Preventing Social Media Armageddon

The accessibility and fluidity of social media leaves organisations open to significant risks. But there are countermeasures organisations can take to prevent reputation disaster.

President Obama has been injured in a terrorist attack on the White House. A Tweet released by the Associated Press (AP) attests to this. It carries the company's "verified" stamp of authenticity. The S&P 500 just lost more than $130 bn. Well, not quite.

The AP's Tweet was the by-product of a computer hack by the "Syrian Electronic Army" and naturally the US president was never injured. AP quickly took its feed down and immediately notified its subscribers of the problem. The market recovered but AP's reputation as a reliable supplier of real time news **was damaged**. Social media are now ubiquitous in the corporate world and in our day-to-day life but the risks they carry are not fully understood yet.

Four threats

There are four main threats they pose.

Fragging: employees can intentionally try to **harm their employer's reputation**. Take the case of HMV, the global entertainment retailer with more than $1.5 billion in annual revenue. In 2013, its Twitter feed suddenly turned bizarre. A message read "We're tweeting live from HR where we're all being fired! Exciting!! #hmvXFactorFiring". The social media team had been downsized and the 21 year old in control of the account had a field day, airing the company's dirty laundry in public. By the time the company regained control of its Twitter account and deleted the messages, they had already gone viral.

Leaking: Employees can also unintentionally hurt their employer. This can happen when they release information that is directly useful to adversaries. For example, information about your CFO vacation or IT procedures can also facilitate fraud by giving valuable operational information. Geotagging of pictures is particularly useful to understand executive travel patterns. An Al Qaeda manual recovered by the British police revealed that 80 percent of the information the organisation seeks to conduct its attacks is available from public sources. A different risk occurs when employees and other stakeholders engage in activities that are damaging to the organisation's reputation in their private time. Take the case of the university engineering professor who wrote a book denying the Holocaust. His departmental webpage, although not advertising his political view, is still online and not the best online advert for his employer (the university had to issue a statement to publicly distance itself from the individual).

Hacking: Non-employees can intentionally hurt an organisation and the AP example is not unique. For example, French television broadcaster TV5 Monde

was **recently the target** of a cyberattack that took down its 11 television channels, website, and social media streams. However, the threat from outsiders is not limited to the cyber world. Spouses commenting on forums or posting pictures to share their frustrations about the company can be problematic. A few months ago, AOL CEO Tim Armstrong mentioned that the company had paid "a million dollars" in medical costs to employees who were the parents of "distressed babies". One of the mothers, the wife of an AOL employee, became incensed at what she perceived to be a breach of her privacy. She launched a PR campaign that started with an interview in the online magazine, Slate. Armstrong had to apologise.

Fumbling: Non-employees can also harm reputations unintentionally. In 2008, the Italian tax authority made **income data available online** by accident and hurt a few individual reputations. A related situation occurs when someone want to create buzz by releasing a controversial information. The goal is not to hurt anyone, even though this consequence may be easily foreseeable. A senior Uber executive suggested at a dinner that the company should hire opposition researchers to pressure critics in the media. A buzzfeed editor was present and, since no one had informed him that the event was off the record, he released the information online. This again ended up in a public apology from the executive.

Counter measures

To address this risk, we offer a four pronged approach.

Mark: Threats need to be identified and linked to your general risk management processes. The different accounts should be identified and their ownership clearly established.

Measure: The risk materiality should be ascertained. For example, armed forces classify the degree of confidentiality associated with each document they produce (from freely available to a general audience to highly classified). This systematic approach is designed to reduce the risk that operations security is inadvertently compromised.

Manage: The best way to deal with a social media crisis **is to prevent it**. A natural response may be to impose additional layers of control but naturally there is a trade-off between reactivity (the point of having a social media activity) and security. This may lead the firm to tolerate a certain degree of risk. Risks can also be treated to minimise their occurrences or their consequences. For example, embedded social media correspondents can be deployed through the organisation to diffuse good practices and to provide a better picture of real company practices to risk managers. An **"outboarding" programme** can be designed to ensure that employees leaving the company are leaving on good terms. The risks can also be transferred either by outsourcing the social media activity to an external provider (and the responsibility that goes with it) or by purchasing insurance in case something goes wrong. In rare cases, the risks can be terminated by closing down the social media channels entirely. This option may be worth considering for small organisations but is unlikely to be possible for larger ones.

Monitor: Detecting emerging crises in matters of minutes can be critical as the AP case has shown. A quick response may even turn a **problem into an opportunity**. Interestingly, monitoring social media can also help you to detect a crisis in another part of your business. For example, companies such as Deutsche Telekom have deployed a technology in their "Situation Room" that can monitor social media activity around their company. This allows these organisations to detect emerging operational or IT issues as soon as they impact their customers.

Once these challenges have been better understood, a crucial question becomes who in the organisation is best positioned to take charge of them. Chief Marketing Officer, Chief Risk Officer, Chief Information Officer or a new type of executive (Chief Digital Officer) can all lay a claim on this. What is clear though is that, irrespective of your position in the leadership team, your reputation is at stake.

Gilles Hilary *is The Mubdala Chaired Professor of Corporate Governance and Strategy at INSEAD and a professor of Accounting and Control.*

Varun Mittal *is the Group Head of Partnership & Marketing at helloPay.*