# Managing stakeholder communication during a cyber crisis

Received (in revised form): 13th November, 2020

**Caroline Sapriel**
Managing Partner, CS&A International, Belgium

Caroline Sapriel is the founder and managing partner of CS&A International, a global risk and crisis management consulting company working with multinational clients across industry sectors in Asia, the Middle East and Africa, Europe and the Americas. With over 25 years' experience in risk and crisis management, she is recognised as a leader in her profession and acknowledged for her ability to provide customised, results-driven counsel and training at the highest level. Over the years, Caroline has advised senior leaders across industries internationally. Her multidisciplinary background and experience has enabled her to provide clients with an in-depth analysis of their crisis management capability as well as help them develop effective risk and crisis response organisations and stakeholder and reputation management strategies. She has been directly involved in helping clients manage crises in the oil and gas, chemical, transport, shipping, aviation, pharmaceutical and consumer product sectors. Caroline is an accomplished trainer, facilitator and coach in risk issues and crisis management as well as in communication skills, and a regular speaker on risk and crisis management at international conferences. She has published articles and co-authored two books on crisis management as well as contributed the chapter on crisis communication to the International Association of Business Communicators' *Handbook of Organizational Communication*. She is a lecturer on crisis management at the University of Antwerp and the University of Leuven in Belgium as well as the University of Leiden in the Netherlands. Caroline is fluent in French, English, Spanish, Hebrew and Mandarin. She holds a BA degree in Chinese studies and a BSc degree in international relations from the Hebrew University of Jerusalem.

CS&A International, Nonnenstraat 40, 2800 Mechelen, Belgium
Tel: +32-486510526; E-mail: caroline.sapriel@csa-crisis.com

**Abstract** The paper examines the impact of stakeholders during cyber crises and how failing to engage with them can quickly escalate a crisis into a reputation train wreck. While organisations must focus their efforts on preventing and mitigating cyberattacks, it is not always possible to fix the problems when they occur and in some cases it may take weeks or months before the issue is resolved. If the affected organisation does not own up and communicate quickly with its stakeholders, this communication vacuum period can seriously erode stakeholder confidence and ultimately destroy the organisation's reputation. Using the famous 'The Good, the Bad and the Ugly' film metaphor, the author delves into three recent cyber crisis examples to define what was done well, which was a badly handled case, and which was a truly ugly one to draw best-practice lessons. Recognising that stakeholders are at the core of our organisations' echo system is a good place to start. By identifying and mapping them in order of importance, degree of influence and threat level, the organisation can develop engagement strategies that are designed to yield measurable results. Furthermore, the stakeholder mapping process helps uncover opportunities as well as worst-case scenarios that can be prepared for and help weather the storm. Ultimately, stakeholder outrage can drive crises into reputation meltdowns and the ability to communicate swiftly, transparently and credibly is the cornerstone of any effective crisis response strategy, but especially cyber ones where there are seldom quick fixes. The ability to retain stakeholder trust in the midst of adversity and chaos underpins the organisation's capacity to protect its reputation and possibly emerge stronger on the other side.

KEYWORDS: stakeholder mapping, scenario planning, stakeholder trust, credibility, reputation, crisis communication

## INTRODUCTION

Everyone agrees: cyber breaches are inevitable and are increasing in scope and complexity.

Much has been written about cybercrime, its origin, motives, players, methods, victims, detection and prevention capability and of course its cost, whether human, operational, financial or reputational, among others.

The 2017 NotPetya cyber strike is a notable case in point. According to the *New York Times*:

> 'In just 24 hours, NotPetya wiped clean 10 percent of all computers in Ukraine, paralyzing networks at bank, gas stations, hospitals, airports, power companies and nearly every government agency, and shutting down the radiation monitors at the old Chernobyl nuclear power plant. The attack made its way to the software maker's global clients, eventually entangling Mondelez and Merck, as well as the Danish shipping conglomerate Maersk and FedEx's European subsidiary. It hit even Russia's state-owned oil giant, Rosneft.'[1]

Cyber criminals almost always seem to be ahead of the curve while law enforcement, regulators, institutions and businesses try to play catch-up. Investigating can take time:

> 'The BakerHostetler "2019 Data Security Incident Response Report" found it took 28 days on average to complete a forensics investigation, meaning answers may not be available to stakeholders for more than a month.'[2]

## QUICK OWNERSHIP AND COMMUNICATION ARE CRITICAL

Therefore, quickly communicating about the incident is almost as important as managing the incident itself. As we have already witnessed in numerous cases, the impact of a cyberattack can be devastating — to the very ability of the organisation involved to continue to operate and to the affected stakeholders, such as employees and customers, etc. Potentially the greatest long-term impact is the loss of trust. The ability to retain stakeholder trust is the differentiating factor between a crisis and a reputation train wreck.

