ZLR IGNITION

BEYOND THE BRIEF

WHERE BRAND STRATEGY MEETS BRAND SECURITY.

A practical playbook for safeguarding your brand through creativity and compliance standards.

CONTENTS

Trust is a brand asset you earn—one action, one decision and one day at a time. It's built through consistency, accountability and care for your customers that reflect your brand promise. When these align, your brand becomes more than just a message; it becomes something people truly believe in.

But in today's hyperconnected, data-saturated world, trust is harder to earn and easier to lose than ever before. In fact, cybersecurity and data protection account for four of the top five risks that the C-suite faces, a clear sign that trust is more than a communications issue. It's a business imperative.

For marketing leaders, it's also a wake-up call. The same focus and discipline used to grow your brand must also protect it. This means holding your team to the highest standards and working only with partners who are genuinely committed to safeguarding your information, customers and brand as if they were their own.

54%

of companies suffered data breaches in 2024, and 44% were affected by ransomware attacks.

GetApp, Data Security Report, 2024

58%

of B2B marketing leaders say their organization's view of brand safety now includes how they form partnerships, choose suppliers and make key business decisions.

Forrester, B2B Brand and Communications Survey, 2024

This timely white paper highlights today's most prevalent—and preventable—threats to brand trust, offering practical steps that marketing leaders can take to reduce risk. It also provides guidance on how partnering with the right organizations can help protect the brand equity you've worked so hard to build.

I. HEIGHTEN CYBERSECURITY AND DATA PROTECTION

Unfortunately, cyberattacks and security breaches are a routine cost of doing business. Today's events are personalized, persistent and public. If you're not prepared to respond, a single incident can seriously damage your brand and your ability to do business.

REPUTATIONAL RISKS

Marketing leaders beware. The very channels used to engage customers are also prime targets for cyberthreats. Bad actors aren't only after data—they're after your reputation.

Erosion of Brand Equity

A cyberattack can strip a brand of its competitive edge and bring its reputation into question, diminishing its value in the eyes of its customers, investors and partners. Stakeholders may shift from seeing your brand as reliable or innovative to viewing it as risky—a perception that can persist long after the incident is resolved.

Shaken Customer Confidence

Compromised private data damage customer trust, and regaining confidence is an uphill battle. Even the most loyal customers may leave, particularly if competitors appear more secure or transparent. Future promises—such as product updates or privacy commitments—are often met with lasting skepticism, making it harder to rebuild relationships and regain momentum.

Financial and Operational Loss

The average cost of a data breach in the U.S. is $9.36 million, nearly double the global average of $4.88 million (IBM, 2024). Aside from the cost of containing the breach, these events often result in immediate revenue losses, as customer trust declines, and public companies may experience a drop in stock prices. Legal fees, fines and compliance costs further strain resources. Additionally, the company is forced to shift its focus to crisis management and recovery.

95%

of organizations agree that customers won't buy from them if they don't believe their personal data are properly secured.

Cisco, Data Privacy Benchmark Study, 2024

1 in 3

consumers said they stopped doing business with a company after it experienced a data breach, and 65% said they lost trust in the organization after it had one or more breaches.

Ponemon Institute, 2017

51%

of organizations say they had to increase their prices following a breach.

IBM, 2024

STRATEGIC SAFEGUARDS

Even the best-defended brands face attacks and potential fraud. What sets them apart is how they prepare and respond.

Secure Strong Partners

External marketing resources are essential to your broader ecosystem, but if not properly managed, they can become a liability. That's why it's important to vet vendors before onboarding them and to evaluate their security practices, data encryption standards and history. Prioritize partners trained to handle sensitive data and who have completed robust internal audits, such as the System and Organizational Control 2 (SOC 2®) examination, which verifies strong safeguards for protecting customer information.

64%

of organizations report that third-party risk management is viewed as a strategic imperative by their boards of directors and executive teams.

ProcessUnity and CyberGRX, 2023

Elevate your brand with stronger security. See how a SOC 2 examination can enhance marketing performance and brand credibility on page 7.

Collaborate Cross-Functionally

Marketing often involves using tools and tactics that handle sensitive data. Team up early with colleagues from your company's IT, legal and compliance units. It will give you time to spot risks, select the right platforms, ensure data security and double-check any disclaimers or disclosures. Getting everyone on the same page upfront helps avoid last-minute surprises and builds a sense of shared responsibility.

