EXECUTIVE PRIMER

Protecting Reputation in a World of Constant Risk

CONTENTS

CONTRIBUTORS AND EDITORS

Harlan Loeb
Phil Gomes, Daniel Webber, Aaron Guiterman, Andrew Liuzzi, Leigh Nakanishi, Aaron Walker, Neely Dockins, Anne Mitchell, Jared Nelson, Elizabeth Pigg, Cailly Morris

SECTION 1

INTRODUCTION: DIGITAL REPUTATION RISK MANAGEMENT IN TODAY'S ALWAYS-ON WORLD

By Harlan Loeb

The ever-evolving communications landscape has intricately linked reputation management with the digital world. Corporate executives now must recognize that brand perception functions more like a real-time trading desk, with 24/7 news, social media and online conversation shaping brand perception frequently without the participation of the organization itself.

What does this mean for executives today? Very simply, managing your reputation must be an active, ongoing strategic investment begun well before any risk or crisis breaks. Protocols, plans and procedures will prove useless if introduced as a crisis erupts. Preparedness planning needs to start with the shared acknowledgement across the company, most importantly at the executive level, that reputation management practices must be built into the fiber of every business. This means that risk management considerations must be a part of the everyday function beyond simple operational readiness. Tactically, this mindset translates into tasks such as conducting online listening on a regular basis to provide an early warning system as well as gather intelligence that will inform your response strategy in a crisis situation. Finally, executives need to train their managers and communicators while testing their procedures under crisis conditions.

The real secret to a successful reputational risk management program depends on leaders' ability to maneuver with agility as they respond to the immediacy and uncertainty of social media. The scale and impact of social media-fueled crises cannot be overstated. Social media gaffes are occurring faster than we can write case studies to learn from them. These crises often

put senior decision makers into operating situations requiring fast decisions in uncertain conditions and team coordination. These situations often resemble combat environments and can serve as a stark contrast to senior leaders' normal working conditions.

For executives, reputation risk management is an integral part of effective leadership. And understanding the critical role that digital communications play in this environment is vital.

This paper outlines the key elements for harnessing the power of digital tools to protect and promote corporate reputation. Each section contains a short "executive checklist" to help spark conversations with your teams, and to illuminate the complex and evolving landscape of communications today.

SECTION 2

BUILDING A FOUNDATION THROUGH IDENTIFYING AND ENGAGING INFLUENCERS

There's an old adage, "Don't count the people you reach. Reach the people who count." In times of crisis, reaching out to those who count the most to your organization is critically important.

This goes beyond determining who has the most followers on social media—people too often confuse "influence" with "reach." The former is most accurately defined as the degree to which someone can inspire others to do something, whether to share a piece of content or actively participate in a demonstration. A pop star, for example, may have millions of followers on Twitter, but it's rare that he or she would be able to move people to, say, launch a sustained and credible protest.

Don't overlook your organization's most devoted fans and followers. They often serve as loyal voices to help shape the conversation and activity in times of crisis and must be identified well before a crisis hits. By engaging them early with authentic communications, these fans can spread your message to their own networks. However, they also are likely to be brand-sensitive, meaning they will prove more likely to take action if a brand delights or disappoints. While your own fan base offers a valuable asset, carefully nurture it with information that's easily grasped and that you wish to share to help defend your organization.

This approach goes a long way toward answering two important variables in Section 3, "When to Engage?"– relationship and influence. In time – and attention – starved scenarios, determining your high-value contacts will help your organization make smart bets quickly.

Your community of dynamic online influencers may change depending on the topic of the situation,

the geography or the groups impacted. To best prepare, first identify core groups ahead of time: loyal fans, industry influencers, key opinion makers such as journalists or bloggers, and finally industry or brand detractors. Knowing potentially negative influencers, such as those who may be constant skeptics or critics from the beginning, is equally as important as knowing positive influencers. From there, establish the systems, tools and processes to reevaluate and identify influencers quickly who are most relevant to the particular situation. Once you have identified the key influencers, carefully consider specific messaging to each group in each situation. No “one size fits all” content strategy exists in a crisis. The sooner you can identify and engage with those who matter most to your organization, the sooner you can begin addressing the situation directly.

