ILLUSTRATION: EDMON DE HARO

Overnight, your information security team discovered unauthorized access to sensitive files. Early this morning, your technology team confirmed some file IDs have been changed and cannot be accessed. Both teams propose taking the network offline until they can find the root cause. This means your people can't work and your customers can't use your services, potentially for days.

You don't know how much information has been accessed, what has been done with it, who has it or for how long. You do know that you cannot serve your customers and, if their accounts have been compromised, their businesses could also be at risk.

This is now your job for the foreseeable future. Good morning.

Blame Game

Your company is now in the spotlight. Rightly or wrongly, in the case of a cyber incident, the brunt of the blame falls on the victim of the attack – not the perpetrator. In a Brunswick Insight survey, financial media readers in the UK indicated that they're well aware of the usual suspects who carry out these attacks. Nearly nine in 10 respondents recognize serious threats from nation-state actors, global terror groups and individual criminals. Even so, nearly half (47 percent) say they'd blame the business that fell victim to the attack, compared to just 32 percent who would blame the perpetrator (Chart 1 on next page).

Companies not meeting expectations of preparedness are the biggest target for blame. In our survey, 83 percent say they're concerned services they rely on will be disrupted (Chart 2); just 53 percent say they're confident those businesses can prevent an attack. Only 10 percent say they're very confident.

Cyber attack headlines are now part of our daily newsfeed. Perhaps we are more accepting of the idea that our personal data has been breached, and we know we bear some of the responsibility to watch out for fraud. But we still expect companies to take all the right steps, mainly because:

You should have seen this coming. "When, not if" has long been a stark warning from cyber experts and regulators.

You should have been better prepared. Despite growing awareness that business can be brought to a standstill, adequate steps are rarely taken in advance.

Don't let the discovery of a **CYBER BREACH** be the first time you've thought about how you will handle it, say Brunswick crisis and cyber specialist **WENDEL VERBEEK** and Brunswick Insight's **JEREMY RUCH.**

It Matters

These events have consequences for leadership, employees, customers, partners and investors. Each

expects that the appropriate steps are being taken by the others to protect the company and sensitive information. But do they all understand the potential financial and reputational consequences?

Regulatory repercussions. The General Data Protection Regulation took effect in May of 2018. We don't know yet what fines for the worst offenders will be, but they could amount to 4 percent of global turnover. The regulator could also force companies to suspend business if they aren't satisfied the proper steps to protect data have been taken.

Loss of business. The June 2017 NotPetya attack aimed at the Ukraine caused material sales impacts for a number of global companies. They were simply collateral damage, the result of perhaps even just one user clicking on malicious links. Maersk has used the experience to warn others. They reported $265 million lost sales in a quarter following a 10-day period where the company was reduced to pen and paper while it reinstalled all of its IT systems.

Share price impact. Breached companies see immediate share price impact and underperform the market in the long term. An analysis by Comparitech of 28 breaches showed that these companies underperformed the Nasdaq by 4.6 percent over the first 14 days and by 11.35 percent over two years.

Lost productivity. Responding to cyber attacks weighs on your company's performance. Production loss accounts for one-third of a company's annualized costs due to cyber crime, the 2017 Accenture and Ponemon study found.

Executives are collateral damage. Companies that have suffered major breaches, like Yahoo!, Equifax, Target and Uber, often see the resignations of either their CEO, CISO and/or General Counsel.

Class action lawsuits. These are not limited to the US. We saw a firm threaten a group action suit against British Airways within days of the September 2018 data breach.

