



Case Study: Facebook In Face of Crisis.

Raquel Pita Guerreiro Marcelino Duarte

Dissertation written under the supervision of Daniela Langaro

Dissertation submitted in partial fulfilment of requirements for the MSc in Management with Specialization in Strategic Marketing, at the Universidade Católica Portuguesa, January 2020.

Case Study: Facebook In Face of Crisis.

Raquel Pita Guerreiro Marcelino Duarte

Abstract

Created to connect people in a limited academic environment, Facebook rapidly became the world's largest social media network, containing numerous, and highly valued features. Despite its rapid growth and outstanding performance, Facebook has seen better days. In March 2018, the giant was caught up in a large-scale data breach scandal, in which the British political consulting firm Cambridge Analytica acquired the personal data of around 87 million users without their consent and used it for political purposes, namely in the 2016 U.S. Presidential elections but also in the Brexit Vote Leave campaign.

The scandal caused Facebook to face the wrath of all those affected by the privacy breach but also of those who were indirectly, in some way, concerned by what happened. Several challenges confronted the company afterwards, such as legal actions for the lack of users' privacy protection. Nevertheless, even if Facebook put in place several measures to prevent such an event from happening again, the biggest challenge was definitely to regain stakeholder's trust and to rebuild the organization's reputation.

The crisis response strategies adopted by Facebook were considered not enough to reassure users and all those troubled by the breach. This case study provides appropriate data that allows students to assess the crisis situation and to put themselves in a position of Facebook's CMO, in order to come up with crisis management path suggestions, through the combination of theories and real-life facts.

Keywords: Crisis, Crisis Management, Reputation Management, Data Breach, Data Privacy, Trust, Social Media

Crisis Management: The Facebook - Cambridge Analytica Data Breach Case

Raquel Pita Guerreiro Marcelino Duarte

Resumo

Criado para interligar pessoas num meio académico limitado, o Facebook rapidamente se tornou na maior rede social do mundo, contendo inúmeras características muito valorizadas pelas pessoas. Apesar do seu rápido crescimento e performance distinguível, o Facebook já viu melhores dias. Em Março de 2018, o gigante foi apanhado num escândalo de violação de dados em larga escala, no qual a empresa britânica de consultoria política Cambridge Analytica adquiriu os dados de cerca de 87 milhões de utilizadores sem o seu consentimento e usou-os para fins políticos, nomeadamente nas eleições presidenciais dos E.U.A em 2016, mas também na campanha Vote Leave do Brexit.

O escândalo fez o Facebook enfrentar a ira de todos os afetados, mas também daqueles que estavam indiretamente, de alguma forma, preocupados com o que aconteceu. Vários desafios confrontaram a empresa posteriormente, como ações judiciais por falta de proteção da privacidade dos utilizadores. Contudo, mesmo com as medidas aplicadas pelo Facebook para evitar a recorrência deste tipo de eventos no futuro, o maior desafio foi definitivamente recuperar a confiança das partes interessadas e reconstruir a reputação da organização.

As estratégias de resposta à crise adotadas pelo Facebook foram consideradas insuficientes para tranquilizar os utilizadores e todos os afetados. Este estudo de caso fornece dados apropriados que permitem que os alunos avaliem a situação de crise e se posicionem como CMO do Facebook, para apresentar sugestões de caminhos para a gestão de crises, através da combinação de teorias e acontecimentos reais.

Palavras-chave: Crise, Gestão de Crise, Gestão de Reputação, Violação de Dados, Violação de Privacidade, Confiança, Redes Sociais.

Acknowledgements

I would like to thank the support and constructive feedback from my Dissertation supervisor Daniela Langaro, without whose help this work would never have been possible.

Acknowledgements are also due to Sara Oliveira and Catarina Alves, who have me much valuable suggestions and advice in early stages of this work.

Moreover, I am particularly grateful to my parents, who invested so much in my education, and whose unconditional support motivated me to reach this final step of my academic path.

Finally, I would like to show my appreciation to my family and closest friends, who somehow contributed to my emotional support and to the outcome of this work.