The mid-July 2020 massive Twitter hack exposing numerous high-profile accounts is a more recent example of the impact of such attacks and the criticality of protecting stakeholder trust to safeguard reputation.

> 'The Twitter accounts of major companies and individuals were compromised on Wednesday in one of the most widespread and confounding breaches the platform has ever seen, all in service of promoting a bitcoin scam that earned its creators nearly $120,000.'[3]

Twitter communicated quickly — 'We are aware of a security incident impacting accounts on Twitter. We are investigating and taking steps to fix it. We will update everyone shortly' — and continued to post regular updates as the investigating team was hard at work, with CEO Jack Dorsey personally tweeting:

> 'Tough day for us at Twitter. We all feel terrible this happened. We're diagnosing and will share everything we can when we have a more complete understanding of exactly what happened. Love to our teammates working hard to make this right.'

Product chief Kayvon Beykpour releasing a public statement on his personal account:

> 'Our investigation into the security incident is still ongoing but we'll be posting updates from @TwitterSupport with more detail soon. In the meantime I just wanted to say that I'm really sorry for the disruption and frustration this incident has caused our customers.'

It is too early to assess whether this crisis will have lasting reputational impact on Twitter.

The verdict is out there. While some lawmakers pressed the platform for more transparency, by all accounts Twitter was out there quickly and regularly with information updates following one of crisis management's key tenets.[4] Yet this is not always the case and it is worth examining the power of stakeholders in making or breaking a crisis.

## THE POTENTIAL FOR STAKEHOLDER OUTRAGE IN RESPONSE TO ANY INCIDENT MUST BE RECOGNISED

Globalisation and the increasing interdependence of our societal systems are generating multiple levels of stakeholders that are a challenge to engage with in normal times, but that become a nightmare to manage in a crisis. Besides employees, regulators, politicians, victims, customers and shareholders, organisations now also have to reckon with other stakeholder groups that become involved through social media networks. The multitude and diversity of these intertwined stakeholder groups are compounding the intensity of crises. Overall, we are witnessing more stakeholder outrage at corporate and institutional misbehaviour.

Statistics from the Institute of Crisis Management's 2019 annual report show that 73 per cent of business crises worldwide are non-event-related, or smouldering, crises.[5] Often the problem or issue exists long before it goes public, yet little is done to address and resolve it — or worse, it is covered up before it escalates. A single trigger — a rumour, a leak, or a stakeholder action — can catapult an organisation into crisis in a very short time, with devastating effects.

In the BCI Horizon Scan 2018 Report, Howard Kerr**,** BSI Chief Executive, writes:

> 'The business world has changed significantly since the report launched, yet there is remarkable consistency to the top business threats. Whilst the pace of technology development moves at lightning speed, the role it plays in society and how it supports business simply becomes more fundamental. So, it's no surprise cyber-attacks, data breaches and unplanned IT outages remain the top threats – if these threats are exposed, the impact can be significant to operations and ultimately reputations.'

As a top threat, a cyberattack is difficult to detect and prevent, with cyber criminals ever so creative and resourceful in their drive to cause maximum disruption. Author of *Future Crimes*, Marc Goodman writes:

> 'Just one compromised e-mail account on Facebook, Google, or Apple can give hackers access to years of your e-mail messages, calendar appointments, instant messages, photographs, phone calls, purchase histories on Amazon, bank and brokerage accounts, and documents in Dropbox or on Google Drive.'

Goodman adds:

> 'According to a Verizon study, once hackers set their sights on your network, 75 percent of the time they can successfully penetrate your defences within minutes and that only 15 percent of the time it takes more than a few hours to breach a system.'

## STAKEHOLDER MAPPING CAN HELP PREVENT A REPUTATION MELTDOWN

So, once an organisation has been targeted, what can be done to mitigate the damage and prevent a reputation meltdown?

All of today's crises, including cyberattacks, have one thing in common: acute stakeholder pressure before, during and after. To anticipate, prevent and mitigate crises, business and crisis leaders must have a solid grasp of the climate in which they are working as well as the stakeholder scene surrounding any emerging issue.

Actively engaging with stakeholders is a make-or-break opportunity every business leader should pursue to dampen the impact of crises. But this is not the case of 'one size fits all'. Different stakeholders will have different perceptions of the situation, information needs and expectations from the organisation in crisis. So, a blanket communication approach will not succeed to address individual concerns. Instead it is necessary to dive into each stakeholder group in more detail to tailor the tone and content of messages and communicate via the appropriate channel.

