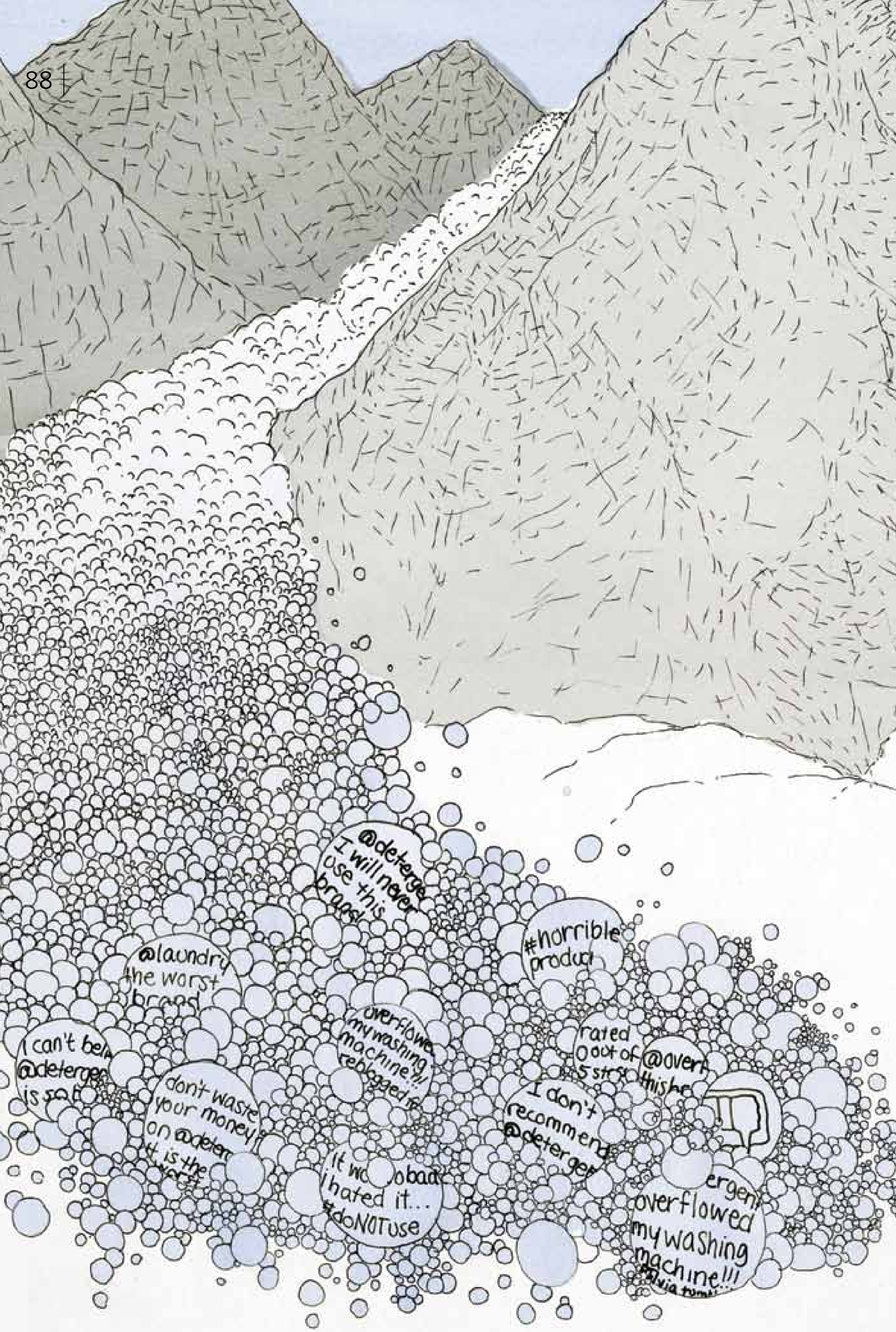
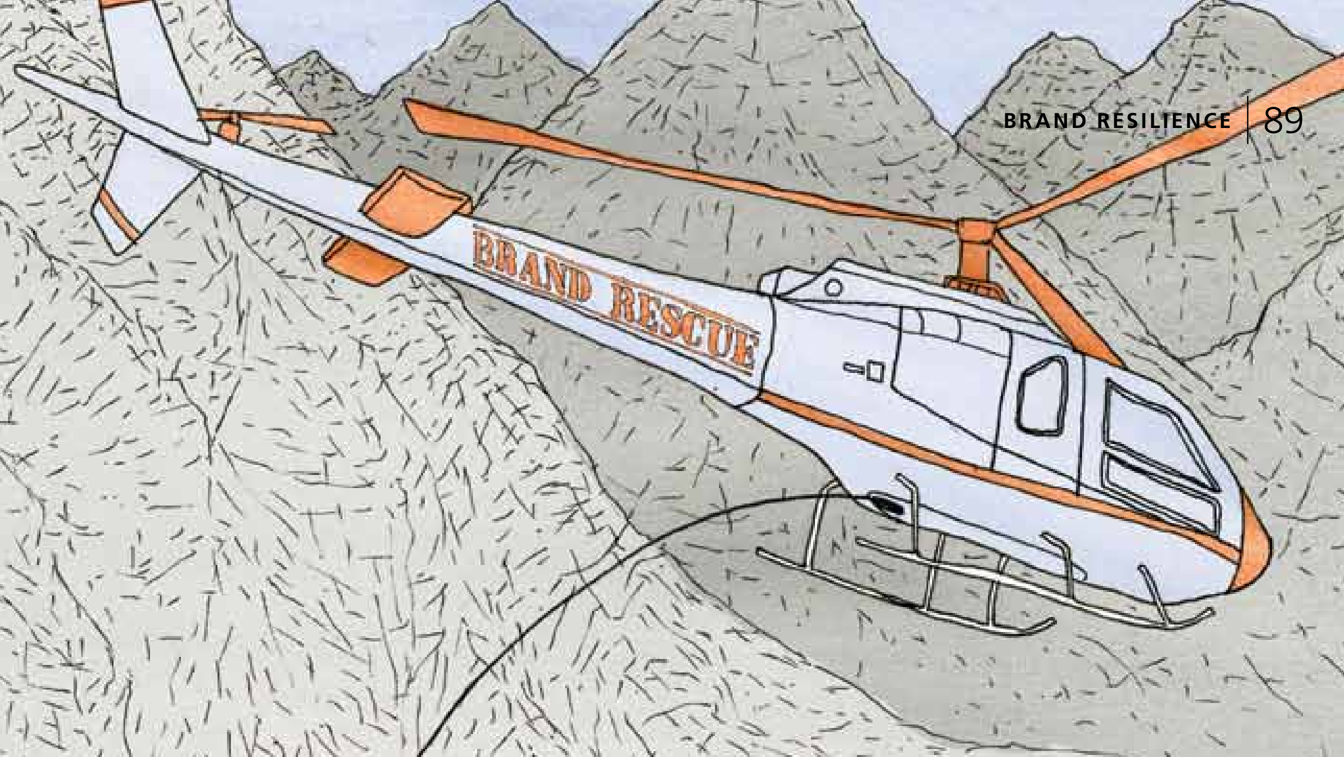