Lisbon, January 2020

Raquel Pita Guerreiro Marcelino Duarte

TABLE OF CONTENTS

Abstract	I
Resumo	II
Acknowledgements	III
Case Appendices	VI
List of Tables	VII
List of Figures	VIII
List of Abbreviations	IX
1. Introduction	1
2. The Case Study: Facebook & Cambridge Analytica Data Scandal	2
2.1. Zuckerberg starts out.	2
2.2. Facebook: the beginning of an era.	2
2.3. Facebook Privacy Controversies	4
2.4. Cambridge Analytica Data Privacy Scandal	5
2.4.1. What is the Facebook data privacy scandal?.....	5
2.4.2. Cambridge Analytica and the uses of the data.	6
2.4.3. Going back to 2014, where it all began.....	6
2.4.4. Facebook learns about the situation.	7
2.4.5. The worst is yet to come... ..	7
2.4.6. Breach Consequences.....	8
2.4.7. Facebook’s reaction.....	9
2.4.8. The Congress.....	11
2.4.9. Facebook under fire, again... ..	14
2.5. Conclusion.....	14
2.6. Case Appendices	16
3. Teaching Note	35
3.1. Teaching Objectives	35
3.2. Introduction	35
3.3. Synopsis	36
3.4. Suggested assignment questions	36

3.5. Literature Review	37
3.5.1. Crisis.....	37
3.5.2. Crisis Management.....	37
3.5.3. Reputation management	39
3.5.4. Information breaches.....	40
3.5.5. Crisis classifications	40
3.5.6. Impact of crisis on publics	42
3.5.7. Crisis recovery.....	43
3.5.7.1 Crisis response strategies	43
3.5.7.2. Select the correct crisis response strategy	45
3.5.7.3 Online response tools	48
3.6. Answers to Assignment Questions.....	49
3.6. Suggestions for the Animation of the Case Study.....	56
4. Reference List	57
Appendix	68

Case Appendices

Appendix 1. Number of monthly active Facebook users worldwide (Statista, 2019)...16

Appendix 2. Mark Zuckerberg post on the controversy of the News Feed (Facebook, 2006).
.....17

Appendix 3. Mark Zuckerberg post on the controversy of Beacon (Facebook, 2007). 18

Appendix 4. Mark Zuckerberg post on FTC settlement (Facebook, 2011).19

Appendix 5. Mark Zuckerberg post on the system malfunction (Facebook, 2013)......23

Appendix 6. Number of Facebook user accounts that may have been compromised in the Cambridge Analytica scandal as of April 2018, by country (Statista, 2018)......25

Appendix 7. Mark Zuckerberg’s first Facebook post after data breach scandal (Facebook, 2018a, March 21).26

Appendix 8. Sheryl Sandberg’s first Facebook post after data breach scandal (Facebook, 2018b, March 21).29

Appendix 9. Blog post on Facebook Newsroom after data breach scandal (Facebook Newsroom, 2018, March 21).....30

Appendix 10. Blog post on Facebook Newsroom announcing audit (Facebook Newsroom, 2018, March 19).32

Appendix 11. Facebook's annual revenue and net income from 2007 to 2018 (in million U.S. dollars) (Statista, 2018).33

Appendix 12. “Document Holds the Potential for Confusion”, Facebook blog post (Facebook Newsroom, 2019).34

List of Tables

Table 1. Types of Crisis (Coombs, 1995).....41
Table 2. Crisis-Response Strategies (Coombs, 1995)45

List of Figures

Figure 1. Faux Pas decision flowchart (Coombs, 1995, p.463)46
Figure 2. Accident decision flowchart (Coombs, 1995, p.465)46
Figure 3. Transgression decision flowchart (Coombs, 1995, p.467)47
Figure 4. Terrorism decision flowchart (Coombs, 1995, p.468).....47

