevitably face at least one significant crisis that may even threaten its operations.

The repercussions, such as damage to reputation, share price, fundraising capabilities, employee morale, and future client and talent acquisition, can be severe, regardless of who is responsible – executives, staff, or external partners.

To safeguard your organization, readiness, and preparedness are crucial. Delaying action or hastily forming a response team can leave you vulnerable to managing the aftermath of the crisis.

Be alert to potential internal or external issues, intentional or accidental, involving breaches, cyberattacks, data mishandling, or deliberate website disruptions. These incidents are becoming more common as our interconnectedness grows, with individuals looking to exploit unprepared companies.





# Cyber Crime to cost **\$9.5 trillion** **trillion** per year.

<https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/>

The internal team holds a crucial role in effectively addressing crises. CEOs, CTOs, CIOs, Compliance Teams, and Corporate Boards heavily rely on this team. In fact, we are seeing more cases of leaders in these roles facing personal legal consequences.

Forward-thinking companies are now supplementing this with external ongoing and on-call support to guarantee thorough coverage.

Collaboration among stakeholders from various departments, including IT, communications, legal, human resources, security, marketing, customer experience, and other frontline business units, along with external consultants, ensures swift and efficient resolution of critical issues.

Delaying the response to a crisis by even a day can significantly impact the organization. It's essential to recognize the costs associated with inadequate planning, resource deployment, and activation during and after a crisis.



# 51%

of organizations are planning to increase security investments as a result of a breach, including incident response (IR) planning and testing, employee training, and threat detection and response tools.

[www.ibm.com/security/data-breach](https://www.ibm.com/security/data-breach)

**In 2023, cyber-attacks, ranging from data breaches to hostile account takeovers, were estimated to have cost 8 trillion USD\* globally.**

**Other business loss can be categorized by:**

- **customer turnover,**
- **lost revenue due to downtime,**
- **and increased new customer acquisition due to diminished reputation.**

<https://expressvpn.com/blog/the-true-cost-of-cyber-attacks-in-2024-and-beyond/>

# SUCCESS COMES BY HAVING A STRATEGY...

Organizations often think they have all the safeguards to stop a cyber security crisis. Businesses that succeed recognize that they cannot predict everything and are constantly preparing and reviewing systems for most issues that will arise.

Above Promotions brings its expertise in cyber security, human factors, technology, storytelling, and crisis communications to our client's incident response strategies. Our team can fully integrate with our clients and achieve a swift and positive outcome.

Your company can succeed by focusing on preparation, response, and restoration.

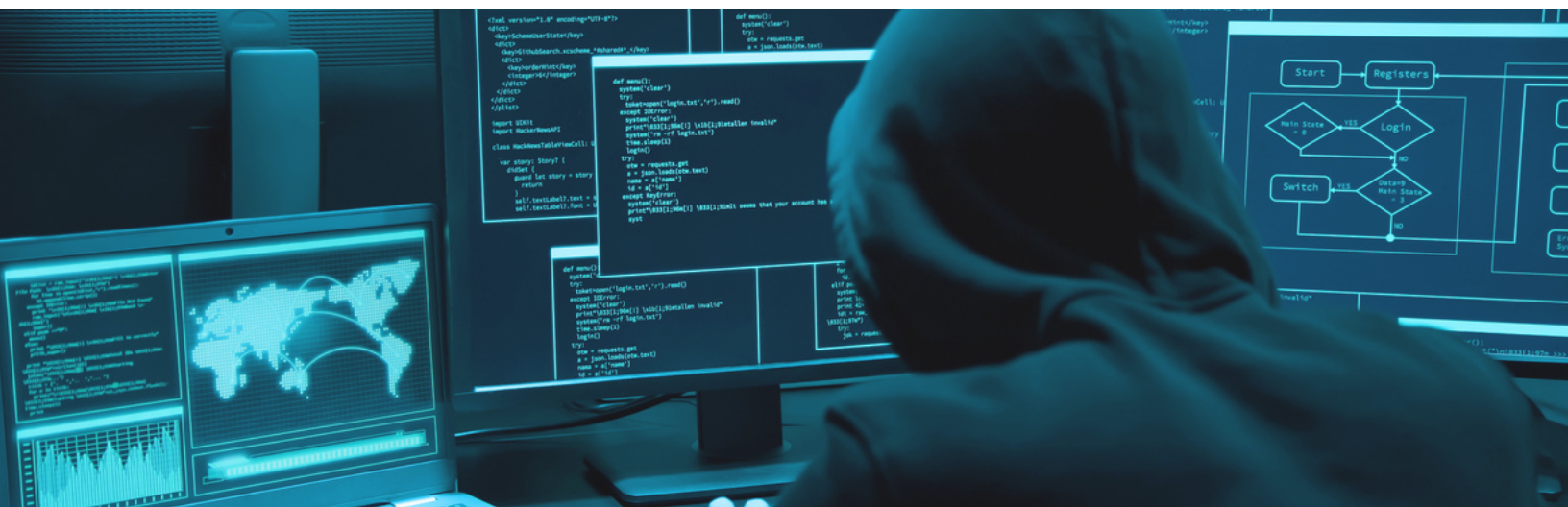
# AND SWIFTLY EXECUTING IT.

The longer you delay responding to an incident effectively, the more consequences you face:

- Risk of losing control of the narrative
- Destruction of trust and credibility
- Decrease in employee morale
- Possibility of suffering significant material impact
- 

Explore our three-pronged strategy to assist clients in thriving post-crisis: Preparation, Response, and Recovery.