EXECUTIVE CHECKLIST

Ensure your team:

1. Establishes a baseline understanding of key online and offline influencers in your industry.
2. Invests in the tools and processes necessary to evaluate quickly those influencers who account for industry, geography and groups affected in any given scenario.
3. Creates a customer data and information strategy that allows the organization to engage fans.
4. Identifies individual fans (or segments thereof) based on their value to the organization to determine the most loyal.

SECTION 3

WHEN TO ENGAGE: FIVE VARIABLES TO ADDRESS AHEAD OF TIME

Triggered by sensational coverage from business publications and industry trades, communicators worry they will become the next well-discussed, what-not-to-do case study. Consequently, companies often assume an odd form of paralysis when a potential crisis or issue starts to percolate online. Namely, they wonder whether responding at all will pour water on the fire – or gasoline.

Judging this critical inflection point is just as much art and instinct as science. Across industries and geographies, however, five basic variables can help prepare a company to determine its best online response posture.

With whom have we maintained consistent relationships?

You must make your friends before you need them. Develop a list of important online stakeholders and maintain steady communications with this group during the quiet times. If news breaks of an issue or crisis, recognize that a response to them is mandatory.

What is our threshold for what we call "influential?"

People reside outside your list of key stakeholders who, nevertheless, are influential and could have an impact on your business. Judging influence, though, encompasses more than simply the arithmetic of counting an influencer's online fan club. You also must consider the degree to which someone inspires others to action.

How quickly does a conversation need to build up steam to warrant a response?

The Web is not so much about "influencers" as it reflects thousands of smaller voices

who can find each other and amplify a message. Recognizing how conversations gain critical velocity and knowing when to time your response accordingly can help introduce your point of view into the conversation before it develops fully.

If the issue you're looking at doesn't pass any of these three tests, you probably don't need to respond to it just yet. In fact, a high probability exists that doing so will worsen the problem. But, if one of these tests is passed, two additional factors must be considered:

What is the timing of our response?

You don't always have all of the answers and, generally, this is fine. Often, a community just wants to know that you're listening to it. Acknowledging that you are aware of the issue

is enough; at least until you are fully able to assess the situation.

Where will we publish our response and notify stakeholders?

The Web has changed the way we look at Marshall McLuhan's timeless adage "The medium is the message." In many cases, a debate will exceed its online medium. Sometimes a response on Twitter or Facebook proves sufficient, although other platforms such as a website or a blog frame complex issues more comprehensively.

One's mileage, though, may vary depending on your industry, geography and topics of interest. That said, these variables are most important to address ahead of time in determining whether it makes sense to engage online during a crisis.

EXECUTIVE CHECKLIST

Ensure your team:

1. Maintains communications with the people who matter to the business, regardless of immediate need.
2. Identifies criteria for what the company considers an "influential party."
3. Identifies a threshold for what the company considers to be a sufficient velocity of discussion before considering a response.
4. Confirms reporting structures and approval privileges to help the company create and approve timely responses when needed.
5. Establishes sufficient control of the company's online properties so it can publish items quickly.
6. Determines the best channels for certain types of content and audiences.

SECTION 4

CONVERSATION MONITORING: FIRST LINE OF DEFENSE

Social media serves as an easy, efficient and express outlet for news to break – whether factual or not – with the ability to impact your business in the blink of an eye. It's critical to keep your finger on the pulse of this online conversation.

Consider online monitoring to be your first line of defense to gauge messages around your organization. When set up in advance, this monitoring provides an understanding of your overall perception. It allows you to adjust rapidly to conversational trends. When not established in advance, you can be caught flat-footed, unable to react quickly enough in today's instantaneous information marketplace.

Your online monitoring program

Setting up an effective conversation monitoring program starts with a deep understanding of your business – the industry, your executives, the countries and languages where you do business and your key rivals. Your team should focus on four key areas when getting started:

Search Audit: Start by grasping the language of your target audiences, especially how they search for information online. This delivers a glimpse into consumer behavior and provides a full set of keywords that are used actively and associate with your organization.

Conversation Audit: Next, identify the keywords to form a taxonomy that can be entered into an analysis tool to monitor online conversations as they happen and help gauge interest in your organization online. This will help you understand language, opinions, industry trends, the key channels on which people engage as well as preferences that may prove

important to an organization's content and messaging.

Influencer Analysis: Identifying the important personalities and organizations in your industry can prove valuable. They serve as key opinion makers that help shape consumer opinions and amplify messaging. Research and identification can help prepare your organization to understand more about influencer communities, what they care about and how they engage online and offline.