List of Abbreviations

CA – Cambridge Analytica

CU – Cambridge University

FB – Facebook

GSR – Global Science Research

FTC – Federal Trade Commission

RBT – Resource Base Theory

DS – Distance Strategy

IS – Ingratiation Strategy

1. Introduction

No organization, in whatever place, is immune from a crisis, even if it is vigilant and actively seeks to prevent such an event. To worsen, the news go viral almost instantaneously and fake news spread like never before. This reality cultivates a need for preparation, and promptness to respond to any crisis, which can briefly be termed of “Crisis Management”. The way the organization communicates, in the aforementioned unstable context, is a critical part of the crisis management process and has a compelling effect on the payoffs of the crisis. The absence of adequate internal and external communications will make interested parties unaware of circumstances, and quickly become confused, angry and negatively reactive. Organizations may be seen as inept at best and negligent in the worst-case scenario, besides the severe impact on financial results and the strength of the reputational harm. Hence, improved crisis management cooperates in protecting both an organization and its stakeholders. Every crisis is a crisis, and every crisis has its own way of being addressed. Therefore, response strategies must be built upon each situation-specific traits, in order to diminish the damage caused.

The present case study is intended to be studied at a Master or MBA level, in a Brand Management and Strategy course, or even Brand communications and Digital Marketing disciplines. It aims providing students with a real-life organizational crisis situation, Facebook’s 2018 data breach, and leading them to discuss crisis and reputation recovery initiatives.

The current case study is structured as follows. The first chapter gives a brief overview of the company and its performance, followed by a story of how the data breach situation occurred and the strategies embraced by Facebook to react to such a crisis, as well as a presentation of the challenges faced by the brand thereafter. The next chapter is a teaching note for the instructor(s), embodying a literature review of the topics and a group of discussion questions, including guidance on how to handle the case study in order to coordinate the flow of in-class dialogue successfully. The final chapter provides recommendations to the proposed case questions, including a PowerPoint slide deck to be used in class. The suggested arguments are based upon a repertoire of crisis response strategies, built on well-known theory.

2. The Case Study: Facebook & Cambridge Analytica Data Scandal

On February 5, Facebook will turn 16 years old. Born in a young American student's dorm, it is now one of the most important and influential tech firms in history. Nonetheless, a black cloud began to hang over the company in recent years. It was March 16, 2018, and Mark Zuckerberg was quietly working at his Silicon Valley headquarters, when all of a sudden, all phones started ringing and moods got heated. What happened?

2.1. Zuckerberg starts out.

Mark Zuckerberg hit the coding road at a very early stage of his life. Motivated by his father, who taught him some programming bases, Mark had already a coding tutor by the age of 11.

Even though he pursued his studies in an elite boarding school, where other of his talents were highlighted, such as fencing and literature, Zuckerberg remained absorbed by the programming world. He created a software named Synapse that learned users' music taste and listening habits in order to generate personalized music playlists. At the time, AOL and Microsoft, two of the biggest tech companies in the world, showed interest in buying that software and hiring Mark, but the latter declined and decided to enroll at Harvard University instead, where he got accepted in the class of 2002.

In college, he built his reputation as the go-to software developer on campus. Among the software he built was "CourseMatch", that aided students to select their courses based on what other users selected. One of his most popular creations was "Facemash", a website that let students judge the attractiveness of each other to create rankings. Nevertheless, the school administration shut it down as it was considered inappropriate. The last project Zuckerberg worked on, before moving on with his lifetime project, was "Harvard Connection", a site designed to collect data from the university students' networks to create a dating website for the Harvard elite.

2.2. Facebook: the beginning of an era.

The origins of Facebook date back to February 2004, when "Thefacebook" was created. It consisted of a social media website that allowed users to create a personal profile, upload photos, share interests, and connect with other people. Immediately after its launch, Zuckerberg

was accused, by his previous Harvard Connection co-workers, of using their ideas to build a competing product. Years later, he was sued after proven that he had broken an “oral contract” with the accusers, who ended up receiving million worthy company shares.

Initially, Thefacebook was only open to Harvard students but, by the end of 2004, it expanded the membership to all universities in the US and Canada, gathering around 1 million users (*Appendix 1*). In the meantime, in June 2004, Zuckerberg had moved the company’s operations from his college dorm to Palo Alto, California. In August 2004, Peter Thiel, co-founder of PayPal, invested \$500 000 in the company and joined the board. This was the first outside investment, followed by a huge one in the following year, from the venture capital firm Accel, equaling an amount of \$12.7 million.

