BUONGIORNO!
NICE TO
MEET YOU!

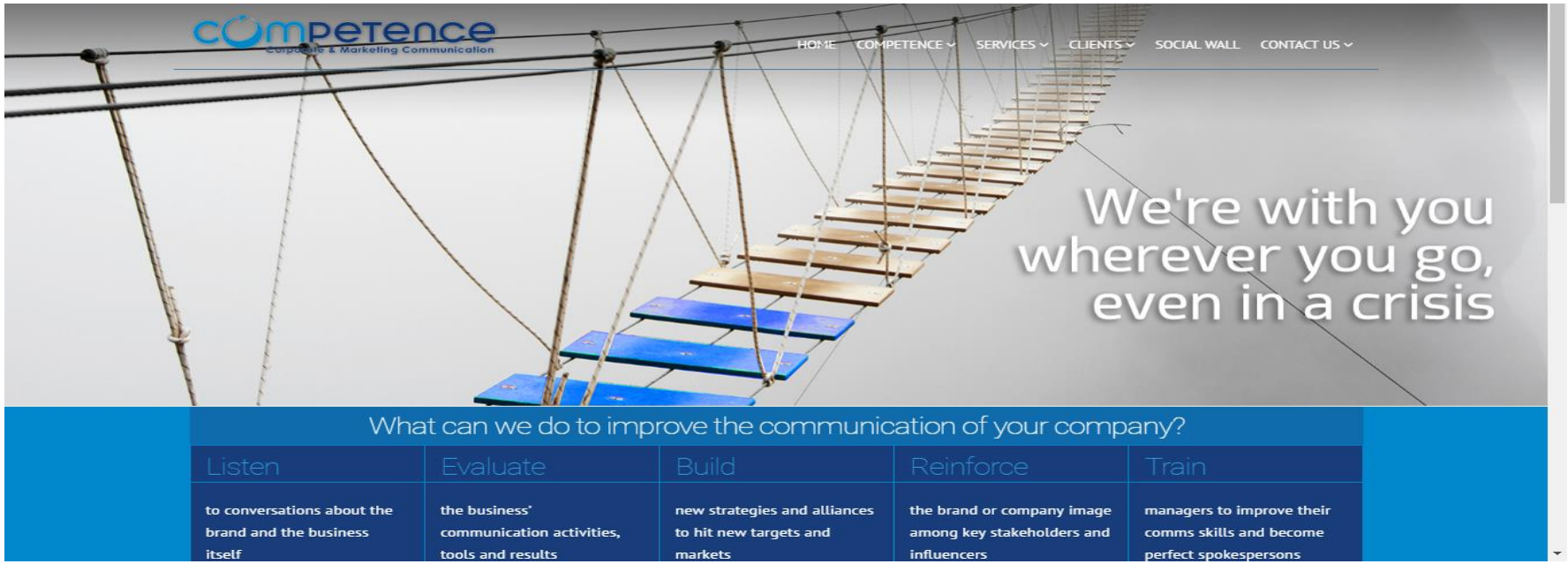
Lorenzo Brufani

Competence CEO - Social Media Crisis, Digital PR, Media Relations,Reputation Management, Online Intelligence, Trainings

Milano, Italia | Pubbliche relazioni e comunicazioni

Attuale	LUISS Business School, Competence Communication, Il Sole 24 ORE Business School ed Eventi
Precedente	LinkedIn, Borsa Italiana, Cohn & Wolfe
Formazione	LUISS Guido Carli University