Measure Performance: Measurement provides context and sets performance baselines. As situations unfold, understand what is expected, what is good and what is bad. Developing measurement criteria, parameters and key performance indicators will furnish the information you need to quickly evaluate threats, opportunities and the effectiveness of your response.

The ability of your team to gauge the impact of an emerging issue to determine an appropriate response also proves critical. As addressed in a later section, this ability to separate emerging issues quickly based on their impact to your organization can ensure an appropriate response.

Handling a reputational challenge or crisis effectively starts with recognizing the warning signs early. With an established program, guidelines and procedures in place early, your team can keep their finger on the pulse of the online conversation. This allows you to begin the so-called OODA loop (observe, orient, decide and act) quickly and nimbly in a time of crisis.

EXECUTIVE CHECKLIST

Ensure your team:

1. Invests in robust enterprise monitoring tools such as Radian6, Sysomos or Command Center™, Edelman's proprietary risk sensing tool.
2. Trains members across the organization to use the tools.
3. Establishes a taxonomy of terms that define the organization, competitors, executives and key industry terms. Translate the taxonomy into all languages in the markets where you operate.
4. Coordinates monitoring and escalation protocols globally.

SECTION 5

CONTENT STRATEGY AS A STRATEGIC CRISIS ASSET

Operational readiness – such as enhancing online monitoring, leveraging decision frameworks or setting up a dark site – is essential in order to swiftly mitigate potential threats to your company's reputation or business. However, one area that is more often a "nice-to-have" rather than a "need-to-have" is incorporating a content strategy into both crisis communications preparation and response.

The term "content strategy" may sound like PR jargon or something pulled out of a marketing plan. Simply put, content strategy combines engaging content with real-time trends to tell a cohesive brand story. In advance of a crisis, this approach is likely something marketing and communications teams are engaged in already. The strategic creation and application of online content in a variety of forms – video, image, infographic, text, article – will allow your brand to build strength and credibility as search results become more optimized over time. This optimization also will serve to aid when an issue or crisis arises and people quickly need to be able to find an official response from your company.

Leveraging strategic content within the context of crisis forces the question, "How are you engaging your key stakeholders and audiences beyond a text response?" At times, the stress of a crisis situation yields the path of least resistance, or posting what response you can, as quickly as you can.

Given the power of visual content – emotionally, and as weighted by Google and other social channels – it is critical that companies incorporate a robust content program into crisis response planning. This will allow you to be well-positioned to share

information in a meaningful, holistic way that will resonate with your audiences during a time when it's arguably most critical. This underscores the need to ensure that communications and marketing functions cooperate and work toward the same set of goals – because someday, a crisis will require each other's resources.

EXECUTIVE CHECKLIST

Ensure your team:

1. Articulates clear goals and metrics for its content marketing program, expressed in business, not publicity terms.
2. Defines its audiences well and knows their user behavior.
3. Develops and iterates a content plan to help ensure that it has high confidence that it can develop the kind of stories that will travel.
4. Produces content that is as close as possible to the audience's normal media consumption habits than traditional marketing material, which relies on interruption.
5. Selects its online channels carefully with regard to audience presence.

SECTION 6

YOUR OWNED MEDIA PROPERTIES: WEBSITES, DARK SITES AND MORE

When you're at the center of an unfolding risk, you must demonstrate a strong voice to counteract the forces of social and traditional media that quickly will shape the narrative. Press releases and news conferences are insufficient to meet expectations – or to fill the growing vacuum for content that exists online, particularly among search engine results. Your owned media properties – in particular, your organization's website and social channels – serve as critical tools to provide information that frames the issue from your perspective, addresses misinformation and, if necessary, apologizes for the situation with a clear action plan.

Strategic use of "owned" media properties will serve as a beachhead, interrupting the rapid pace that information, rumors and misinformation get shared online. The owned property or channel should serve as a clearinghouse of information that includes statements, points of view, Q&As and other materials (e.g., videos, audio, infographics) that are shared easily across social and traditional media and appear prominently in search engines. Your organization must emphasize rapid content creation and distribution at the earliest stages of a rapid response strategy. Creating and distributing your own content provides a new opportunity to reach stakeholders and influencers directly without having to go through a filter (e.g., the media).