In August 2005, Thefacebook suffered a slight change in its name, becoming officially “Facebook”. By the end of 2005, the network had around 6 million users. After opening to high-school students and expanding to Mexico, UK, Australia, New Zealand and Ireland, Facebook finally freed it to everyone aged 13 and over, on September 26, 2006. Thereon, the company knew nothing but growth. Zuckerberg focused on expanding the social network, opening the gates of his project to outside developers by launching the Facebook Platform¹ in May 2007, and adding more and more features every year.

In 2007, Facebook announced its presence in the Mobile Web, promising an optimized experience in a small screen. By 2009, Facebook apps were available on mobile phones, with some exceptions. With all these new easy accesses, Facebook had gathered an amount of 500 million users, by July 2010. By December, the company was valued at \$50 billion (Techcrunch, 2011). Facebook was now the third-largest American Web company, behind Google and Amazon. According to a Nielsen study, in 2011, the social media had become the second-most visited site in the U.S., following Google (BBC News, 2012).

2012 was a year of major events for Facebook. Among the most important FB’s acquisitions was Instagram, which the company acquired for an amount of \$1 billion. In May of that year, Zuckerberg took Facebook public, through the company’s first initial public offering, which raised \$16 billion, making in the biggest IPO ever (The New York Times, 2012). The IPO was

¹ **Facebook Platform:** set of application programming interfaces and tools provided by Facebook to third-party developers, allowing them to create applications to interact with core Facebook features (Facebook Platform).

controversial and caused immediate price declines (Yahoo!, 2012) and was the subject of lawsuits. The CEO announced in October that FB had 1 billion active users (CNN, 2012).

2.3. Facebook Privacy Controversies

A variety of privacy concerns has caused Facebook to be scrutinized over time. Even if repeatedly adjusting its privacy settings and policies, the company has been experiencing a continuous stream of controversies over how it safeguards users' privacy.

Problems regarding user privacy started emerging in 2006, when the News Feed was launched, a feature that would spot recent friend activity and which shared personal details without user's consent. The intrusive nature of the News Feed upset students (the only users allowed at the time), which organized themselves to protest against it. Zuckerberg responded to it with a post titled "Calm Down. Breathe. We Hear You." (*Appendix 2*), in which he acknowledged the users' reactions, reiterated the privacy features and promoted the new feature as "cool" way to keep up with their friends' life events, etc. (Time, 2006).

In late 2007, the Beacon system, which formed part of Facebook's advertisement system, tracked users' online purchases from third-party partner websites, once again without their knowledge, and shared it on their News Feed. Zuckerberg issued an apology speech (*Appendix 3*), in which he announced that the Beacon program would now be optional. Two years later, the company was forced to shut down Beacon following legal action and ended up paying \$9.5 million to resolve the privacy concerns (The Telegraph, 2009). Two-thirds of the amount were used to establish a foundation called "Digital Trust Foundation", aiming to "fund and sponsor programs designed to educate users, regulators and enterprises regarding critical issues relating to protection of identity and personal information online", and the other third was allocated to lawyers (NBC News, 2013).

At the end of the year 2011, Facebook agreed to settle Federal Trade Commission charges. As stated by the regulators, the company was failing to comply with its users' expectation of data privacy, making public to third-party apps and sharing with advertisers, all of the users' personal information (FTC, 2011). Due to these violations, the firm was required to take various steps to make sure it delivered on its promises for at least the following 20 years, namely by warning and getting users' approval before making any changes in the way it shared their data.

In the FTC proposed settlement, Facebook agreed to be subjected to a privacy audit every two years. Zuckerberg admitted on his apology post that his company has made a “bunch of mistakes” (*Appendix 4*) but stated that it had already solved some of the privacy problems mentioned by the Commission. Moreover, he wrote that transparency and control were the company’s priorities, listing control features that the network has made available to its users over that year and presenting two new corporate officer privacy roles (The New York Times, 2011).

In 2013, FB acknowledged the existence of a bug that had exposed personal details of six million users over nearly a year. This malfunction allowed a user’s contact information (email address and phone number) to be shared with anyone having some contact information about that user or some type of connection to it (ZDNet, 2013). In a statement (*Appendix 5*), Facebook guaranteed that the bug was fixed the day after it was discovered. Moreover, the company said that the user’s contact information was only exposed to one or two other users with whom it had a connection with, and that no other data, such as financial data, was breached. Facebook announced it had already notified regulators and that it would inform those affected, one by one, via email.