PRO TIP:

"The right marketing partner doesn't just support your brand; they protect it like it's their own. With shared values, trust and true alignment, an agency should feel like a trusted extension of your team."

— Jason Boucher, Vice President of Client Services, ZLR Ignition

Build a Security-Aware Marketing Culture

Make security part of the marketing team culture. This means training staff to recognize phishing attempts, secure log-ins and understand how social engineering can target brand accounts. When teams understand the risks and their role in preventing them, they're more likely to adopt secure practices in their everyday work. Security awareness should be as routine as creative reviews or campaign analytics.

CASE STUDY

Mailchimp Social Engineering Attack

In January 2023, leading email marketing platform Mailchimp suffered a breach after attackers used social engineering to trick employees into revealing credentials. The intruder gained access to internal tools and data from 133 customer accounts, potentially exposing names, email addresses and mailing lists.

Although MailChimp acted quickly to contain the breach and reassure users that no payment data were compromised, the reputational damage was already done. For a brand built on enabling secure, direct communication between businesses and their audiences, this was the second major breach in less than a year, raising serious concerns about its internal cybersecurity culture.

Takeaways: Even the most secure platforms are only as strong as their weakest human link. Ensure that your team—and your vendors—are trained to recognize cybersecurity threats, follow strict data protection protocols and have strong processes in place to preserve trust and brand integrity.

II. STRENGTHEN PAID MEDIA COMPLIANCE OVERSIGHT

Your brand's stage is as important as its script. Promoting and protecting it in the complex world of media call for smart tools, clear standards and a strategy that's always one step ahead.

REPUTATIONAL RISKS

What you can't see in your metrics might be the most dangerous. Risks associated with paid media are often hidden, but the consequences are painfully real.

Ad Fraud and Bots

Ad fraud is one of marketing's most costly—and most overlooked—threats, with U.S. advertisers losing over $15 billion in 2024 (Statista, 2025). Driven by bots and bad actors, it generates fake clicks, impressions and conversions that make underperforming campaigns appear successful.

~50%

Nearly half of all internet traffic comes from nonhuman sources.

Imperva, 2024

However, the real damage runs deeper. Ad fraud distorts your data, misguides your strategy and quietly drains your budget. Left unchecked, it erodes brand trust and makes connecting with genuine customers more difficult.

Non-Contextual Ad Placements

When your ads show up near off-brand content that doesn't align with your audience, it hurts your reputation. This kind of mismatch lowers engagement and weakens your message. But it's not only about performance. Irrelevant ad placements could also cloud your brand's identity and leave your customers uncertain about what your brand stands for.

Association with Harmful Content

Placing paid media is about visibility and association. When your brand appears near harmful or inflammatory content, such as misinformation, controversial content or graphic imagery, your audience may perceive it as an implicit endorsement. It can provoke swift backlash, trigger distrust and push you into crisis mode. For brands that invest heavily in purpose and positioning, this kind of exposure can seriously undermine hard-won equity.

PRO TIP:

"Context is the unsung hero of brand trust and one of the pillars of media targeting. When your ad appears in the right environment, it speaks louder, lands better and builds stronger connections."

— Jess Kennedy, Director of Media, ZLR Ignition

7 in 10

consumers believe a brand's ad placement reflects its values, and 1 in 2 say they'd abandon a brand if its ad appeared near inappropriate content.

Integral Ad Science, 2024

STRATEGIC SAFEGUARDS

Expert oversight is no longer a luxury—it's a necessary line of defense. Strategic media expertise helps determine where to place your message, how to spot threats and when to pivot.

Enlist the Experts

The media landscape is crowded and constantly shifting. Protecting your brand demands innovation, sharp oversight and deep expertise to spot risks and respond quickly when tactics change. That's why working with a proven partner is a smart strategic move.

Today's agencies do more than buy ad space; they protect your investment using advanced tools to detect fraud, monitor performance and strategically place messages where they will have the greatest impact. They know how to catch low-quality traffic before it drains your budget and ensure that every dollar you spend drives real, measurable results. Equally important, they give your internal team the space to focus on what matters most: long-term brand growth.

Insist on Transparency

Unclear buying of both traditional and digital media can hide risky placements and needless spending. Demand full transparency from agencies, platforms and vendors. Know exactly where your ads are running, which audiences you're reaching and how your budget is being spent. Work with partners that provide detailed reporting and that openly share inventory lists and performance insights.