Some organizations house content on "dark sites" – websites built in advance of a crisis and staged with templates and materials that activate with the flip of a switch. Others simply put a protocol in place to provide guardrails on what must be done during a crisis – whether it's posting materials in an online pressroom or prominent

social media channel, or creating a section on the organization's homepage specific to an issue. Preparation and rehearsal are important in responding swiftly in a crisis.

Establishing these protocols and systems in advance of a crisis – and then testing and training on them – provides discipline and structure. This prevents a lag in response time and minimizes the potential impact of a crisis.

EXECUTIVE CHECKLIST

Ensure your team:

1. Discusses the potential need or benefit of creating "dark sites" – microsites and social media assets – that can communicate information immediately during a crisis.
2. Creates a plan for generating and posting content on your website and other "owned" assets during a crisis.
3. Develops a map or audit of all of the company's "official" company digital assets with a corresponding list of primary contacts to update each asset.
4. Institutes a specific crisis plan or escalation framework for each owned channel should an issue arise and require a response on one of those channels.
5. Develops a plan to increase bandwidth for the principal website to ensure that the site doesn't go down during a crisis.
6. Creates easily accessible template materials and content that can be updated quickly.
7. Drafts a plan for paid advertising or search-engine optimization tactics that helps amplify your content during a crisis.

SECTION 7

PAID MEDIA: CONTROL AND SWIFTLY MANAGE RISK

As issues break, audiences will look to validate news and build context in search engines; additionally, social networks (Facebook, Twitter, etc.) become additional filters through which audiences will discover news through the trusted filter of friends. Reaching and engaging key audiences through these channels and others, with the right message at the right time is critical in successfully managing risk and crises scenarios.

With nearly infinite creative, channel and targeting possibilities, paid media is among the most effective vehicles available for ensuring messages make impact with the right audiences and can additionally provide fast and meaningful insight into audience feedback and response.

Ways brands may leverage paid media throughout crisis and risk planning and management may include, but are not limited to:

- Conditioning the environment
- Stabilizing and building positive brand reputation
- Managing issues-focused news cycles
- Reaching key stakeholders, driving message visibility in real-time
- Addressing and suppressing detractors
- Repairing reputation
- Retargeting, re-messaging stakeholders

EXECUTIVE CHECKLIST

Paid media is most effective and can be activated quickly when proactive measures are in place. Ensure your team:

1. Develops paid media accounts and establishes credit lines with platforms including: Google, AdWords, Facebook Business Manager (including Instagram), YouTube Analytics (through Google) and Twitter Analytics.
2. Activates website analytics and applies tags (ex. Google Analytics) to accurately measure results, assess behavior and engagement with content.
3. Establishes a template for ad creative that can be adjusted quickly and deployed when needed.
4. Identifies priority target audiences, channels and platforms.
5. Establishes priorities for geographic and demographic targets of key stakeholders.
6. Organizes staffing structure (including coordination with agency partners and internal teams) to deploy quickly in support of crisis response efforts.

SECTION 8

TRAINING AND TESTING

When talking about crisis training and table top exercises, there's a saying that we frequently use at Edelman: Fail to Prepare, Prepare to Fail. In the digital environment, it is more critical than ever to properly test and train properly for crises. The fact is this – if the first time you're reading through your crisis plan is in the heat of an operational or reputational crisis, you're likely going to be behind the curve. And with the pace of today's digital age, it will be hard to recover. In fact, recent data shows that 28 percent of crises spread globally within one hour. Organizations that effectively navigate a crisis and operate ahead of the curve are those who refer to – and are familiar with – a detailed plan, trust a tested staff, and follow established rapid response protocols.

Decisive and effective crisis response is a capability, not a coincidence. It takes preparedness. While there is no way to fully prepare for every possible crisis, it is possible to prepare and test response plans and processes for potential scenarios. The very action of participating in a crisis exercise helps build "muscle memory." Meaning, you identify weaknesses and, often more importantly, shed light on the paralyzing digital unknowns that may lurking (e.g., an attack of your Facebook page, offline crises escalating due to exponential online conversation, Change.org petition calling for operational changes, etc.).

At Edelman, we have created the Edelman Guardian Crisis Simulator Suite to take preparedness to the next level. The suite helps ensure companies and organizations gain customized experiences that create realistic, interactive workshops and training sessions based on known potential threats. We simulate crises that require real-time

responses to multiple converging issues. We identify strengths, weaknesses and gaps in existing response plans and provide a road map for effective response in the event of an actual crisis.