These were just some examples of how hard it has been for the tech company to keep up with good data privacy practices, but the worst is yet to come.

2.4. Cambridge Analytica Data Privacy Scandal

2.4.1. What is the Facebook data privacy scandal?

The Facebook data privacy scandal fluctuates around the collection of the personal information of around 87 million users worldwide (*Appendix 6*), by a political consulting firm named Cambridge Analytica. The latter, in collaboration with Global Science Research, owned by Aleksandr Kogan, was able to gather data through a personality test app, called “thisisyourdigitallife”. Millions of users were paid to carry a personality test, agreeing that their data could be used just for academic purposes. The information collected allowed to build the users psychographic profile according to their openness, conscientiousness, extraversion, agreeableness and neuroticism levels (the OCEAN model). By adding the app to the Facebook account to answer the questionnaire, the people behind it could easily compile profile

information, such as age and status updates, likes and, in some cases, private messages. And this happened not only to the people that took the test but also to all their Facebook friends. The idea was that, by gleaning people's Facebook likes, the company could begin to understand one's personality, and then more effectively target political advertising at that person. The app was downloaded around 270 000 times.

2.4.2. Cambridge Analytica and the uses of the data.

Cambridge Analytica was an offshoot of the SCL (Strategic Communication Laboratories) group. SCL was behavioral research and strategic communication company, based in the UK. CA was itself created in 2014 and maintained offices in London, New York and Washington. There were three key people involved: the U.S. billionaire Robert Mercer (investor), Steve Bannon (VP) and Alexander Nix (CEO). CA marketed itself as a provider of "consumer research, targeted advertising and other data-related services to both political and corporate clients" (Reuters, 2018).

Soon after its creation, a Cambridge data professor, Aleksander Kogan, approached the company, with its recent app "thisisyourdigitallife". This app allowed a much cheaper and faster way of collecting data of Facebook users, but also their whole network of friend's data. The data was then used for political purposes to support several campaigns. These included the Ted Cruz and Donald Trump campaign for the 2016 presidential elections and also the Vote Leave campaign, which acted in favor of Brexit (The Guardian, 2018, March 18)

The company closed its doors on May 1st, 2018, after the scandal.

2.4.3. Going back to 2014, where it all began.

To really undermine what is behind the famous Facebook data breach, it is necessary to go back to the year of 2014. In February, a series of reviews were made on the Turkopticon² website, a third-party review website for users of Amazon Mechanical Turk³ (MTurk). These reviews detailed a task ordered by Aleksander Kogan, asking users to complete a survey in the

² In this platform, workers are allowed to give reviews on their employers. It aims to help potential workers by providing recommendations of the best employers and this way, avoid shady jobs (Turkopticon)

³ MTurk is a crowdsourcing website, available for individuals and businesses, to outsource their processes and jobs to a distributed workforce who can perform these tasks virtually. These tasks may include survey participations, answering questions, conducting data validation, etc. (Amazon Mechanical Turk)

“thisisyourigitallife” app. First of all, the survey required them to add the app to the Facebook account, which violated MTurk’s terms of service. Second, one of the reviews transcribed the implications of participating in the survey: “provide our app access to your Facebook so we can download some of your data, some demographic data, your likes, your friends’ list, whether your friends know one another, and some of your private messages.” (TechRepublic, 2019).

2.4.4. Facebook learns about the situation.

The Guardian revealed the scheme in December 2015 (The Guardian, 2015) and Facebook took notice that all the gathered data from the Kogan’s app had been shared with CA. At the time, Facebook users were not notified by the social network that their data had become the property of another company. Zuckerberg only commented on the subject when the scandal surfaced again in 2018. He stated: “we immediately banned Kogan's app from our platform and demanded that Kogan and CA formally certify that they had deleted all improperly acquired data. They provided these certifications.” (Facebook, 2018a, March 21). In August of 2016, Facebook took legal action against GSR, the company owned by Kogan, for passing along illegally collected data.