@deterge
I will never
use this
#horrible
produc
@laundry
the worst
overflowe
my washing
machine!!!
rated
0 out of
I can't be
@deterger
don't waste
your money!!
on @deter
it is the
I don't
recommend
@deterger
I hated it...
#doNOTuse
overflowed
my washing
machine!!!



BRAND RESILIENCE

Protecting your brand from saboteurs in a high-speed world

BY JONATHAN COPULSKY, ALICECHANDRA FRITZ AND MARK WHITE
> ILLUSTRATION BY JACKIE HAHN

ON NOVEMBER 27, 2009, at approximately 2:25 a.m., a man drove his car into a fire hydrant. Initial reports notwithstanding, the driver sustained no major injuries and was quickly released from the hospital. Under normal circumstances, the accident might have merited a brief mention in the police blotter of the weekly community newspaper. But news of this particular accident made virtually every major newspaper, broadcast and blog in the world because the driver was Tiger Woods, golf's most influential player and, arguably, the most famous athlete in the world.

Over the ensuing months, the Tiger Woods story unraveled with a series of disclosures about indiscretions and marital infidelity. The exposure of what *New York Times* columnist Frank Rich described as "the maniacally reckless life we now know [Woods] led" was a turning point in the world of marketing, triggering the meltdown of a seemingly unassailable personal brand and threatening the value of high-profile sponsors whose reputation (and integrity) was closely tied to his.[1]

Many of the top brands that featured Woods in their marketing efforts dropped Woods or significantly decreased their reliance on him in an effort to mitigate the damage. A study by Chris Knittel, professor of economics at University of California at Davis, indicates that "… seven publicly held companies that have or had sponsorship deals with Woods lost $12 billion in market value in the month after Woods' statement in December that he was taking a leave from golf."[2]

The Tiger Woods situation vividly illustrates the phenomenon of brand sabotage and why brand stewards need to be more concerned than ever about unintentional, as well as deliberate, attacks on their brands. With a 24-hour news cycle and omnipresent social media that can turn even small blunders into public relations catastrophes, brand reputation is more precarious than ever, and even the most venerable brands are vulnerable. Developing capabilities to detect threats and respond effectively is key to making seemingly healthy brands truly resilient.

The Tiger Woods situation is not an isolated example. Recently we have seen incidents involving:

- *A quick service restaurant – Employee creates viral video while manager watches:* An employee at a local franchise bathes in a sink used to wash utensils while a fellow employee videotapes and a manager watches. The video is posted to YouTube for public viewing.
- *An airline – Flight attendant snaps at passengers before making dramatic exit:* A disgruntled flight attendant, angry with a belligerent passenger, verbally abuses the passenger over the loudspeaker, grabs two beers and makes an exit by sliding down the emergency exit chute. While some hail the flight attendant as a hero for employees everywhere, the incident threatens the airline's strong reputation for customer service.