Our crisis training has been developed for not just the front line PR staff and social media manager, but an organization's senior leadership – the people actually addressing the crisis and making minute-by-minute decisions.

To be clear, our goal isn't to teach an organization how to simply tweet through a crisis. Rather, we expect our participants to walk away with first-hand experience of working under rapid-fire crisis conditions that mimic an accurate scenario with their established team. We want our participants to realize that they may potentially need a microsite, pay for Google ads, or post engaging content in

a high-stakes training, rather than floundering for the right answer in the heat of battle.

This type of training should be included before the launch of new major initiatives or product launches, the introduction of a new social media channel, and leading up to pre-identified issues that might challenge the business' license to operate. Social media management requires too much investment in time, money and resources to be misused or even unused during a crisis.

Putting the team through a vigorous stress test, simulation or table-top exercise is a great way to mitigate risk, strengthen the competencies of the team, create needed redundancies and eliminate some concerns. At the very least, it will empower more staff to respond when the inevitable issue does arise.

EXECUTIVE CHECKLIST

Ensure your team:

1. Creates realistic, interactive workshops based on existing or potential threats and issues.
2. Determines materials needed to respond after identifying areas of potential risk,
3. Provides front-line social media personnel with coaching and training experiences that include crisis 101, spokesperson training, regulatory overviews, etc.
4. Turns the tables and allows the response team to "attack" the back-up team to exploit weaknesses.
5. Develops and circulates case studies of relevant issues among managers and employees alike.

SECTION 9

RECOVERING FROM A CRISIS

Most crises – even those expertly managed – leave brands facing a trust-and-reputation deficit. Sadly, in the immediate aftermath of a crisis, too few companies take the time and make the investment to apply the lessons learned effectively and efficiently to improve their own state of readiness and help expedite their reputation recovery.

When reviewing successful recovery campaigns, five common strategies help organizations repair lost trust and each has a clear tactical extension into the digital/social universe. In fact, given that digital/social media platforms often serve as the de facto battleground for crises and issues, the same platforms often responsible for inflaming an issue are ideally suited to help support and expedite recovery efforts.

Emerging from a destabilizing crisis, organizations at a macro level must:

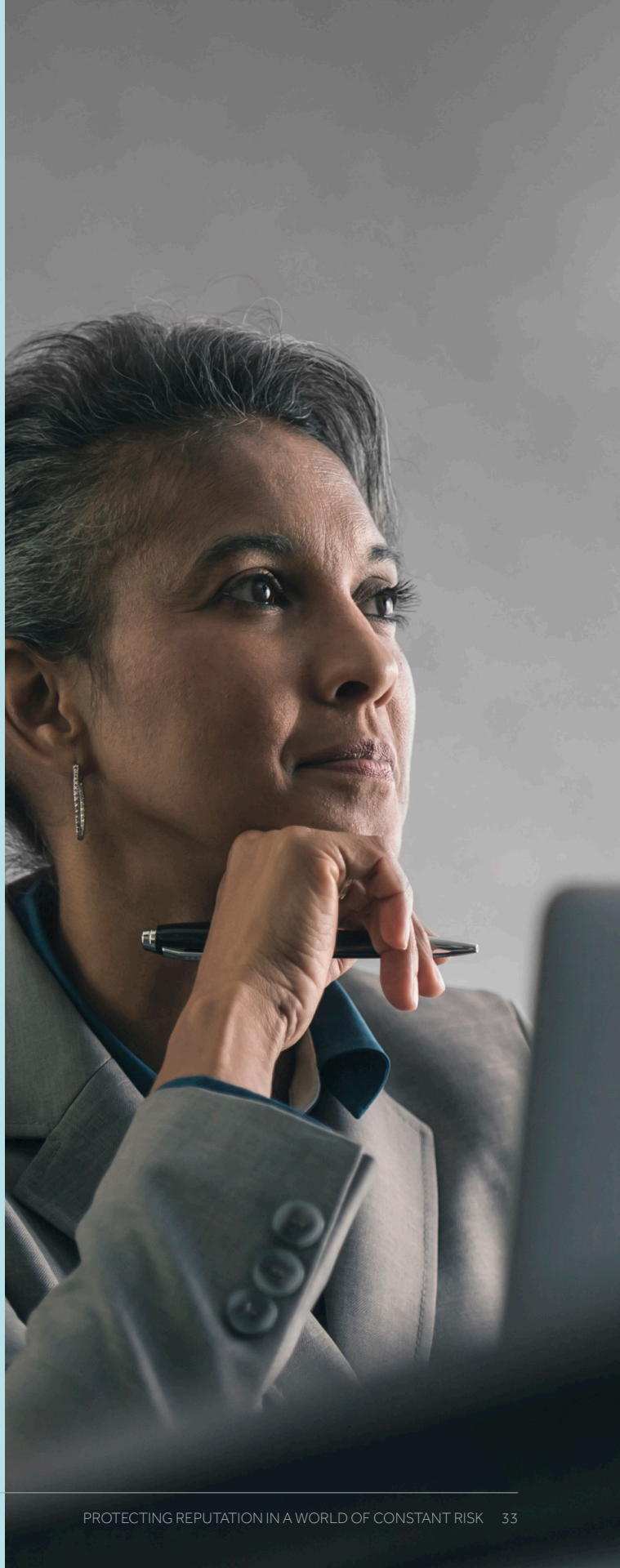
- Listen and engage in two-way dialogue
- Use third-parties to reaffirm stability of core business competency
- Engage in radical transparency
- Employ operational and organizational changes that address the business challenges presented by the core crisis
- Create a stronger industry environment post-crisis