(The Guardian, 2015)

2.4.5. The worst is yet to come...

On March 2018, Christopher Wylie, a GSR former employee, came upfront and reported the scheme behind the collection of the data. On March 17, two big journals, The Guardian and The New York Times, made publications on the subject, with big revelations. They exposed

that 50 million Facebook profiles were harvested by CA, this figure being later revised to “up to 87 million” profiles. Wylie, who worked on the data collection through the “thisisyourdigitallife” app, alleged that the data was sold to CA, which then used it to build “psychographic” profiles of the users in order to posteriorly target them with specific advertising. The whistleblower told the Observer: “We exploited Facebook to harvest millions of people’s profiles and built models to exploit what we knew about them and target their inner demons. That was the basis the entire company was built on” (The Guardian, 2018, March 17). CA denied the allegations made by Christopher.

A day before the publication of these news, on March 16, Facebook threatened to sue The Guardian over the disclosure of the story. Carole Cadwalladr, a journalist of the *Observer* and author of the articles, announced it through a Tweet (Twitter, 2018) and later addressed the topic in a Ted Talk (TED, 2018). By the same token, the data-mining firm, CA, also threatened to bring legal charges against The Guardian for defamation (The Guardian, 2018, March 18).



(Twitter, 2018)

2.4.6. Breach Consequences

Suddenly, all eyes were on the social media giant and on CA. People were not pleased with what they heard and read on the news. Many users were worried and wanted increased regulations around their personal data, while others were even investigating on how to delete their Facebook account. Indeed, a growing movement to delete Facebook rapidly moved across the world (Independent, 2018), namely through the viral hashtag #deletefacebook. Financially,

the day after the scandal, Facebook's share price went down by 7%, and its market value fell more than \$36 billion (CNBC, 2018, November 20).

Facebook and CA were now object of an investigation, by the British Information Commissioner's Office. Likewise, the Electoral Commission also started investigating what role the political consulting firm had in the EU referendum (The Guardian, 2018, March 17). The Guardian was able to get a testimony for an information commissioner, named Elizabeth Denham, which stated: "We are investigating the circumstances in which Facebook data may have been illegally acquired and used. It's part of our ongoing investigation into the use of data analytics for political purposes which was launched to consider how political parties and campaigns, data analytics companies and social media platforms in the UK are using and analyzing people's personal information to micro-target voters."

2.4.7. Facebook's reaction

On the day Wylie's revelations became public, Facebook's primary reaction was refuting the way the news framed the incident. Paul Grewal, the company's deputy general counsel, wrote on the network's blog (Facebook Newsroom, 2018, March 17) that "Aleksandr Kogan requested and gained access to information from users who chose to sign up to his app, and everyone involved gave their consent.", thus defending the soft policies of the social media. Later, the company seemed to recognize that blaming users for not understanding its complex privacy terms would not be the best way forward, especially because of all the public fuss (The Guardian, 2018, March 22).

Mark Zuckerberg broke his silence on the CA data scandal five days after its revelation, on March 21 (The Guardian, 2018, March 22). He made a public statement on his Facebook page, saying "We have a responsibility to protect your data, and if we can't then we don't deserve to serve you" (*Appendix 7*). The leader of Facebook briefly reviewed critical past events, starting in 2007 until the moment they learned that CA had not deleted the data extracted, as requested years before. He reminded that in 2014, the platform announced changes in its privacy policies, including limiting abusive apps to aggregate data on users' and friends, without their consent. By the same token, he addressed the scandal that involved Facebook, recognizing that its policies that allowed an improper use of data caused users' trust in the company to be broken. He wrote: "(...) it was also a breach of trust between Facebook and the people who share their

data with us and expect us to protect it”. At the time, Sheryl Sandberg, Facebook’s COO, shared the CEO’s post and communicated to people through her own comment: “We know that this was a major violation of people’s trust, and I deeply regret that we didn’t do enough to deal with it.” She added “You deserve to have your information protected — and we’ll keep working to make sure you feel safe on Facebook. Your trust is at the core of our service. We know that, and we will work to earn it.” (*Appendix 8*).