As social media and mobile technologies continue to embed themselves in our lives, brand sabotage incidents will undoubtedly increase. Four areas may be particularly problematic when it comes to managing brand and reputational risk:

1. Product safety and sustainability across extended supply chains, particularly involving outsourced components and third-party suppliers

2. Disclosure of confidential customer information

3. Inappropriate employee behavior, on the part of senior executives as well as front-line employees

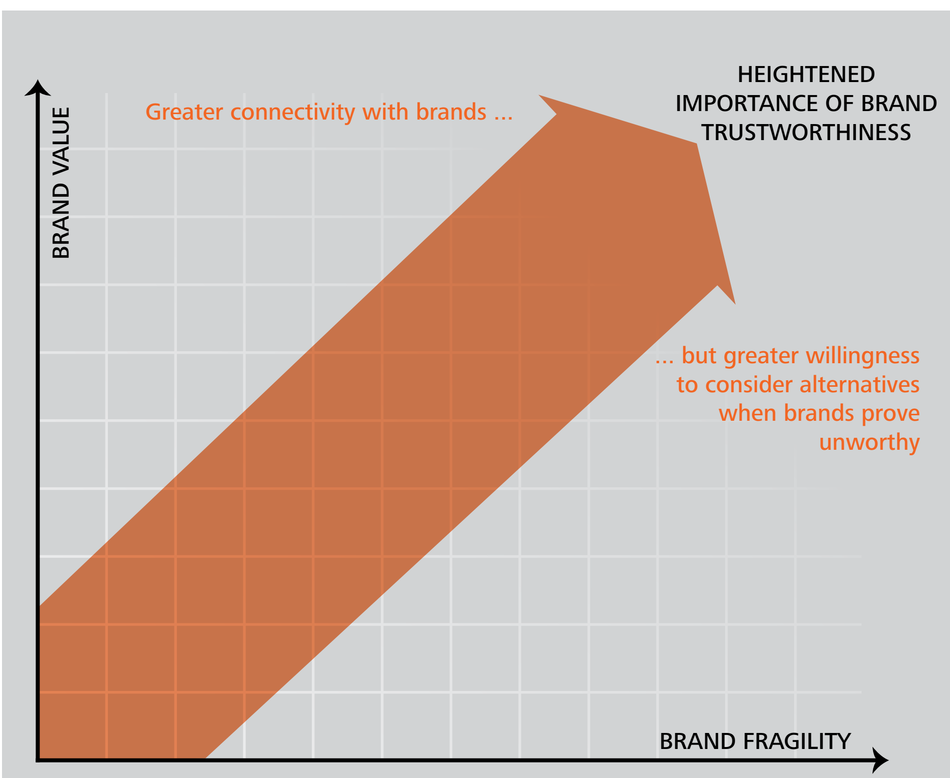
4. Disclosure of highly confidential information (as seen in the 2010 WikiLeaks revelations)

Building a great and resilient brand now requires playing aggressive defense, as well as offense. Building the capabilities to detect, respond to and recover from incidents of brand sabotage will increasingly be key to an organization's marketing and risk management strategy.

DON'T ASSUME THAT VALUABLE BRANDS ARE INVULNERABLE

Increased brand vulnerability seems paradoxical since it comes at a time when brands seem to be more valuable than ever. According to Millward Brown Optimor's 2010 study "BrandZ Top 100 Most Valuable Global Brands," the top 10 most valuable global brands account for almost $700 billion of value.[3] The 2009 version of this study states that in the preceding year of "… global economic turmoil, when every key financial indicator plummeted, the value of the top 100 brands increased by 2 percent to $2 trillion."[4]

Figure 1: The brand paradox



The most valuable brands would seem to enjoy strong relationships with their customers. But strong customer relationships depend on trust and "trust," as the 2010 *Edelman Trust Barometer* notes, "is fragile."[5] Put another way, an untrustworthy brand is a vulnerable one, and every product defect, every incident of egregious executive behavior, every inadvertent disclosure of confidential customer information and every report about what companies say when they thought that no one was listening contributes to this vulnerability. It's a short step from losing a customer's trust to losing their business.