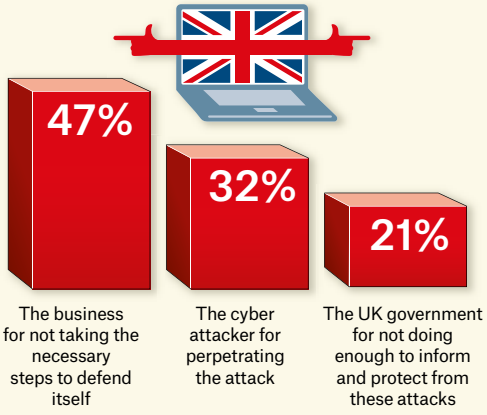
Preparation Pays

This is the seatbelt moment for companies. The expectation is on them to protect their business and any that they work with by thinking now about how to increase cyber reputational resilience. Consider the critical decisions you will be faced with to inform your everyday approach to arming your people, systems and your leadership team:

1. **Align your response team.** Swift coordination in a pressured situation requires a defined decision maker. The CEO needs to know when that decision-making power should sit with her and how the critical details to inform decisions will be shared. When

1. FINGER POINTING

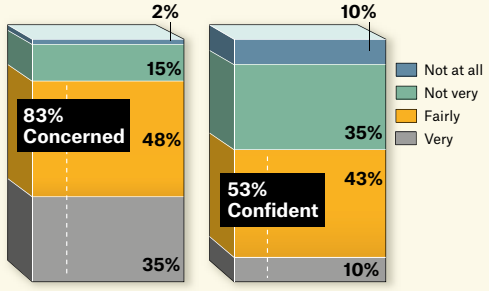
Who would you blame if a business you use here in the UK experienced a cyber attack that resulted in serious inconvenience or disruption for your life?



2. CONCERN VERSUS CONFIDENCE

LEFT, how concerned are you that a business or service you rely on will be disrupted?

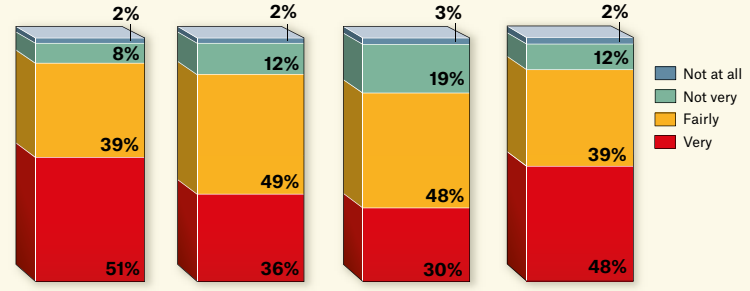
RIGHT, how confident are you in their ability to prevent a cyber attack?



IN THE CASE OF A CYBER INCIDENT, THE BRUNT OF THE BLAME FALLS ON THE VICTIM OF THE ATTACK – NOT THE PERPETRATOR.

3. WHICH GROUPS POSE THE GREATEST THREAT?

Based on your understanding, how serious are the threats posed by cyber attacks from each of the following?



Source: Brunswick Insight

CHARTS: PETER HOEY

facing a business unit incident that affects a global customer base and requires international regulatory alerts, that responsibility can get muddled.

The smoother the public response, the shorter the public follow-up cycle and scrutiny. That only comes with practice.

2. **Consider the tough decisions.** You want to be able to offer your customers something in response to a potentially protracted disruption. The first debate about exactly what that offer will be should not happen under the pressure of a tight deadline. As with any critical decision that could affect your long-term reputation with customers and employees, understand the likelihood of risks and weigh how you could respond.

When would you advise customers of a potential risk? When should you inform the market, given that it may be some time before you have a complete picture? How often should you communicate during the disruption? How will disclosure affect different parts of the business? You have to be prepared to communicate clearly but cautiously and your first communication has to be accurate.

How would issues in different regions drive decisions? Global companies must reconcile the different cultural and geopolitical pressures around the level of information expected in each market when hit with a cyber incident. Which of your markets will guide your response strategy?

How would you respond to extortion? Does your executive team agree how you would respond to threats of extortion? Would you take a public stance around refusing to pay ransom, and is that more effective in your key markets?

3. **Get to grips with the potential consequences.** With the right questions, you can understand where you are most at risk of a cyber incident. That should inform both how much you put toward mitigation of key risks and how you prepare to respond. If a phishing attack could grant access to sensitive IP critical to your business, extra defenses and training are required.

Are those most sensitive systems the first ones your information security team would check at the notice of potential unauthorized access? Do you appreciate the level of complexity involved in understanding what could have been accessed? Where will you need to be prepared to offer compensation and how much?