Implement PreBid Filtration

Don't wait to respond. Use tools that screen suspicious domains, invalid traffic and unsafe environments before your ad is placed. Pre-bid filtration instantly checks whether an ad placement is contextually appropriate and relevant for your audience. It also blocks and monitors risky sites and content categories, helping ensure that your ads will never appear alongside content that doesn't align with your brand standards.

Invest in Fraud Protection Software

Choose advanced fraud detection and prevention solutions that monitor traffic patterns, flag anomalies and continuously update protections against emerging bot behaviors. This will keep your campaigns clean and your budget focused on reaching real people.

CASE STUDY

Uber's Battle Against Ad Fraud

During a 2017 paid campaign to boost app installations, Uber noticed it was underperforming. A closer look revealed that many of the downloads were fake. Fraudsters had used tactics such as click flooding—where fake clicks overwhelm an ad to fool tracking systems—and spoofed installs, which trick the system into thinking an app was downloaded when it wasn't. In the end, Uber estimated that more than two-thirds of its $150 million online ad budget had been wasted due to ad fraud.

The discovery exposed Uber's lack of transparency and control in its performance marketing strategy, critical factors for a tech-forward brand that relies heavily on digital channels to grow and engage its customer base.

Takeaways: Even the most sophisticated brands are vulnerable to ad fraud, making blind trust in performance metrics risky. Don't mistake high numbers for real results. Demand clear reporting, vendor transparency and access to raw data for independent verification. Regular audits, real-time monitoring and tools like anomaly detection and secure analytics attribution are essential to spot fraud and protect your budget.

III. THE STANDARD YOUR AGENCY PARTNER SHOULD ALREADY BE MEETING

For smarter, safer and more strategic marketing support.

Marketing leaders are expected to move fast, cut through the noise and deliver measurable results. As campaigns become more data-driven and integrated, one question stands out: *Can we truly trust the systems and partners powering our brand*? That's why working with agencies that don't just talk about security but are committed to adhering to it with verifiable standards is key.

Short for System and Organization Controls 2, SOC 2® is a recognized auditing framework developed by the American Institute of Certified Public Accountants. It assesses how well an organization protects customer data based on five key trust principles:

- **Security:** Are systems protected against unauthorized access?
- **Availability:** Can your marketing partner's infrastructure perform updates while campaigns are live?
- **Processing Integrity:** Are operations functioning as intended, without errors or manipulation?
- **Confidentiality:** Are audience segments, campaign data and creative assets handled securely?
- **Privacy:** Are personal details collected, used and stored according to regulatory standards?

> "The SOC 2 examination doesn't test intentions—it demonstrates a company is doing the work. It's the difference between merely saying you take data security seriously and proving that you have processes in place to follow through."
>
> — Colton Rodgers, Director of Security at Zirous, ZLR Ignition's Managed Services Provider

A SOC 2 report isn't bought—it's earned. And keeping it takes commitment and an ongoing effort. Organizations must build and document robust systems: from those that strengthen data protection and cybersecurity controls to those that audit and upgrade hardware, applications and vendor relationships. It also requires continuous testing, monitoring and staff training.

Working with an agency that has a SOC 2 report means you have a like-minded partner that takes regulatory and reputation risk as seriously as you do. It also leads to stronger governance, smoother continuity and greater accountability.

ZLR Ignition received its first SOC 2 report from the certified public accounting and advisory firm UHY LLP.

"Having a SOC 2 report signals that our agency understands the stakes. Participation is voluntary and shows we're invested in the transparency, secure infrastructure and responsible processes to deliver a higher level of support to our clients."

— Xan McNelly, CEO and Chairman, ZLR Ignition

IV. BUILD BRAND CONSISTENCY AND ALIGNMENT

Every interaction has the power to strengthen or weaken your brand. That's why marketing teams need a solid strategy to ensure alignment, consistency and protection.

REPUTATIONAL RISKS

More than a creative misstep, brand inconsistency is a strategic liability. It undermines performance, confuses customers and erodes your brand equity. The consequences can have a ripple effect.

Diluted Brand Identity

When teams use different messaging priorities and brand visual cues, the core value proposition starts to splinter. Over time, the brand becomes harder for customers to recognize, remember and trust. Instead of a unified identity, you're left with a patchwork that weakens your brand's impact and confuses your audience.

Customer Confusion

If your brand's look or message varies across channels, it creates confusion. Customers may question what your brand truly stands for or worse, may wonder if it's really you. That uncertainty can stall conversations, weaken trust and ultimately cost you revenue.

89%

of customers expect a consistent experience across a brand's digital platforms, but only 29% say they actually get it.