START THINKING LIKE A COUNTERINSURGENT

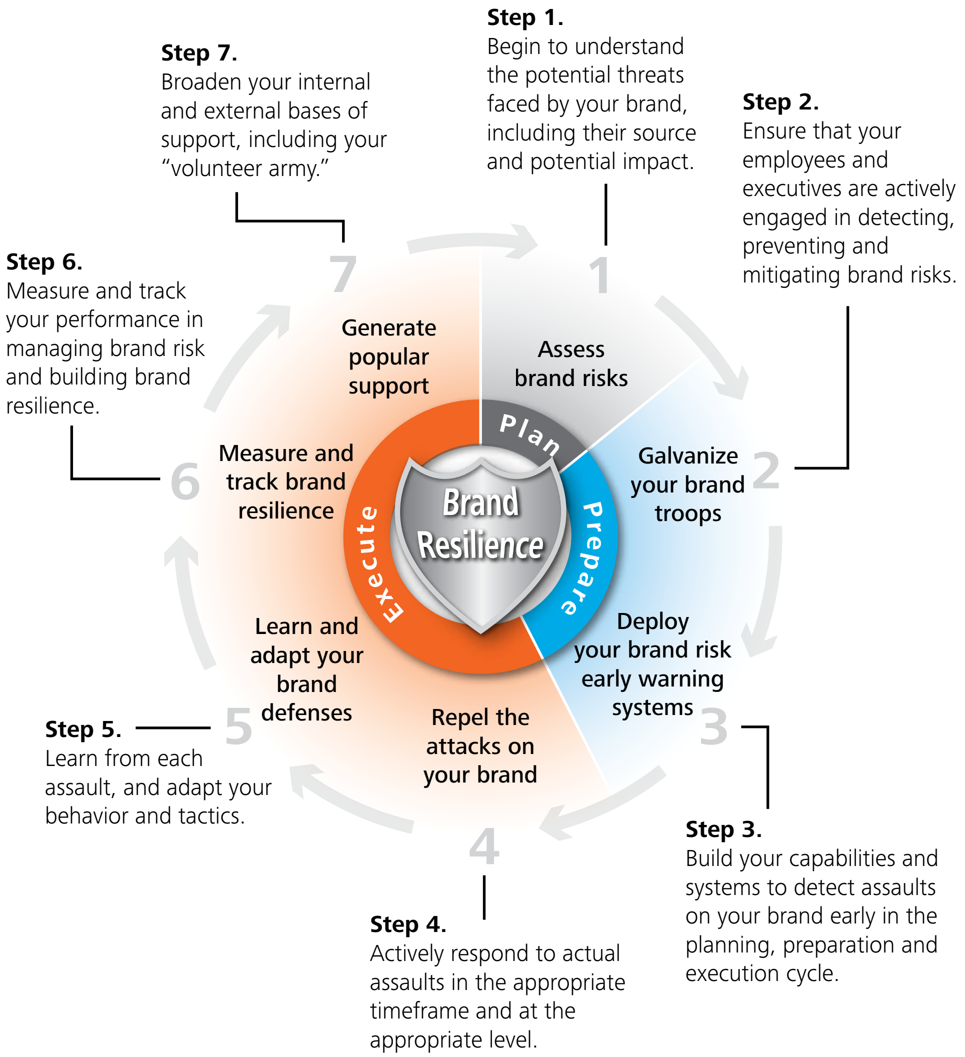
Brands facing random assaults, anonymous enemies using unconventional, but lethal, weapons, incidents of friendly fire, and other threats from insurgents may want to consider taking a page from the handbook written for military commanders to wage conflicts with real insurgents. The guidance in *The U.S. Army/Marine Corps Counterinsurgency Field Manual FM 3-24* seems custom-made for brand stewards struggling to contain brand risks:[6]

1. At first, you may not recognize that you're under attack.
2. Your impulse to respond with an overwhelming show of force to attacks may be misguided. Sometimes, the more force you use to protect yourself, the less secure you may actually be. Doing nothing may, at times, be the most effective response.
3. In wars of insurgency, the winner is the one who learns and adapts quickest.
4. Some of the most effective weapons for combating insurgents are not those aimed directly at them. An engaged populace capable of identifying, disarming and responding to threats may be your most effective weapon.
5. If a tactic works this week, it might not work next week; if it works in this market, it might not work in the next. Effective counterinsurgents need to remain flexible and nimble and continuously evaluate how to defend their brand.

The Counterinsurgency Field Manual organizes recommended actions into three categories: Plan, Prepare and Execute. We have taken these actions and condensed them into a seven-step program designed for marketers and brand stewards who are ready to embrace and apply the principles of effective counterinsurgency.

Each of the seven steps is integral to building a resilient brand, but two steps to consider for immediate action are deploying a systematic and scalable process to detect the earliest signs of brand sabotage (Step 3) and systematically harvesting

Figure 2: Brand resilience framework



learnings in the aftermath of brand assaults to be better prepared for the inevitable next time (Step 5).

ENLIST THE VOLUNTEER ARMY IN DETECTING BRAND RISKS

Given the rate at which brand saboteurs invent new tactics and the speed at which news travels across globally-connected social media networks, it is unlikely that any organization can completely predict and pre-empt potential attacks. Nevertheless, a brand risk early warning system can be a powerful weapon in the fight against intentional and unintentional brand sabotage.