The foundation to an effective crisis communication strategy is the stakeholder map, but stakeholder mapping cannot be done on the fly. It is a process that requires skills and therefore training.

Stakeholder mapping consists of identifying all audience groups with a stake in the crisis and categorising them in at least three groups: allies, neutral and opposition. 'Stakeholder mapping identifies stakeholder expectations and power and helps in understanding political priorities', write Gerry Johnson, Kevan Scholes and Richard Whittington, in their book *Exploring Corporate Strategy.*

> 'There are different ways in which stakeholder mapping can be used to understand stakeholder influence. It underlines the importance of two issues: (1) how interested each stakeholder group is in impressing its expectations on the organisation's purposes and choice of strategies, and (2) whether stakeholders have the power to do so.'

The stresses of crises often cause leadership teams to go into a siege, feel victimised and fail to recognise that there are diverging, and equally valid, perspectives on the situation. Yet the ability to empathise is possibly one of the most critical crisis leadership skills. Stakeholder mapping is very powerful to help decision makers put themselves in the shoes of different stakeholders and thus make better decisions.

**Stakeholder mapping steps**

1. *Identify all audience groups,* no matter how small or remote to the crisis situation, that have a stake in the crisis; consider breaking it down to individuals;
2. *Categorise audiences* in at least three groups: allies, neutral and opposition;
3. *Define each audience group's specific issues* regarding the situation, whether a group is likely to take any action either for or against you;
4. *Define whether your organisation has any influence* on each stakeholder group (and if not, focus instead on the ones that can be influenced);
5. *Define the desired outcome*, the strategy for reaching it and the key messages to use.

During crises, the stakeholder map must be continuously reviewed and fine-tuned as the situation develops and more stakeholders come onto the scene. Short training sessions and the use of digital stakeholder mapping tools are recommended to master and facilitate the process. Feedback collected during training indicates a consistently positive experience from trainees who quickly demonstrate the ability to populate stakeholder maps that provide valuable insight for to the crisis teams to take action.

In cyberattacks, where investigation and resolution take time, rapid, active and regular stakeholder engagement becomes critical to retain trust, survive the crisis and possibly emerge stronger on the other side . The sheer multitude of stakeholders, however, with their varying and sometimes conflicting agendas, can be intimidating and a daunting task to undertake. Consequently, organisations often fall into the trap of trying to remedy the problem, before acknowledging that there is one with their stakeholders.

Good and bad examples abound, and it is worth examining a few for their successes and failings in terms of communication, stakeholder engagement and ultimately reputation protection. To do so, let us borrow the famously catchy movie title: 'The Good, the Bad and the Ugly'.

## THE GOOD — NORSK HYDRO

Norsk Hydro, a fully integrated aluminium and renewable energy company with 34 per cent Norwegian state ownership, 35,000 employees in 40 countries, became the victim of a cyberattack on 19th March, 2019.

Norsk Hydro's central system as well as the user and log-in system went down as a result of the 'LockerGoga' ransomware attack. The ransomware affected operations in several business areas globally.

Norsk Hydro quickly isolated its plants, switched to manual operations where possible, eg aluminium smelters, as digital systems were affected, did not pay the ransom and fixed the problems themselves.

Two days after the attack, they managed to detect the root cause of the problems. A plan was implemented in order to restore the IT systems:

- *After three days*: Sixty per cent of business operations were up and running;
- *After three weeks*: Production was almost back up to normal, but administration lagged behind;
- *After one month*: Norsk Hydro announced that they would postpone their first-quarter earnings report from 30th April to 5th June, due to the problems caused by the cyberattack.

Besides the strong and swift operational response, which is not specifically the subject of this paper, the Norsk Hydro case stands out for its exemplary stakeholder outreach and drive to be transparent from the onset.

Specifically, in terms of internal and external communication, the company took the following measures:

- *Clear and fast communication* with stakeholders and media:
  - Held a press conference announcing the hack and what they were doing about it immediately;
  - Made active use of social networks to communicate updates and fixes to internal and external stakeholders;
- *The newly launched website* became the primary communication channel regarding the attack;
- *Actively engaged with key stakeholders* including Microsoft, national cybercrime bodies, industry groups and relevant authorities;
- *Documented their recovery efforts* via videos, social media platforms, etc.

Total losses caused by the attack have been estimated at US$52m. While the company's core profit fell 82 per cent in the first quarter (better than expected), the value of Norsk Hydro shares went up following the news.