By focusing on these core elements, an impacted organization will harness critical hindsight that serves as a powerful predictor and calibrates its post-crisis, public-engagement and recovery strategy correctly. By integrating valuable insights from digital/social media into the broader reputation-management program, an organization will protect its license to operate in the short-term and strengthen its brand equity long-term.

EXECUTIVE CHECKLIST

Ensure your team:

1. Leverages owned social channels to take proprietorship around the crisis and establishes a communications foundation for immediate next steps in response.
2. Continues to engage openly and transparently with your community.
3. Activates existing allies/supporters to create an echo chamber of support for the organization.
4. Determines the influential advocates online (both in support of and against the organization) who will shape the post-crisis landscape.
5. Commits to providing critical updates and key information to affected stakeholders.
6. Establishes metrics to gauge the qualitative and quantitative impact across the organization.
7. Deploys paid media efforts to transmit your message to your targeted audiences.
8. Reviews existing marketing strategies (including online, advertising, etc.) to determine cultural sensitivity and if/when programming can return to "normal."
9. Conducts a postmortem on internal team response to determine if established protocols were followed in response to the issue.



SECTION 10

EMPLOYEES AS ADVOCATES: GAINING MANAGERIAL CONFIDENCE

Edelman's annual Trust Barometer, now in its 16th year, has demonstrated consistently that the three most credible spokespeople are 1) My friends and family 2) An academic expert, and 3) Companies that I use.

When a crisis occurs, however, the frequent instinct is to place the CEO front and center as chief spokesperson. Considering that the chief executive often ranks close to a government regulator—that is, near the bottom of the Trust Barometer—it's advisable to question why companies are so quick to do this.

While certainly sound reasons (beyond the scope of this essay) exist to use the CEO as chief spokesman, executives often fear that placing a mid-to-lower-level employee out front may risk reputational damage. They figure that such employees may be unaware of the larger impact of their statements, or are unfamiliar with the inherent liability in throwaway comments. (For example, it's common for employees to use terms such as "layoff" and "reduction in force" interchangeably, even though they possess very different legal meanings.) This aversion receives greater velocity and impact when considering the power of the Internet to spread such communications faster than they can be corrected or contextualized.