The explosive growth of online networks in the past decade has created a vast pool of collaborators who share news and opinions, create content and solve problems for free. We see crowdsourcing at work at news organizations like CNN where we hear not just from CNN reporters, but also from amateur photo journalists via their iReports. Through iReport, anyone with a camera phone can report firsthand from the front line of news. CNN's iReport has more than 753,000 registered "iReporters," and iReporters provided much of the footage of the destructive earthquake and tsunami that hit northeast Japan in March 2011.[7]

The U.S. Geological Survey Twitter Earthquake Detection (USGS TED) Project exploits the willingness of volunteers to provide information for free to benefit others. Using funding from the American Recovery and Reinvestment Act, the USGS:

> . . . is developing a system that gathers real-time, earthquake-related messages from the social networking site Twitter and applies place, time and key word filtering to gather geo-located accounts of shaking. This approach provides rapid first-impression narratives and, potentially, photos from people at the hazard's location. The potential for earthquake detection in populated but sparsely seismically-instrumented regions is also being investigated.[8]

According to USGS Seismologist Paul Earle, "People like to tweet after earthquakes. After an earthquake, they often rapidly report that an earthquake has occurred and describe what they've experienced."[9]

Like CNN's iReport or the USGS TED project, crowdsourcing can be part of a brand's early warning system to create awareness of brand sabotage events as they unfold.

LISTEN CAREFULLY

PepsiCo launched Mission Control in April 2010 as part of a larger effort to kick-start sales of Gatorade, which had been on a 3-year sales slide. According to an article that appeared in *The Wall Street Journal* in September 2010, "PepsiCo is trying to breathe new life into one of its most profitable brands by using Internet services to reconnect with teen athletes who snubbed Gatorade when it became ubiquitous – and uncool."[10]

The facility, located in a glassed-in converted conference room at Gatorade's marketing offices in Chicago, is manned by four full-time employees who continuously track social media posts and "[produce] a consolidated picture of the brand's Internet image."[11]

Mission Control also allows Gatorade to learn more about its customers and get a quick market pulse on new product and promotional ideas without having to rely solely on time-consuming traditional market testing methods. Just by listening, Gatorade is able to "bulk up production of its recovery drinks because of complaints they were selling out" or know "how the new products fare with influential groups" or respond to "Facebook queries such as when to use the new protein drink."[12]

While Gatorade may have been an early adopter, other companies are rapidly establishing their own social media listening platforms. In December of 2010, Dell launched its new Social Media Listening Command Center at its headquarters in Round Rock, Texas. As reported on Mashable, "The center will track on average more than 22,000 daily topic posts related to Dell, as well as mentions of Dell on Twitter. The information can be sliced and diced based on topics and subjects of conversation, sentiment, share of voice, geography and trends."[13] According to the company, "Over 5,000 Dell employees have been trained in social media and many of those are listening and engaging with customers . . . "[14] By monitoring online customer chatter, Dell promotes its brand, engages with its customers by answering their questions, and proactively manages any misinformation about the company and its products.

LINK LISTENING TO ANALYSIS AND ACTION

When it comes to early warning systems, the good news is that help, ranging from free services to customizable solutions, is readily available. There are over 200 tools and platforms in the market for social media monitoring.[15] Services in this nascent market are rapidly evolving from "basic brand monitoring tools to integral technologies that inform campaign measurement, market research, customer support, and sales enablement."[16]

Consider the wide spectrum of available listening tools and platforms for monitoring potential sources of brand sabotage:

Free or low-cost tools such as Google Alerts and social media analytics applications within Google Analytics provide small- and medium-sized businesses with out-of-the-box functionality at no or minimal costs. These tools provide basic social media listening capabilities but put the onus on the user to analyze data and draw insights.

Limited service listening tools are offered by several independent technology companies such as Trackur. These solutions gather and aggregate robust real-time data on online conversations and enable customers to analyze data via dashboards. The vendors provide customers with technical support and training on their suite of tools.

Full service listening platforms and analytics companies such as Radian6, Alterian and Converseon offer their customers the capability to turn information into insights and recommendations via advanced analytics, research methodologies and human review.

Today, many vendors are beginning to differentiate their services by developing scalable platforms that can be deployed across multiple functions and integrated with internal applications (e.g., customer data warehouses). These offer strategic capabilities beyond basic monitoring like building customized enterprise solutions and integrated dashboards, as well as offering capabilities such as customer segmentation, multiple language analyses and human data review.

Not everything that one learns from an early warning system will matter. Understanding "echoes" that come from repeating (or, in the language of Twitter, "retweeting") content, assessing the true influence or clout of the individual launching an assault with a sharply negative comment, and disambiguating nontextual data and colloquial language are important ingredients in going from information to useful insights. This is also an area where advanced analytical capabilities can serve a major role. Equally important, however, is a clear line of sight between the insights harvested from a brand risk early warning system and an effective action plan with well-delineated roles and responsibilities. Absent this clear line of sight, investing in a brand risk early warning system and associated analytical capabilities is unlikely to yield dividends.