https://www.linkedin.com/in/lorenzobrufani



http://www.competencecommunication.com/en/

competence
Corporate & Marketing Communication

A COMM PLAN CAN NOT AVOID A CYBER ATTACK BUT IT COULD HELP ANY ORGANIZATION TO TURN THIS ISSUE INTO A BRAND OPPORTUNITY

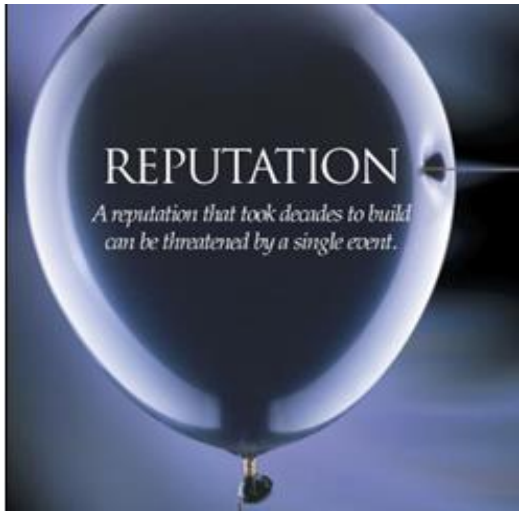
Did you know?

33% of clients declared to have **more TRUST** in hacked company that immediately and directly alerted them on a data breach.

94% of Customers consider today **TRUST more important than CONVENIENCE**. Deloitte's 2016 Privacy Index

CBS.com notes that **1.5 million cyberattacks** occur every year, which translates to over **4,000 attacks every day**, 170 every hour, or nearly **three every minute**. While few attacks succeed, the high probability of cyber incidents dictates that every organization **needs to be prepared** to respond effectively.

Traditionally the main responsibility and focus on a Cyber Attack are linked to IT & Legal Dept and there is a **LACK OF ATTENTION on Internal & External Communications Team strategic role**.



"It takes 20 years to build a reputation, and 5 minutes to ruin it" -Warren Buffet

COMPETENCE
Corporate & Marketing Communication

THE 10 NEW RULES OF CRISIS COMMUNICATIONS

By Melissa Agnes

1

Communications are now a **two-way** street, whether you want them to be or not.

Real-time is not just a suggestion but an expectation of your audience - an expectation that will not turn in your favor if unmet.

2

3

Being **Informative** is the only way. If you're not informative somebody else will be – on a channel that your organization has zero control over.

Listen, listen, listen! Listen to what others are saying and publishing, to what they're not saying, and where they are and are not saying it.

4

5

When you properly combine real-time and two-way you get responsive. Your audience will be responsive and so must you.

Sincerity, honesty and meaningful apologies go a long way. But remember: actions speak so much louder than words. You have to say what you mean and prove it.

6

7

Humans dealing with humans. Forget the corporate and legal talk. Forget hiding behind a logo. Your audience expects to hear from the humans behind the brand.

Adaptability and **flexibility** need to be incorporated into your corporate culture - not to mention your crisis communications strategy. The digital landscape changes often and quickly. Staying stagnant will leave you vulnerable.

8

9

Twitter is the social media platform that dominates the dissemination of news and information in a crisis. Making your crisis communications Twitter-friendly is essential.

Internal communications are key to today's successful crisis management. Point final.

10

DATA BREACH & CRISIS: IT IS VITAL TO START PREPARING BEFORE!