4. **Increase your IT security literacy.** There is a call to action for boards to increase their understanding of the cyber risks their companies face, and to do that they need to understand their current defenses. This extends to the preparedness of the members of your supply chain.

Earn a Return from Managing Cyber Risk

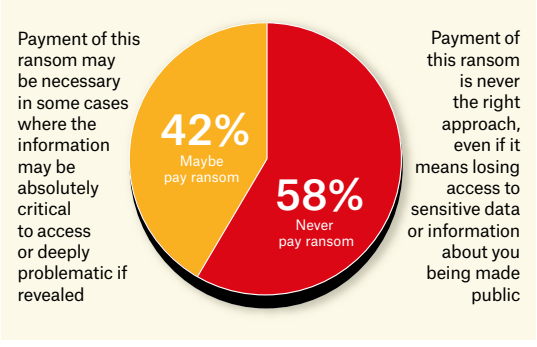
Cyber resilience is not just a matter of risk management. Robust preparation across your business should be value enhancing.

An informed executive team will demand higher standards from everyone in the business. If it is a theme heard from the top, information security will be echoed across the business making it a message your customers and partners hear too. Employees want to be part of a solution and understand the role they play.

Good management appeals to investors. Our survey shows a very positive response to senior executives detailing how they've dealt with ongoing cyber threats and strengthened defenses and preparation.

Cyber attacks can disrupt business and carry long-term consequences. Hackers work full time to get into your system. Advance planning and company-wide cyber awareness can make their job considerably harder. ◆

4. EXTORTION RESPONSE



"WARNING! All your important documents are now encrypted and cannot be unlocked without a unique private decryption key. You have 48 hours to pay $5,000 or your files will be permanently locked."

Messages like this throw millions of people into panic each year. For those who find sensitive business or financial information locked and inaccessible, this is an immediate crisis.

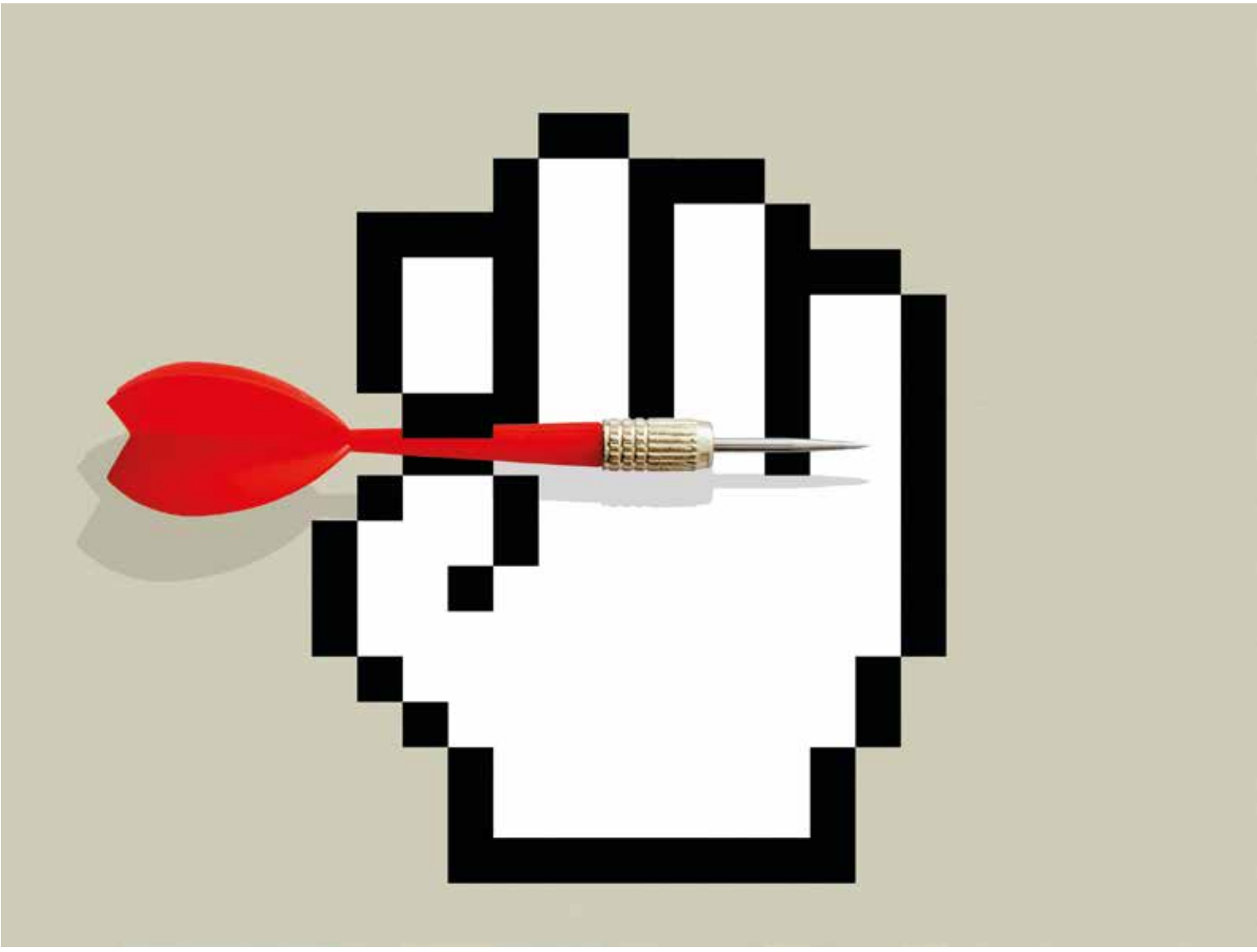
We'd all like to think that cyber attacks and ransomware find victims only among the most unsuspecting and unprepared. And, we all know that paying a ransom is never recommended as it frequently doesn't even give you renewed access to your data.