NEVER WASTE A CRISIS

In November 2008, Rahm Emanuel, then chief of staff to President-Elect Barack Obama, addressed a *Wall Street Journal* conference of chief executives. The economic situation was, at the time, grim. Emanuel's remarks suggested that the crisis could provide the impetus for action: "You never want a serious crisis to go to waste."[17]

A crisis due to an unexpected attack on a brand can be equally galvanizing. Assume that a company has a brand risk early warning system in place, with responsibility for tracking online brand chatter assigned, analytics produced and conversations with influencers and skeptics initiated. The company would seem to be ahead of the game. But saboteurs will likely evade even well-designed early warning systems and breach robust defenses. Each time this happens, the opportunity to learn from the attack and adapt behaviors presents itself. Brand stewards need to make sure that an organization does not succumb to its natural temptation to simply respond, fix and move on.

Examining what really happened is fundamental to improving brand risk management skills. Once again, we can take a page from the playbook of a federal agency, in this case the National Transportation and Safety Board (NTSB).

The NTSB is an independent United States federal agency responsible for investigating transportation accidents and "[issuing] safety recommendations intended to prevent future accidents."[18] With the assistance of a 24-hour communications center at its Washington, D.C. headquarters, the NTSB monitors global news events, allowing it to quickly respond and deploy a "Go Team" to the

Figure 3: NTSB approach to accident investigations

LESSONS LEARNED FROM THE NATIONAL TRANSPORTATION SAFETY BOARD'S APPROACH TO "LEARN AND ADAPT"

1. **Be prepared:** Practice makes perfect. If the first time you react to a crisis is at the moment the crisis occurs, you are already too late.
2. **Be organized and be available:** Expect the worst and hope for the best, and be ready to react to any situation. Have contingencies in place in case key players are not accessible.
3. **Have experienced leadership**: Have the appropriate resources at hand who have prior experience with crisis management and understand exactly what to do and how to lead.
4. **Monitor and assess:** Listen for changes among employees, competitors and customers, and proactively monitor what is being said about your organization.
5. **React quickly:** Take the time to understand the situation, but respond quickly and efficiently.
6. **Debrief a crisis:** Internalize and review what happened, and apply your learnings to improve future-state tracking and monitoring processes.[19]

As communication has evolved, so too has the NTSB and its ability to respond to crises. According to Jim Hall, former Chairman of the NTSB, there were incidents "in which *The Today Show* (and the 24-hour news networks) was at an accident site before the NTSB was." As a result, Hall led the creation of a 24-hour communications center housed at NTSB headquarters in Washington, D.C. As Hall explains, "The center constantly monitors worldwide events regarding any transportation news and tragedy." This enables the NTSB to learn of accidents and immediately deploy its Go Team to the accident site. The 24-hour communications center handles all logistics for the Go Team, freeing the professional investigators to focus on the investigation.[20]

accident site.[21] A Go Team is a multidisciplinary group of investigators whose job is to systematically unearth facts related to the accident under investigation. The onsite investigation kicks off the first of a four-step process that allows the NTSB to determine the cause of the accident and make recommendations for improving transportation safety.

While most organizations may not be responding to an event as devastating as a major transportation accident, the NTSB approach highlights the importance of thorough "after-action" investigation and analysis as the foundation for continuous learning. As Jim Hall, former chairman of the NTSB, says, "If the first time you are reacting to a crisis is at the moment the crisis occurs, you are already too late. . . . A number of {organizations} are unwilling to make the front-end investments of being prepared, but usually they find that these investments are extremely cost effective."[22]

MAKE RESPONSES TO CRISES VISIBLE TO STAKEHOLDERS, PARTICULARLY CUSTOMERS

On August 28, 2009, a family in San Diego driving a 2009 Lexus ES350 was involved in a fatal car crash. Preliminary investigation pointed toward faulty floor mat installation that may have interfered with the accelerator pedal. Toyota reacted quickly and aggressively to find a fix and restore public confidence. On September 29, 2009, Toyota announced a safety notice for 3.8 million vehicles across seven models. In addition to the millions of recalls that followed, the company decided to halt sales and production for eight models in January 2010. In a report dated February 10, 2010, CNNMoney quoted Toyota USA Group Vice President Bob Carter: "Helping ensure the safety of our customers and restoring confidence in Toyota are very important to our company. This action is necessary until a remedy is finalized." As the company made hard decisions involving car recalls and sales and production stoppages, its engineers were busy finding a technical fix to the underlying problem. In early February 2010, Toyota announced that it had a fix and the required parts were being delivered to dealers. Part of the reason the acceleration problems with Toyota vehicles received the attention that they did was because of Toyota's long track record of manufacturing quality based on its "learn and adapt" approach.[23, 24, 25]