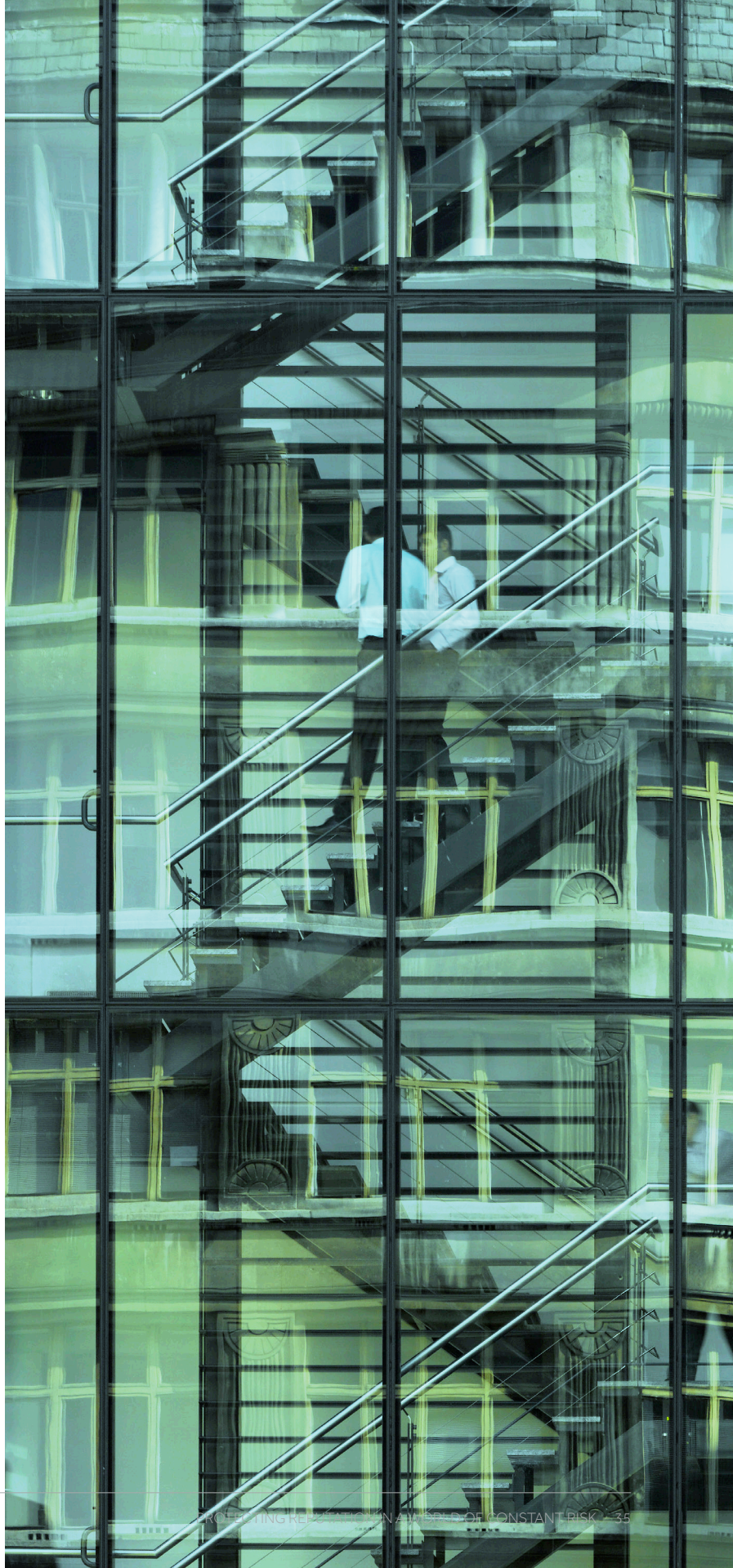
So, how does a company leverage this most trusted set of employees while gaining managerial confidence that employee-spokespeople online won't contribute to "Day Two" of a crisis?

Here are some recommendations:

Prepare a solid online behavior

policy for all employees.
In most cases where the press discusses the latest case of an employee "fired for Facebook," you can count on the company possessing an online behavior policy deficient or wholly nonexistent. Make sure that a policy is in place that not only conforms to regulatory and communication concerns, but understands an employee's motivation and the nature of online communities.

Create a special certification for identified internal experts.
You likely know the people in your company with deep domain expertise and solid spokesperson instincts. Create a formal certification program that helps advance these employees' media capabilities and gives the company managerial confidence that these newly minted spokespeople can be counted on.



EXECUTIVE CHECKLIST

Ensure your team:

1. Media-trains experts and executives, also making them aware of the company's social media policy as well as general online behavior norms.
2. Identifies who in the organization, regardless of title, could become strong advocates for the company and its brands.
3. Puts formal certification programs in place that can deliver spokesperson skills more broadly within the organization.
4. Considers progress-reporting mechanisms that give leadership confidence in this wider group of official advocates.
5. Confirms that internal communication channels allow the company to deliver new certification, news, insights and messaging points to employees.
6. Aggressively seeks out the next group of superstar advocates.