> 'But what they've lost in productivity and revenue, they've arguably gained in reputation. The company's response is being described as "the gold standard" by law enforcement organisations and the information security industry. Not only did they refuse to pay the hackers but they've also been completely open and transparent with the outside world about what happened to them.'[6]

## THE BAD — MARRIOTT

On 30th November, 2018, Marriott revealed that its Starwood division's guest reservation database had been compromised by an unauthorised party. Information accessed included payment information and other highly sensitive data such as names, phone numbers, e-mail addresses and passport numbers.

> 'The affected hotel brands were operated by Starwood before it was acquired by Marriott in 2016. They include W Hotels, St. Regis, Sheraton, Westin,

> Element, Aloft, The Luxury Collection, Le Méridien and Four Points. Starwood-branded timeshare properties were also affected. None of the Marriott-branded chains were threatened.'[7]

The massive data breach understandably caused alarm among customers and investigators. Yet Marriott's perfunctory messages, lacking empathy and a much-needed apology, fell short of stakeholder expectations as documented in multiple tweets:

> 'I've used @MarriottIntl hotels often enough that I have an active @MarriottRewards acct. Given this data breach — the kinds of data leaked, the number of customers affected, and the CEO's appallingly lame public response — I am considering never staying at a Marriott property again.'

> 'Words that are missing from the Marriott statement: sorry, inconvenience, apologise, "your data" … The closest I find is that Marriott "regrets this incident happened". It's like they're upset that now they have to do some work, rather than upset that they hurt their customers.'

In addition, Marriott only started sending e-mails to customers on 30th November, yet it first knew of the problem two months before and had identified what information was stolen by 19th November. Investigators later said the breach stretched as far back as 2014.

The lack of transparency and slow communication further infuriated stakeholders and contributed to an erosion in trust. Yet although the crisis was certainly bad news for customers and the company's reputation, six month later it seems to have had little impact on its bottom line.[8]

In January 2019 Marriott announced that the hack had affected an estimated staggering 383m customers, less than the initially stated 500m, arguably making it the one of the largest security breaches on record. Sadly, there are worse examples.

## THE UGLY — CATHAY PACIFIC AIRWAYS

In May 2018, Cathay Pacific confirmed that the personal data of around 9.4m passengers was compromised, including 860,000 passport numbers, 245,000 Hong Kong ID card numbers, 403 expired credit card numbers and 27 current credit card numbers without CVV, e-mail, physical addresses and frequent-flier programmes, as well as historical travel information, which could be used to reset passwords or obtain private financial information. Yet, the breach was suspected to have already started in March, with IT security experts focusing solely on containment and prevention throughout March, April and May.

While the carrier apologised after making the announcement, holding back this information for three months seriously dented its credibility among stakeholders and the airline was criticised for not telling customers about the hack immediately.

Specifically, contradicting statements were made: Paul Loo, chief customer and commercial officer, stated that the company was not able to confirm if its IT system had been breached until early May, but failed to mention that the company had been subjected to attacks for more than three months at that time.

The hack prompted a formal investigation by the Hong Kong privacy watchdog, as well as a police investigation. Cathay was questioned by 27 regulators from 15 countries. The company was also accused of a cover-up by Hong Kong lawmakers.

Investigators later revealed that the airline's computer systems had exposed details of 111,578 UK residents. The regulator said it subsequently uncovered 'a catalogue of errors' during a follow-up investigation, including:

- Back-up files that were not password protected;
- Internet-facing servers without the latest patches;
- Operating systems that were no longer supported by the developer;
- Inadequate anti-virus protection.

At least one attack involved a server with a known vulnerability; however, the fix was never applied, despite having been public knowledge for more than ten years.

Steve Eckersley, the ICO's director of investigations, said there were 'a number of basic security inadequacies across Cathay Pacific's system, which gave easy access to the hackers'. The airline failed four out of five of the basic cyber essentials guidance from the National Cyber Security Centre, he added.[9]

The combination of lack of transparency prompting a free flow of criticism from various stakeholders, coupled with documented failure to take the adequate protection measures and various errors, has caused Cathay Pacific reputational harm as well as considerable cost. As of October 2018, the airline's shares had sunk the most in almost two years, shaving US$201m off its market value.

In March 2020, the Information Commissioner's Office (ICO) fined Cathay Pacific Airways £500,000 — the maximum possible fine under the Data Protection Act 1998 — for failing to protect customers' personal data.[10]

## WORST-CASE SCENARIO PLANNING AS AN ESSENTIAL STRATEGIC TOOL

Besides the clear benefit that mapping stakeholders has on the ability to assess perceptions, identify friends and foes, anticipate potential actions and reactions and craft messages that resonate with audiences and influencers, the process also helps to define escalating scenarios and corresponding mitigation strategies.