Besides acknowledging that his company has failed to keep up with its users’ expectations, by not notifying them that the personal data of 87 million among them had been harvested and improperly shared, Zuckerberg noted that, up to that moment, the social media giant had made important changes in the way its shared data with third-party applications. In his written speech, the Facebook founder said it would enlighten the users that were affected by the data reaping but also, that the company would put in place several measures that would favorably prevent such incidents from happening again (CNBC, 2018, March 21). One of the measures that were promised to be implemented was an investigation of all apps with a connection to Facebook and thorough audits to any app with dubious activity. Furthermore, the company also announced it would create strong data access restrictions to developers, in order to block privacy intrusions. Moreover, to facilitate users’ access to which apps they have allowed to collect their data and easily remove those apps’ permissions, Facebook would provide a tool at the top of the News Feed that would enable a faster approach to manage privacy settings.

More measures were outlined in another post made by the company in the Facebook Newsroom blog, on March 22 (*Appendix 9*). Namely, the company showed intention to increase the bug bounty program, for people to report cases of security vulnerability, namely developers misusing their data, and get rewards for it.

Zuckerberg was also interviewed by a few media channels to communicate to users his side of the story. Among these, a televised interview with CNN’s Laurie Segall, in which he once again regretted the incident, acknowledging that it was an enormous breach of trust: “I’m really sorry that this happened”. Moreover, he provided an explanation of why Facebook did not make any effort to communicate with the concerned users back in December 2015. Indeed, the company had trusted the data-mining firm when the latter legally certified to have deleted all the data, believing that the problem would be solved. “It was a mistake”, declared Zuckerberg. He tried to rest people by claiming “I’m serious about doing what it takes to protect our community.”

(CNN, 2018). In resembling conversations with the New York Times, Wired magazine and Recode, a tech news website, he showed openness to clarify any issue related to the case and showed agreement with some existing changes needed in the company's policies (The Guardian, 2018, March 22). The fact that no higher executive made earlier comments with respect to the incident was not by mistake. In fact, they wanted to wait for the company to be audited on the compromising handling of the users' data. They hired a digital forensics firm to conduct an audit of CA, which agreed to submit to it, and to other key people involved, namely Aleksandr Kogan and Christopher Wylie. The first one showed willingness to participate in it, but Wylie refused. On a blog post (*Appendix 10*), Facebook said: "We are moving aggressively to determine the accuracy of these claims. We remain committed to vigorously enforcing our policies to protect people's information,". However, the audit, which started on March 19, was obstructed by lawmakers from U.K. which started their own investigation and advised Facebook to back out from their own inspection (CNBC, 2018, March 21). Zuckerberg's words came days after tech insiders, lawmakers and even employees from his own company demanded explanations on the most recent privacy scandal. Even an online petition was created, in order to call for the disclosure of all the people that were affected by the breach, which gathered more than fifteen hundred signatures (The Guardian, 2018, March 22).

2.4.8. The Congress

In the following month after the CA story broke in newspapers, Facebook's CEO presented himself before Congress, in a two-day testimony, to address the data-sharing scandal (The Guardian, 2018a, April 11). He travelled to Washington, to Capitol Hill, for the scheduled meetings on the April 10 and 11, 2018.

In the first day of hearings, Zuckerberg testified before a five-hour joint hearing of the U.S. Senate commerce, science and transportation committee and the Senate judiciary committee. The young executive was wearing a suit, white shirt and a sky-blue tie, rather than his usual t-shirt. During the session, he adopted a silent and regretful posture, while senators asked him several questions. His confidence increased as the afternoon advanced, but he always showed himself willing to cooperate. "The most important thing I care about right now is making sure no one interferes in the various 2018 elections around the world," he declared, which gave awareness of how influential Facebook is in many democratic societies. A senator mentioned some images, supposedly spread online by Russians during the presidential elections of 2016,

which included Donald Trump. In this context, Zuckerberg was asked if he could guarantee that those kinds of images would not come out on the social media again. The CEO replied “Senator, no, I can’t guarantee that because this is an ongoing arms race,” and added, “As long as there are people sitting in Russia whose job it is to try and interfere with elections around the world, this is going to be an ongoing conflict.”. With this in consideration, he recognized that one of his “greatest regrets in running the company” was being passive in acting against the disinformation campaigns by the Russians during election time.