You can assess your organization's crisis preparedness with our quick quiz.



**Cyber threats have expanded** from targeting networks — to anything with a heartbeat or an electronic pulse.

<https://www.esentire.com/resources/library/2022-official-cybercrime-report>



# PREPARATION

## 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:

- 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

**It takes up to 277  
days to detect  
and contain a  
data breach.**

<https://www.statista.com/statistics/1417455/world-wide-data-breaches-identify-and-contain/>

## Response

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

We work with rapid response teams to:

- 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.

**Regain trust and  
Reset the brand.**

We provide:

- post-crisis action items
- communications reports
- reputation audit
- adjustments to 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.



# 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 in a timely manner.

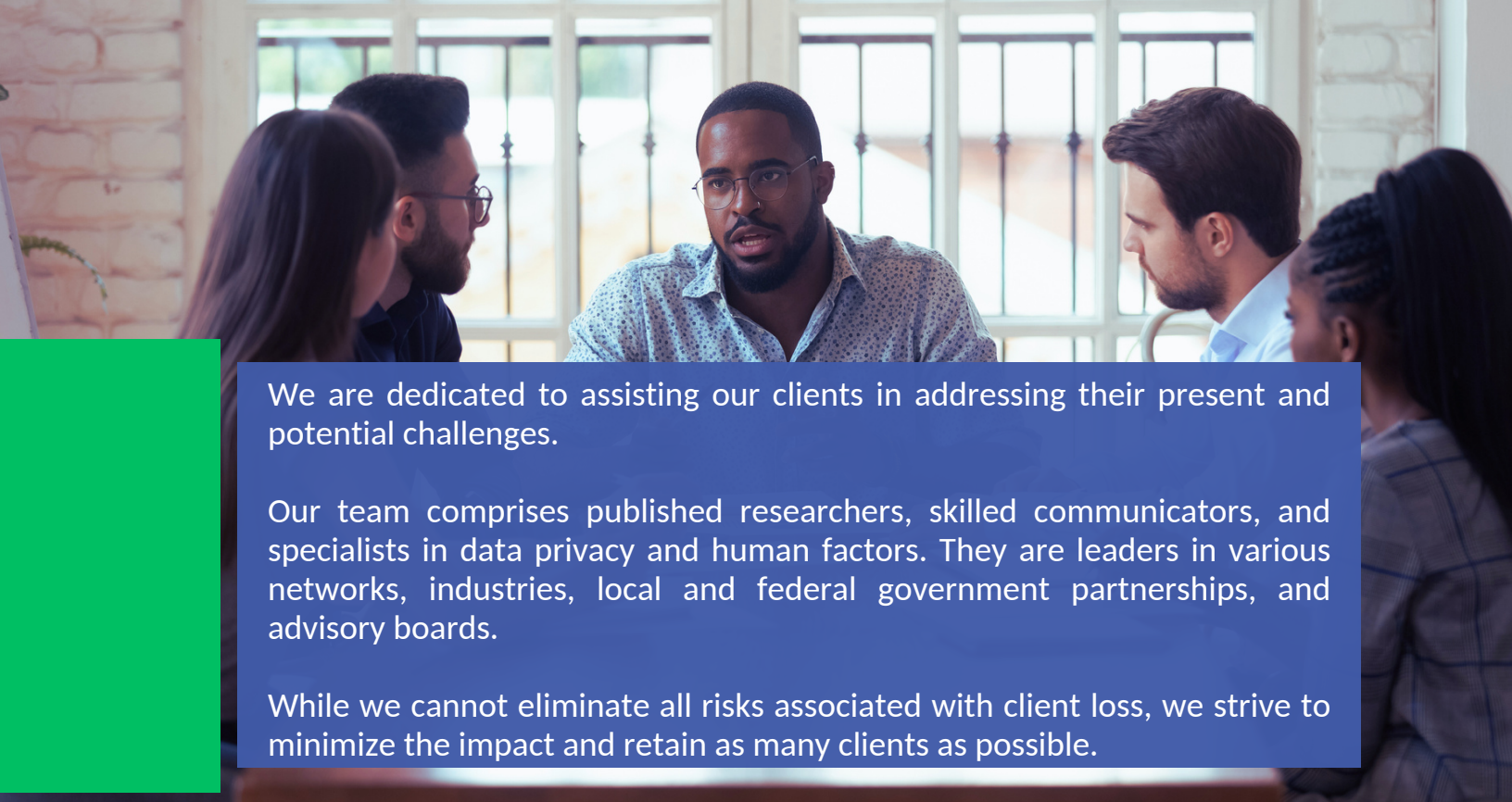
To assess your crisis readiness, take our Crisis Ready Quiz and consider the following questions with your team:

- ☐ 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 the necessary resources to arrange a press conference?
- ☐ YES or ☐ NO Are your internal tools equipped for online reputation management?
- ☐ YES or ☐ NO Is your entire company confident in its ability to recover swiftly from a cyber incident?
- ☐ YES or ☐ NO Do employees promptly complete new cybersecurity training sessions?
- ☐ 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.

# ABOVE PROMOTIONS

PUBLIC RELATIONS MARKETING PROMOTIONS

Problems with:

Data Breach

Cyber Hacking

Phishing Attacks

Investigative Reports

Theft

Audits

Litigation

Contact Above Promotions today.

(813) 383-1914 office

[www.abovepromotions.com](http://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.

2024 Copyright