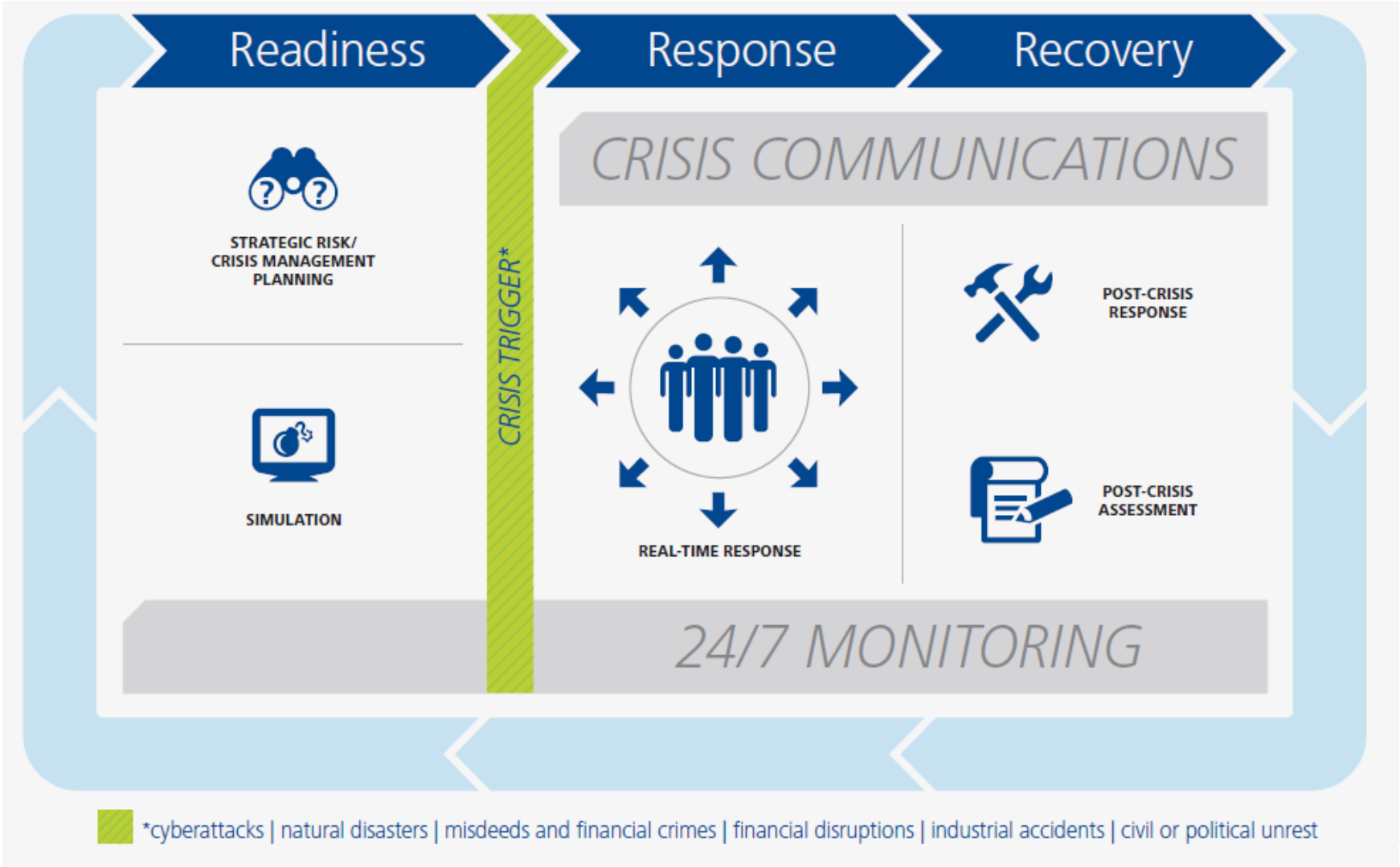
The traditional communication approach is the typical "***Let's cross our fingers and we will see…"*** with no strategy and no crisis tools.

A good crisis communication plan can be designed and tested NOT during the cyber attack but it must be **prepared BEFORE** and adjusted when our company is working in ordinary and safe business conditions.

We need **CRISIS-READY CULTURE**.

competence
Corporate & Marketing Communication

DELOITTE'S CRISIS MANAGEMENT LIFECYCLE



4 STEPS FOR RESPONDING TO A DATA BREACH OR HACK

Step 1: Right Here - Right Now

While IT & Security teams are working on containing and securing the breach, crisis communications team's first and most important priority is to **communicate directly & ASAP with your affected stakeholders**.

✓ Be honest and to the point

Show **remorse and** how deeply you care and are taking the situation seriously.

✓ Be Pragmatic and Time-focused

Clearly communicate how this breach affects those impacted, what they should do to immediately protect themselves and where/when you will provide them with another update.

✓ Relation Management is the Key

Focus on maintaining and even strengthening your relationships with these stakeholders. They have every right to be pissed and worried but if you focus on your relationship and being transparent & empathetic, they may just forgive you.