Crises typically get worse before they get better. Under the high-pressure conditions of a crisis, scenario planning helps the team pursue a dominant strategy related to the likely worst-case development. This is not a matter of gazing into a crystal ball to predict the future, but rather a fast and powerful methodology to be ready for the worst.

In their book *Strategic Management Theory: An Integrated Approach*, Charles Hill and Gareth Jones state:

> 'The great virtue of the scenario approach to planning … is that it can push managers to think outside the box, to anticipate what they might have to do in different situations, and to learn that the world is a complex and unpredictable place that places a premium on flexibility, rather than on inflexible plans based on assumptions about the future that may turn out to be incorrect.'[11]

## RETAINING CREDIBILITY AND SAFEGARDING STAKEHOLDER TRUST TO SAVE THE DAY

When an organisation faces a crisis, be it a cyberattack, an industrial accident, an environmental contamination, a scandal or an ethics breach, taking stock of the situation is a good place to start. It will help determine stakeholders' positions, the areas of influence and define a strategy based on worst-case scenarios. Only then can the affected organisation have a better chance to not only survive the crisis but also potentially emerge stronger from it.

It is always a challenge to assess the true impact of a crisis on short and long-term reputation, and time often helps erase bad memories. It is safe to say, however, that in today's increasingly exposed and scrutinised environment, organisations must work harder to establish and retain trust. Irresponsible or unethical conduct quickly ends up in the court of public opinion and placed under the microscope of investigators, regulators and litigators.

Reputation cannot be acquired. It depends on the goodwill of stakeholders to grant organisations their reputational licence. As Warren Buffet famously said: 'It takes 20 years to build a reputation and five minutes to ruin it. It you think about that you'll do things differently.'

Crises happen and while it is not always possible to control the events, it is well within our power to choose how we respond to them. If internal and external stakeholders are the pillars of our organisations' existence, speed, transparency and honesty are the pillars of credibility. Without credibility there is no trust. In a crisis, mapping stakeholders is the starting point to communicating sensitively and effectively. And a key way to prevent a reputation meltdown.

## References

1. Satariana, A. and Perlroth, N. (April 2019), 'Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong', *New York Times*, available at https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html (accessed 21st December, 2020).
2. Abrams Kaplan, D. (April 2020), '4 Tips for Communicating Through a Data Breach', International Association of Business Communicators.
3. Statt, N. (July 2020), 'Twitter's massive attack: What we know after Apple, Biden, Obama, Musk and others tweeted a bitcoin scam', The Verge, available at https://www.theverge.com/2020/7/15/21326200/elon-musk-bill-gates-twitter-hack-bitcoin-scam-compromised (accessed 21st December, 2020).
4. CS&A, 'CS&A's 10 Commandments of Crisis Management', available at https://www.linkedin.com/in/carolinesapriel/detail/overlay-view/urn:li:fsd_profileTreasuryMedia:(ACoAAABv1gMBX82sqNPB43XRUQJGhRxv4dEgmlY,1597245531007)/ (accessed 21st December, 2020).
5. Institute for Crisis Management, 'ICM Annual Crisis Report', available at https://crisisconsultant.com/icm-annual-crisis-report/ (accessed 21st December, 2020).
6. Tidy, J. (June 2019), 'How a ransomware attack cost one firm £45m', BBC News, available at https://www.bbc.com/news/business-48661152 (accessed 21st December, 2020).
7. AP News (January 2019), 'Fewer affected in Marriot hack, but passports a red flag', available at https://apnews.com/2e2f9aad21fc4fdd87b7852e5db2327f (accessed 21st December, 2020).
8. Isidore, C. (May 2019), 'Marriot hasn't paid the price for its massive data breach', CNN, available at https://edition.cnn.com/2019/05/10/business/marriott-hack-cost/index.html (accessed 21st December, 2020).
9. National Cyber Security Centre, 'About Cyber Essentials', available at https://www.cyberessentials.ncsc.gov.uk/advice/ (accessed 21st December, 2020).
10. BBC News (March 2020), 'Cathay Pacific fined £500,000 over customer data protection failure', available at https://www.bbc.com/news/technology-51736857 (accessed 21st December, 2020).
11. Hill, C., Jones, G. and Schilling, M. (2014) *Strategic Management Theory: An Integrated Approach*, South-Western College Publishing, Cincinnati, OH.