Or do we? In a survey of 316 UK readers of top-tier financial publications conducted by Brunswick Insight, 42 percent said that paying a ransom may sometimes be necessary when the information is absolutely critical to access, or if it would cause deep problems when revealed.

THE SMOOTHER THE PUBLIC RESPONSE, THE SHORTER THE PUBLIC FOLLOW-UP CYCLE AND SCRUTINY. THAT ONLY COMES WITH PRACTICE.

JEREMY RUCH and **WENDEL VERBEEK** are Brunswick Directors, based in London.

SURVEY: BRUNSWICK INSIGHT research conducted between September 21 to 24, 2018 in the UK among 316 readers of top-tier financial publications.



Much has been made about the rise of fake news – false reports that look like genuine news articles – and the threat it poses to elections and democracy in general. Less well understood is the role disinformation can play in damaging the reputations of private corporations and institutions. Ill-timed disinformation attacks – perhaps around an IPO, key investor meeting, merger or product launch – could result in a significant loss of value.

For example, in April 2016, a clickbait site posing as TV news published false reports that Coca-Cola's bottled water brand Dasani was being recalled because of the presence of a parasite in the water that purportedly caused "several hundred" hospitalizations. As an illustration, standing in for an actual parasite, the hoax story carried a spooky image of a flat and transparent eel larva.

Falsehoods in the marketplace have a long history. What's different now is the ease with which they can spread. True, opinion is protected by free speech rights, but corporations are not defenseless against intentional distortion, especially when used to enrich another party.

We asked WilmerHale Partner Jason Chipman and Senior Associate Matthew F. Ferraro, who are both visiting fellows at the National Security Institute at George Mason University, for their thoughts and insights into what legal options C-suites may consider when faced with a crisis brought about by disinformation attacks.

What kind of threats do businesses face from fake news?

Fake news is just a new way to refer to an old problem of false reports, misinformation, innuendo

ILLUSTRATION: EDMON DE HARO

and smears, all of which can threaten corporations in profound ways. We generally group these threats into three categories. First are individuals motivated by animus, ideology or a simple desire to make trouble. They operate largely independently and do not seek remuneration or ransom but merely the satisfaction of damaging corporate brands they dislike. These actors leverage near-anonymous social media, like 4Chan, to find like-minded confederates and utilize specialized, "news article"-producing websites to target brands with relatively slick content.