Salesforce, 2023

3.5X

Consistent brands are 3.5 times more likely to enjoy excellent visibility than inconsistent brands.

Inc., 2017

PRO TIP:

"Consistency in a brand's look and voice crafts a story that resonates—one that audiences not only recall but come to trust."

— Phil Schriver, Creative Director, ZLR Ignition

Regulatory Issues

In regulated industries like insurance, financial services and health care, incorrect messaging or missing information isn't only off-brand; it can also be a compliance violation. These missteps can cost you credibility and momentum, and may lead to financial penalties.

69%

of compliance officers cite marketing content governance as a top area of emerging risk.

Gartner Risk Management Survey, 2022

STRATEGIC SAFEGUARDS

Having a solid framework in place helps ensure that you are focusing on the right brand priorities and staying true to delivering your brand promise while remaining compliant with legal and regulatory standards.

Turn to Your Touchstone

Use your vision, mission and values to filter decisions. Whether you're evaluating a new partnership, launching a campaign or navigating a brand crisis, ask yourself: *Does this reflect who we are? Does this partner align with our values?* These aren't only philosophical questions—they're strategic guardrails that help you protect your brand.

PRO TIP:

"Go beyond clicks and conversions. Prioritize your brand health and reputation and monitor it on an ongoing basis."

— Katie Geraty, Strategy Lead, ZLR Ignition

Simplify with Standards and Structure

Establish policies for content creation and review. Provide easy-to-follow brand guidelines, tone-of-voice standards and compliance checklists that enable your teams to know exactly what is expected of them. Don't forget a sunsetting process for retiring outdated content.

Centralize Content Management

Store all brand assets—messaging, visuals, documents and digital assets—in a single, secure system. This approach helps streamline updates, enforce version control and reduce the risk of releasing off-brand or noncompliant content. Centralized content management helps protect brand integrity while keeping teams aligned and referencing the most up-to-date brand information and materials.

V. PLAN FOR CRISIS COMMUNICATIONS

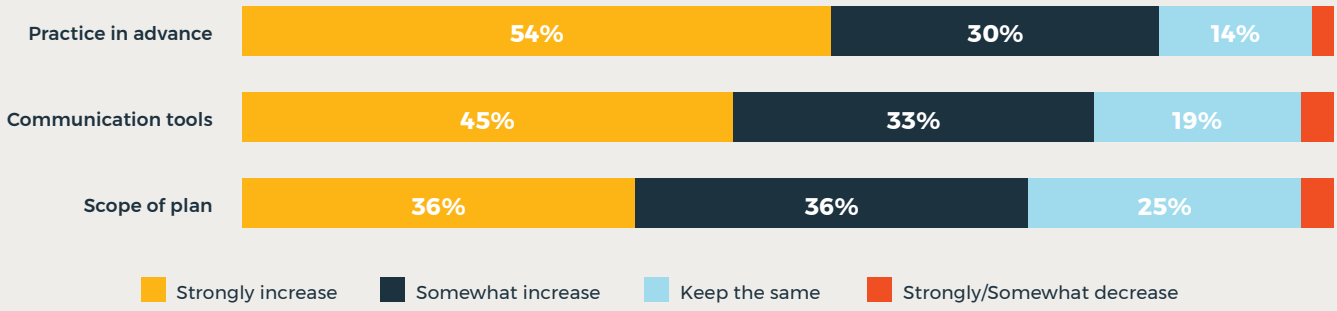
No brand is immune to crises, but every brand can be prepared. In an era of viral headlines and instant reactions, news spreads faster than your team can respond. That's why the best time to prepare for a public relations crisis is long before it begins.

72%

of business leaders who used a communications plan during a crisis say they would broaden its scope.

Capterra, 2023

What Organizations Say They'll Do Differently After Facing a Crisis



Source: Capterra's 2022 Crisis Communications Survey

REPUTATIONAL RISKS

The difference between surviving a crisis and being defined by it often comes down to one thing: communication. Without a strategy, brands risk losing control and damaging their credibility.

Loss of Public Trust

Without a crisis communications plan, brands often respond too slowly—or worse, with conflicting or problematic messages. This erodes trust with customers, employees, investors and the public. Even after the crisis passes, search results, news archives and social media trails can keep the misstep alive and make it a permanent part of the brand's record.

Narrative Hijacking

If your organization doesn't control the story, someone else will. In the absence of a proactive strategy, misinformation, speculation and criticism can quickly dominate the narrative. Allowing others to frame the crisis undermines your credibility and makes your recovery far more challenging.