4 STEPS FOR RESPONDING TO A DATA BREACH OR HACK

Step 2: Official Statement/Stand-By Positioning

If we know that this breach is going to create headlines we have to draft an official statement and **publish it in our crisis communications home base.**

- ✓ Make sure you have a mention of the hack and a **link to this statement** from your website's homepage (or a banner)
- ✓ Don't make people go searching for your comms, **make it easy** for them to find. **Update** this statement as more questions get answered.
- ✓ If the media will be reporting it, **let's give journos the true story** to use.
- ✓ Be **transparent** and focus on strengthening your media relationships
- ✓ Clearly state **repercussions**, what you have done and what you will do
- ✓ Create **an intuitive title** that will rank well for the keywords people will use to search for more information on this data breach.
- ✓ Evaluate to include a **video apology** from Top manager/CEO
- ✓ Provide a specific contact for media inquiries (**Social Crisis Expert**).

Step 3: Make sure your Social Media Team is ready

You will have **to link/pin your official statement** from your social media accounts and **monitor 24/7 social media local/national** scenario as well.

Your Social Media Team needs to be armed with:

- ✓ **Clear messaging** for proper response.
- ✓ Information on **where to send inquiries** that need to be redirected.
- ✓ A **response flow chart** that will help SMT answer the tough questions, such as when to respond, when to sit back and when to escalate a specific case to the crisis team.
- ✓ Your SMT will also have the task of monitoring social media to identify **rumors and speculation** and to gauge the overall brand sentiment.

4 STEPS FOR RESPONDING TO A DATA BREACH OR HACK

Step 4: Keep an eye on your Online Reputation

Articles will be indexed in the search engines, so you will want to:

- ✓ Make sure that your communications are **helping to shape** the narrative of this crisis in as much of a positive way as possible.
- ✓ Basically what we want is to **be recognized** for our quick, compassionate response and our brilliant crisis management skills.
- ✓ Do what you can to make sure that these **ranked articles are not going to overpower** your own online presence and rankings
- ✓ Do an **online vulnerability audit** and a proactive On Line Reputation management with **SEO and Digital PR actions**.

BUFFER: A BEST PRACTICE ON DATA BREACH CRISIS MANAGEMENT

Buffer, social media pre-scheduling app, was hacked on October 23 2013.

All Buffer users received **immediately and directly in their inbox a message** on the hack before they even had the chance to discover the situation.

What made Buffer's crisis communications such a success?

- ✓ They **weren't scared** to get ahead of the story, making sure that their customers heard the details of the situation **from them** before they heard it from any other source
- ✓ They expressed **true concern, care and sincerity** – and were completely human
- ✓ They **proved** that they were taking the situation seriously.
- ✓ They kept their **audiences updated on the situation**, **in real-time**, from their corporate blog as well as from their social media platforms
- ✓ Once the situation was resolved, they **heightened their security measures** so as to protect the situation from happening again
- ✓ They provided **updates and promised even more updates** in the near future
- ✓ They **welcomed feedback** – which made their crisis communications two-way

As a result, their users trust and feel connected to the brand **in a more positive way than they did before the hacking occurred.**

https://open.buffer.com/buffer-has-been-hacked-here-is-whats-going-on/

BUFFER CEO EMAIL SENT DIRECTLY TO ALL USERS AFFECTED

"Hi there,

I wanted to get in touch to apologize for the awful experience we've caused many of you on your weekend. Buffer was hacked around 1 hour ago, and many of you may have experienced spam posts sent from you via Buffer. I can only understand how angry and disappointed you must be right now.

Not everyone who has signed up for Buffer has been affected, but you may want to check on your accounts. We're working hard to fix this problem right now and we're expecting to have everything back to normal shortly.