Toyota's costs associated with the recalls have been estimated at $2 billion according to a 2010 CNNMoney report. Despite these costs, Toyota made a strong comeback. In May 2011, *USA Today* reported that "Toyota has regained its position as the world's most valuable auto brand. The value of Toyota's brand increased 11 percent to $24.2 billion, the BrandZ Top 100 annual ranking of the world's most valuable brands finds. In the report, which looks at top brands in every retail category, it is noted that Toyota's unintended acceleration crisis seemed to wash away with the government's finding that the reports couldn't be substantiated. It says that Toyota's comeback shows how strong brands can bounce back." The notion of accident investigation with a focus on identifying the root causes and fixing them works for aviation accidents. It works in manufacturing plants. It works with cars. It works with failures of engineered products. And it can work for brands.[26]

In another example of an organization that has been able to learn and adapt, Facebook deployed the same social media that was used against it to communicate with its customers. Facebook, the product itself and the channel used to discuss product concerns were the same: Facebook. In September 2006, Facebook users took to Facebook to complain about its new product called News Feed that was launched without any market testing. Users feared their friends would now have easy access to their Facebook goings-on as the News Feed aggregated and displayed a user's recent Facebook updates.[27] In a modern-day nonviolent protest, users created Facebook groups, such as "Students Against Facebook News Feed," objecting to the new feature. This prompted Mark Zuckerberg, Facebook's CEO, to address user concerns via his Facebook blog.

Within hours of News Feed being unveiled on September 5, 2006, Zuckerberg posted a blog entitled "Calm down. Breathe. We hear you." Zuckerberg explained that the News Feed feature would stay but welcomed input. "We're going to continue to improve Facebook, and we want you to be part of that process. Test out the products and continue to provide us feedback," Zuckerberg wrote.[28] Three days later, on September 8, Zuckerberg blogged again, beginning, "We really messed this one up."[29] It was a striking display of a leader owning up to a mistake, but more importantly, learning and adapting in order to move forward. In the end, the user outcries only helped improve News Feed and Facebook's privacy settings. As Zuckerberg wrote, "This may sound silly, but I want to thank all of you who have written in and created groups and protested. Even though I wish I hadn't made so many of you angry, I am glad we got to hear you."[30]

Rather than run from its mistake, Facebook was able to learn and adapt and turn moments of brand sabotage into moments that matter by evaluating itself, setting new courses and responding to and reconnecting with customers.

IT'S WHAT YOU DO NEXT THAT COUNTS

We opened with a description of a highly visible incident of brand sabotage – the decline and fall of Tiger Woods as a brand. Perhaps, it makes sense to return to the caption of a once widely distributed ad featuring Woods in the rough. The caption reads, "It's what you do next that counts."

An increase in the incidence of brand sabotage, combined with the fact that brands are becoming more valuable over time, requires organizations to more actively manage brand risk.

While not every brand sabotage event can be prevented, developing a brand risk early warning system is a key step in the fight against brand sabotage. Everyone in the brand ecosystem can play a part, from employees to business partners to customers and even competitors. Brand stewards can begin by building or buying a listening platform that tracks brand chatter and then listening and linking what they hear to a clear set of actions.

Fostering an enterprisewide culture of "learn and adapt" provides additional protection for brands against unanticipated attacks. Brand attacks that make it past early warning systems and strong defenses can provide companies with the opportunity to "go to school" and incorporate what they learn into the next generation of brand defenses. Often this requires evaluating what went wrong (and what can be improved) from the customer's perspective.

Among the developments we expect to see on the rise:

- Integration of traditional and social media monitoring into existing enterprise resource management systems and risk management processes
- Use of advanced analytics to predict potential brand risks and proactively manage these risks
- Incorporation of brand risk management into an overall risk management framework
- Improved training for employees on brand risks and their role in reducing the likelihood of brand risks
- Better tracking of brand risk and brand value metrics, including incorporating these metrics in management and external reporting

The battle between insurgent brand saboteurs and counterinsurgent brand stewards will probably only intensify in the coming years. But constructing brand defenses today may well help determine how resilient a brand will be tomorrow. DR

__Jonathan Copulsky__ is a principal with Deloitte Consulting LLP in the Strategy & Operations practice and author of Brand Resilience: Managing Risk and Recovery in a High Speed World (Palgrave Macmillan, 2011).

__Alicechandra Fritz__ is a senior manager in the Strategy & Operations practice of Deloitte Consulting LLP.

__Mark White__ is a principal with Deloitte Consulting LLP in the Technology Strategy and Architecture practice. He is the chief technology officer of Deloitte Consulting LLP's Technology practice.

The authors gratefully acknowledge __Manik Gupta__ of Deloitte Consulting LLP and __Jeffrey Samotny__ for their contributions to this article.