TARGET of Disinformation

In August 2017 for example, agitators launched a bogus campaign against Starbucks with tweets advertising "Dreamer Day," that claimed the coffee company's US stores would give out free Frappuccinos to undocumented immigrants. Advertisements, complete with the company's logo, signature font and pictures, raced around the web with the hashtag "#borderfreecoffee." It was all a hoax dreamt up by a rabble-rouser on 4Chan who wanted to inflict pain on what he called a "liberal place."

The second group covers actors who seek some defined benefit by engineering the release of misleading information. These individuals might aim to accrue advertising dollars by pushing traffic to websites or videos. Think salacious, attention-grabbing clickbait headlines that sound too good to be true – because they are. Similarly, false or misleading stories released at the right moment can drive down stock prices and provide opportunities for stock shorts and other financial windfalls.

In October 2018, for example, shares of both Broadcom and CA Technologies briefly plunged after a memo purporting to be from the US Department of Defense appeared, which said that the Committee on Foreign Investment in the United States (commonly known as CFIUS) would review Broadcom's $19 billion acquisition of CA Technologies. But according to press accounts, the memo was a forgery. Neither the DoD nor CFIUS were reviewing the deal. It is not clear who authored the phony document, but short sellers would have profited handsomely from the dip.

The third group includes state-backed actors. While we have seen no public evidence of them targeting private companies with fake news, it may be only a matter of time. One can easily imagine foreign cyber operations targeting the reputation of American companies with disinformation campaigns that seek to damage their brands and drive business to a foreign country's national champion.

Going forward, it will be critical for corporations to know how to navigate a world in which deceptive "news" stories propagated by all of these actors can race around the world at the speed of light, threatening reputations and revenue streams.

WilmerHale attorneys **JASON CHIPMAN** and **MATTHEW F. FERRARO** talk fake news attacks and the law with Brunswick's **PRESTON GOLSON.**

Have there been any digital disinformation cases where bad actors have been found or convicted?
This is a relatively new phenomenon with no obvious examples where purveyors of "fake news" were held liable for false reports. But trafficking in innuendo and libel is an ancient vice and current laws provide significant protection and well-established causes of action that can likely be employed. It is just a matter of applying proven strategies to new contexts. Consider the potential applicability of the following causes of action, among others.

Defamation and Trade Libel. There are many cases where courts have sustained claims for defamation against people who post smears on customer review websites. The same logic would apply to people who manufacture genuine-looking news articles that are just dressed-up libel. False statements denigrating the quality of a company's goods or services may also give rise to a claim for another tort known variably as trade libel, injurious falsehood or product disparagement. These torts are broader than pure defamation because they are not typically confined to false statements that damage a company's reputation.

Economic and Equitable Torts. State laws protect against malicious and dishonest interference in another party's future business relationships, which is essentially what fake news targeted at corporations

does. For example, the "Dreamer Day" hoax was intended to harm Starbucks' business with third-party patrons of their stores. Similarly claims for deceptive trade practices and unjust enrichment could also likely be made against unscrupulous short sellers who rely on fake news to drive down stock prices.

Intellectual Property Law. Federal trademark infringement laws could provide a cause of action against anyone who posts a fake news item which incorporates a company logo to make an "article" or post look genuine, because the poster would be using a trademark in a manner that would be likely to cause confusion among consumers.

The purveyors of disinformation are often overseas. Does international law offer any recourse for businesses?

This is a global problem, and that poses a hurdle to successful suits in US courts, but it can be surmounted, depending on the facts of the case. Furthermore, many countries have protections similar to those found in US law.

When is suing or seeking law enforcement action useful to counteract disinformation?

This is an important question that each client must answer for itself. It's important to consider remedies short of litigation, as well. For example, engaging with web-hosting platforms may reveal potential remedies to limit the damage from false stories. Where litigation is being considered, key issues to evaluate include:

1. **Jurisdiction.** Does the hoaxer reside in the US or have sufficient contacts with the country to establish jurisdiction?
2. **Ability to pay.** Is the defendant judgment proof? Do they have any funds to pay a civil award if they are found liable?
3. **Time and expense.** Litigation can be expensive and slow. A client will need to consider whether the effort is worth it in time and money.