Internal Misalignment and Leaks

Without internal protocols, employees may learn about the crisis from the media or social platforms instead of from the company's leadership. This will cause confusion, lower morale and increase the risk of leaks, speculation or harmful internal commentary becoming public, only compounding the crisis.

#1

Employees rank as the most effective brand influencers.

Cision, 2025

Regulatory and Legal Exposure

Poor crisis communication invites scrutiny from regulators, legal authorities and watchdog groups, especially for issues involving data privacy, safety or misleading practices. A well-prepared plan helps ensure timely, accurate and compliant messaging, mitigating legal and reputational risks.

STRATEGIC SAFEGUARDS

Staying ahead in a crisis means combining sharp risk intelligence and a thoughtful communications strategy with coordinated action—before trouble strikes.

Audit Brand Vulnerability

The goal isn't merely to react to what's in front of you, but to anticipate what's around the corner. Practice social listening, monitor shifts in public sentiment, track competitors and follow emerging industry and cultural trends. When you detect issues early, you stay in control of shaping perceptions before panic sets in.

Work with partners who meet higher security and accountability standards. Ask your agency if they have a SOC 2 report and learn what it means for trust, performance and protection on page 7.

Build a Cross-Functional Team

Bring together key voices from management, operations, legal, customer service, internal and external communications departments and any other critical stakeholders. Your crisis plan should clearly outline roles, the chain of command and how decisions will be made and approved. Include detailed checklists: who gets notified (and when), how quickly the team will mobilize and which audiences to consider. Designate a spokesperson who can deliver clear, confident messages under pressure. Making these decisions in advance ensures that your response will be faster, focused and more effective.

Create a Message Library and Templates

For the scenarios most likely to impact your brand, prepare holding statements, sample press releases, talking points, social media posts, website copy, etc. That way, in the critical moments of a crisis, you won't be scrambling to write from scratch. Instead, you will be ready to respond with clarity and consistency, using preapproved language that reflects your brand's values and voice. Your plan should also outline which communication channels to use and when to use them, so that every message will reach the right audience at the right time.

Turn Planning into Performance

Planning is only half the battle. Confidence in a crisis comes from turning plans into practice with regular training and simulations. Conduct realistic crisis scenarios that target your brand's unique vulnerabilities at least annually, or more often for high-risk industries. These exercises will stress-test your protocols, reveal decision-making gaps and sharpen the instincts your team needs when every minute counts.

Always follow up with a thorough debriefing to identify areas for improvement and to update your plan accordingly. Be sure to equip your spokespeople with media training to ensure that they will remain calm, clear and credible under pressure.

PRO TIP:

"Smart brands don't plan for failure—they plan to protect what they've built. Having a strategic crisis communications plan lets you lead with confidence and uphold your reputation and relationships."

— Rhonda Clark-Leyda, Director of Public Relations and Content Strategy, ZLR Ignition

CASE STUDY

CrowdStrike's Communications Crisis

In July 2024, a global outage of the cybersecurity platform CrowdStrike disrupted millions of Windows systems and brought critical infrastructure to a standstill. What began as a technical failure quickly escalated into a full-blown reputational crisis. CrowdStrike CEO George Kurtz's initial statement was delayed and widely perceived as defensive, too technical and lacking empathy. It failed to acknowledge the real-world chaos unfolding for hospitals, airlines and businesses worldwide.

The fallout was swift: CrowdStrike's enterprise customers lost confidence, media coverage turned sharply critical and social media sentiment became overwhelmingly negative. While CrowdStrike's brand is built on trust and protection, in a moment when those values mattered most, it struggled to lead with the accountability that its stakeholders expected.

Takeaways: Every organization needs a communications plan that prioritizes speed, clarity and transparency. Being well-prepared gives your team the ability to respond strategically rather than reactively when a crisis occurs. It ensures your messaging is timely, consistent and empathetic while protecting your brand and reinforcing trust. The fundamentals remain the same: act fast, be honest and always consider your audience.

ZLR Ignition is a brand and marketing agency that turns bold ideas into powerful results. We blend insight-driven strategy, creative communications and relevant media to help organizations connect with their audiences in meaningful ways. From big-picture brand platforms to nimble digital campaigns, we turn complexity into clarity—and ambition into action.

Let's create what's next. Send us a message at ceo@zlrignition.com or call us at 515.244.4456.