Give these internal experts access to your online publishing workflow. Most organizations online have a formalized workflow that governs how, where and when content is published. Consider giving your employees access to this process, perhaps with varying levels of privilege and pre-publication review requirements.

Keep the internal dialogue going. Make sure certification can be maintained quickly and easily. Mobile or computer-mediated learning works well for this, as do periodic workshops. Developing and maintaining a portal on the company intranet also is effective, especially one that contextualizes industry news for your employee spokespeople.

Allow yourself to be surprised. Your next superstar spokesperson probably thinks the role is out of reach. Ensure that the certification mechanisms you offer your superstars are made available eventually to everyone. When you make the barrier to entry low and the barrier to achievements high, you are apt to create a much deeper bench of credible representatives when you need them.

The following matrix gives an outline for a broader way to think about your spokesperson pool.

	Employee is not proficient in media and/or online engagement	Employee is proficient in media and/or online engagement
Employee's area of expertise is of external public interest	**Missed Opportunities:** High **Risk:** High **Minimum Learning Goal:** Competence	**Missed Opportunities:** Low **Risk:** Low **Minimum Learning Goal:** Expertise
Employee's area of expertise is not of external public interest	**Missed Opportunities:** Low **Risk:** Medium **Minimum Learning Goal:** Awareness	**Missed Opportunities:** High **Risk:** Low **Minimum Learning Goal:** Competence

SECTION 11

COMMUNICATING ABOUT A CYBERSECURITY BREACH ONLINE

Today, media coverage is dominated by cyber-crime – occupying 63 percent share of voice among reputational risk issues even though attacks decreased 36 percent from 2013 to 2014. With the increased media attention, CEOs, Boards and communications teams are demanding greater levels of preparedness, training, response capabilities and protocols.

Unfortunately, one of the biggest challenges in creating a framework for responding to cybersecurity crises lies in the variety of diverse actors and potential threats that can arise. They make it nearly impossible to take a one-size-fits-all approach to preparedness and defense. A few of the main categories of threats emerging include:

Malicious attacks – a direct attack on the organization that creates a denial of service on your websites, erases data or, otherwise, cripples an organization.

Data breach/cybercriminals – criminal activity that involves stealing money or data, blackmail, selling data, stealing intellectual property, etc.

Reputational breach – vandalizing websites to be a nuisance or to commit "hacktivism," broad social media attacks to harm reputation (e.g., creation of activist accounts), releasing private information publicly, impersonation of the company or executive online, etc.

Internal breach – disgruntled employees hijacking websites or social media accounts; industrial espionage, leaks, spying, etc.

Opportunistic breach – lost or stolen devices that provide access, unsecured data and systems, bad passwords and policies to protect data, etc.

No way exists to prepare fully for every possible cybersecurity issue. But it's possible to prepare – and test – response plans and processes for likely scenarios. The very act of participating in a preparedness exercise helps build "muscle memory," identify procedural weaknesses and shed light on any paralyzing cybersecurity variables.

Finally, no technology yet deployed (or reasonably considered) provides 100 percent security against a digital security leak or breach. The occurrence of such a leak is not always an indicator of negligence or failure. The important notion to keep in mind is that an organization must assume that data will leak or digital resources could be undermined. This makes the integration of cybersecurity response principles absolutely essential.

EXECUTIVE CHECKLIST

Ensure your team:

1. Builds an incident response framework that includes communications - not just your technology, security or web teams.
2. Creates a monitoring protocol that seamlessly integrates or partners IT and social media to ensure that as much intelligence is gained as possible around key areas of concern.
3. Develops internal processes and protocols that include a rapid-response team with clear decision makers, builds response plans for each digital asset and assembles scenarios and toolkits for the largest areas of vulnerability, etc.
4. Creates and publishes content across multiple channels (the likelihood of an attack wiping out your communications channels at the same time is low).
5. Practices the plan to help streamline the process and to think through the dynamics associated with potential responding parties (FBI, FTC, FCC, SEC, CFIUS, etc.).

CONCLUSION

Building your reputation in today's complex and always-on world is a complex and evolving process. Answering the questions provided in the Executive Checklists will give you the ability to start engaging your team in a strategic manner and to begin investing in these critical areas before a crisis hits. Just as you invest in human resources, equipment and your business processes, investing in your reputation proves critically important to maintaining your license to operate.

Edelman