On the other hand, litigation not only can vindicate a corporation's rights but also deter other malefactors from similar behavior, bring to light valuable information about opponents, or expose wrongdoing to the press and the marketplace. Businesses will want to consider the facts of each situation and confer with outside counsel before making any moves.

Are there other ways corporations or institutions could respond to digital disinformation?

Fake news poses a serious threat to the integrity of corporate brands and their bottom lines. Like other new phenomena, such as cyber hacking and ransomware, corporations should not wait for the worst to happen before taking proactive steps. We recommend three broad strategies to defend against digital disinformation.

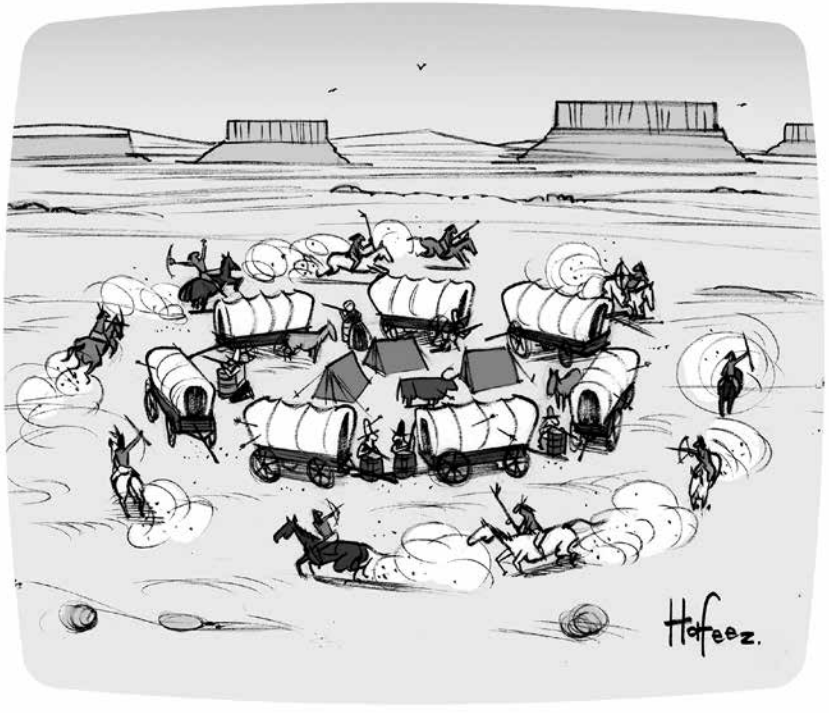
First, prepare. Increasingly, companies prepare for cybersecurity breaches through planning and table-top exercises. In the same vein, now is the time to game-out how a company will handle a fake-news attack. Assign roles to in-house talent who will lead in a crisis. Identify third-party validators who will vouch for the brand. Establish a brand presence on all major social media platforms, from Facebook and Twitter, to Instagram and Snapchat.

Second, proactively engage in the new media environment. Do not be caught flatfooted when an anonymous Twitter troll's misinformation reaches traditional media outlets. Stay attuned to what is being said about you and your brand. Communicate with your customers, business partners, employees and suppliers. Build trust so they know to whom to turn with questions about what's true and fake.

Third, speak for yourself. Be prepared to talk directly to customers and the public at large to debunk fakery. In this context, the solution to bad speech is more direct and credible speech. ◆

"DO NOT BE CAUGHT FLATFOOTED WHEN AN ANONYMOUS TWITTER TROLL'S MISINFORMATION REACHES TRADITIONAL MEDIA OUTLETS."

PRESTON GOLSON is a Brunswick Director based in Washington, DC. He is a former CIA spokesperson.



*"**We** know the cavalry aren't coming, but if we announce it on Twitter, they'll probably **think** the cavalry are coming."*

ILLUSTRATION: KAAMRAN HAFEEZ