Endnotes

1. Frank Rich, "Tiger Woods, Person of the Year," *The New York Times*, December 19, 2009, http://www.nytimes.com/2009/12/20/opinion/20rich.html.
2. Ken Belson and Richard Sandomir, "Insuring Endorsements Against Athletes' Scandals," *The New York Times*, January 31, 2011, http://www.nytimes.com/2010/02/01/sports/01insurance.html.
3. BrandZ, "Top 100 Most Valuable Global Brands 2010," Millward Brown website, http://www.millwardbrown.com/Libraries/Optimor_BrandZ_Files/2010_BrandZ_Top100_Report.sflb.ashx.
4. Ibid.
5. 2010 Edelman Trust Barometer Executive Summary, page 4, http://www.scribd.com/full/26268655?access_key=key-1ovbgbpawooot3hnsz3u.
6. This article references *The Counterinsurgency Field Manual*, also known as FM 3-24 and MCWP 3-33.5. FM 3-24 was released by the Department of the Army in December 2006 and is publicly available at http://www.fas.org/irp/doddir/army/fm3-24.pdf. The document is approved for public release, with unlimited distribution. FM 3-24 is also available in a printed and bound edition for purchase through the University of Chicago Press at http://www.press. uchicago.edu/presssite/metadata.epl?mode=synopsis&bookkey=263154. The University of Chicago Press edition of FM 3-24 includes additional materials, and the University of Chicago Press has agreed to donate a portion of the proceeds from this book to the Fisher House Foundation, a private-public partnership that supports the families of America's injured servicemen. All quotes from FM 3-24 that are used in this article are taken from the publicly available downloadable version.
7. "The Future of User Generated Content? CNN, iReport and Open Story," Generated by Users website, March 28, 2011, http://generatedbyusers.wordpress.com/2011/03/28/the-future-of-user-generated-content-cnn-ireport-and-open-story/.
8. "U.S. Geological Survey: Twitter Earthquake Detector (TED)," Department of Interior Recovery Investments website, September 9, 2010, http://recovery.doi.gov/press/us-geological-survey-twitter-earthquake-detector-ted/.
9. Timothy Hurst, "USGS Develops Twitter-Based Earthquake Detection System," *Ecopolitology*, January 7, 2010, http://ecopolitology.org/2010/01/07/usgs-develops-twitter-based-earthquake-detection-system/.
10. Valerie Bauerlein, "Gatorade's 'Mission': Sell More Drinks," *The Wall Street Journal*, September 13, 2010, http://online.wsj.com/article/SB10001424052748703466704575489673244784924.html.
11. Ibid.
12. Ibid.
13. Barton George, "Dell Opens its Social Media Command Center," Dell Inside Enterprise IT blog, December 16, 2010, http://en.community.dell.com/dell-blogs/enterprise/b/inside-enterprise-it/archive/2010/12/16/dell-opens-its-social-media-command-center.aspx.
14. Lionel Menchaca, "Dell's Next Step: The Social Media Listening Command Center," Dell Direct2Dell blog, December 8, 2010, http://en.community.dell.com/dell-blogs/Direct2Dell/b/direct2dell/archive/2010/12/08/dell-s-next-step-the-social-media-listening-command-center.aspx.
15. J.D. Lasica and Kim Bale, "Top 20 Social Media Monitoring Vendors for Business," Socialmedia.biz website, January 12, 2011, http://www.socialmedia.biz/2011/01/12/top-20-social-media-monitoring-vendors-for-business/.
16. Zach Hofer-Shall, Suresh Vittal, Emily Murphy, and Michael J. Grant, "The Forrester Wave™: Listening Platforms, Q3 2010, Converseon, Nielsen, and Radian6 Lead A Fragmented Market," July 12, 2010.
17. http://online.wsj.com/article/SB122721278056345271.html
18. "About the NTSB: History and Mission," National Transportation Safety Board website, http://www.ntsb.gov/abt_ntsb/history.htm.
19. Deloitte Consulting LLP interview with Jim Hall, former chairman of the National Transportation Safety Board, March 21, 2011.
20. Ibid.
21. Ibid.
22. Ibid.
23. CNNMoney, http://money.cnn.com/authos/storysupplement/toyota_timeline/
24. CNNMoney, September 29, 2009, http://money.cnn.com/2009/09/29/new/companies/toytota_lexus_floor)mats/index.htm
25. CNNMoney, January 26, 2010, http://money.cnn.com/2010/01/26/news/companies/toyota_recall/index.htm
26. *USA Today*, May 10, 201, http://content.usatoday.com/communities/driveon/post/2011/05/toyota-bounces-back-as-worlds-most-valuable-auto-brand/1
27. Sarah Lacy, "Facebook Learns from Its Fumble," *Bloomberg Businessweek*, September 8, 2006, http://www.businessweek.com/technology/content/sep2006/tc20060908_536553.htm.
28. Mark Zuckerberg, "Calm down. Breathe. We hear you," Facebook blog, September 5, 2006, http://www.facebook.com/blog.php?post=2208197130.
29. Mark Zuckerberg, "An Open Letter from Mark Zuckerberg," Facebook blog, September 8, 2006, http://blog.facebook.com/blog.php?post=2208562130.
30. Ibid.