We're posting continual updates on the Buffer Facebook page and the Buffer Twitter page to keep you in the loop on everything. The best steps for you to take right now and important information for you:

Remove any postings from your Facebook page or Twitter page that look like spam

Keep an eye on Buffer's Twitter page and Facebook page

Your Buffer passwords are not affected

No billing or payment information was affected or exposed

All Facebook posts sent via Buffer have been temporarily hidden and will reappear once we've resolved this situation

I am incredibly sorry this has happened and affected you and your company. We're working around the clock right now to get this resolved and we'll continue to post updates on Facebook and Twitter.

If you have any questions at all, please respond to this email. Understandably, a lot of people have emailed us, so we might take a short while to get back to everyone, but we will respond to every single email.

– Joel and the Buffer team"

SEX DATA BREACH: HUGE DAMAGE TO MANY HUSBANDS REPUTATION

https://techcrunch.com/2015/08/19/ashley-madison-data-dumped/

competence
Corporate & Marketing Communication

BEFORE CLOSING…PLEASE REMEMBER 5 TIPS ON CRISIS

There’s no substitute for preparedness

Wargaming, rehearsals, and other structured preparations do much to position the organization to launch a coordinated response.

Every decision counts

In a crisis every decision can affect stakeholder value mainly through heightened reputational risks, which can destroy value faster than operational risks.

Response times should be in minutes

Teams on the ground must respond rapidly, not in 24 hours or days. They must take control, lead with flexibility, act on incomplete information and inspire confidence.

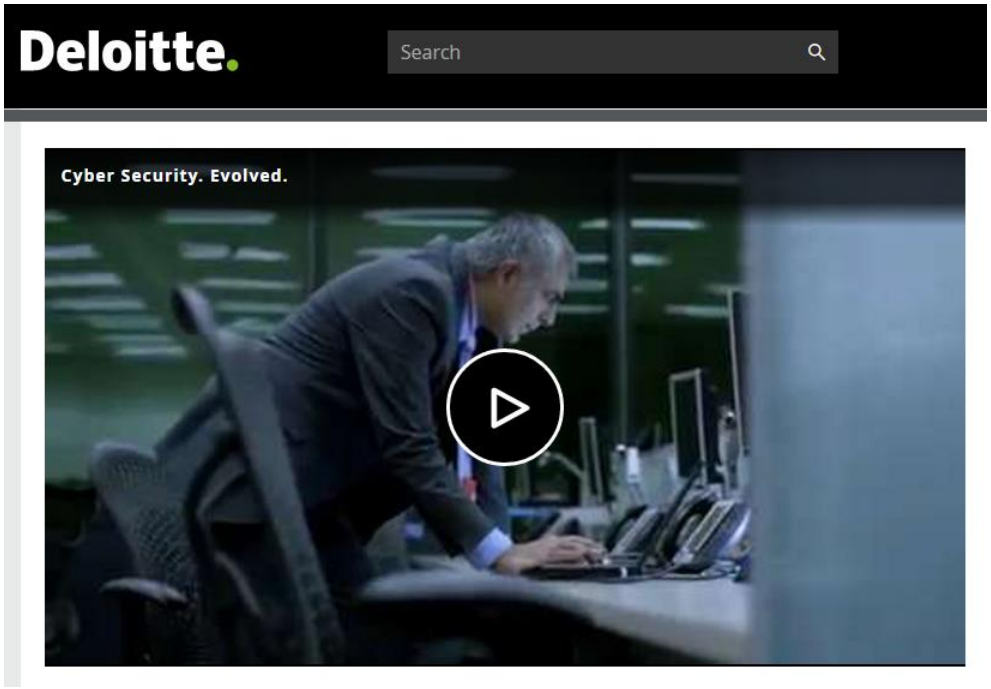
When the crisis has passed, work remains

After breathing a sigh of relief, you must capture data, log decisions, manage finances, handle insurance claims, and meet legal and regulatory requirements.

You can emerge stronger

Almost every crisis creates opportunities for an organization to shine, first, by responding effectively and, second, by searching out opportunities to improve.

THANK YOU FOR YOUR ATTENTION!



https://www2.deloitte.com/global/en/pages/risk/topics/cybersecurity.html#

competence
Corporate & Marketing Communication