Moreover, when confronted with the 2015 facts, the moment they learned that CA was gathering massive amounts of users’ data, Zuckerberg admitted that the company did not inform the FTC about the situation of the data collection. He claimed, in his defense: “In retrospect, that was a mistake. We shouldn’t have taken their word for it. We considered that a closed case.”. Under interrogation, he pledged that his company was handling a “full investigation” into all the thousand apps that had access to user’s info. “If we find they’re doing anything improper, we’ll ban them from Facebook,” he communicated.

Still regarding CA, he stated that the company had not been an advertiser in 2015. However, after consulting his staff, he rectified his statement, claiming that the data marketing firm had been indeed an advertiser later that year and thus, could have been banned by Facebook once it discovered that it was harvesting data from people. Indeed, advertising was and is the core source of the giant’s revenues. During the U.S election of 2016, online advertising played a major role, which was reflected in the company’s financial statements (*Appendix 11*)

Furthermore, when asked if Facebook would embrace regulation, Zuckerberg said: “If it’s the right regulation, then yes.”. On the whole, Zuckerberg and Facebook admitted “It’s clear now that we didn’t do enough to prevent these tools from being used for harm. That goes for fake news, foreign interference in elections, and hate speech, as well as developers and data privacy.”. Taking responsibility for the company’s actions was always clear in Zuckerberg’s mind: “I started Facebook, I run it, and I’m responsible for what happens here.”.

In the second day of hearings, before the U.S. House energy and commerce committee. This time, he ran into tougher questions about privacy, surveillance, censorship and politics, which Zuckerberg struggled to respond (The Guardian, 2018b, April 11). During his testimony, Zuckerberg revealed that his data had also been sold to CA. Facebook’s privacy terms and conditions were accused of being a “minefield”, and the young entrepreneur was asked if he

was willing to change his business model to protect user's privacy. He replied, evasively: "Congresswoman, I'm not sure what that means.". Also, regarding CA, the CEO was asked if his company was planning to sue Kogan, Cambridge University or the consulting firm that had stolen the data of its users. He responded that legal action was on the table and said: "What we found now is that there's a whole program associated with CU where ... there were a number of other researchers building similar apps. We do need to understand whether there is something bad going on at CU overall that will require a stronger action from us.". He declared that the company had to figure out whether "something bad" was happening inside CU, and if so, they would be considering bringing legal charges against it.

Another representative raised the CA topic and accused Facebook to close its eyes to the situation and asked: "When the Guardian made the report, was that the first time you heard about it?" and claimed "There is a real trust gap here. This developer data issue is just one example. Why should we trust you to follow through on these promises?". Zuckerberg argued: "Respectfully, I disagree with that characterization. We've had a review process for apps for years. We've reviewed tens of thousands of apps a year."

Furthermore, Zuckerberg was requested to commit to making changes in all Facebook's default settings in order to reduce possible collections of personal information. He refused to simply answer with a "yes" or "no", because of all the complexity behind it: "Congressman, this a complex issue that I think deserves more than a one-word answer".

Several members of the House committee questioned the young CEO on his company's transparency about the quantity of information it collects on users and non-users. Tech specialists found discrepancies in Zuckerberg's speech, accusing of merging dissimilar points on the topic if whether users own and control their personal data. Indeed, when interrogated about who owns "the virtual you", Zuckerberg's chosen response was to indicate that each user owns all the "content" he uploads and can delete it at will. But, in fact, besides not directly answering the question, it is known that the advertising profile that the social network builds up about each user cannot be eliminated, and the latter has no control over it.

With respect to better regulation, Zuckerberg stated: "The internet is growing in importance around the world in people's lives, and I think that it is inevitable that there will need to be some regulation. So, my position is not that there should be no regulation, but I also think that you have to be careful about the regulation you put in place."

2.4.9. Facebook under fire, again...

Zuckerberg statements, regarding what and when they knew that CA was improperly using Facebook users' data, were proven to be fallacious. Indeed, the CEO claimed that the company learned about the situation in December 2015, when in reality, communications between Facebook employees showed that the company knew about CA as early as September 2015, way before The Guardian revealed that the political research firm was using the data collected to profile and target voters. This information was obtained through emails, that were released by Facebook, in the context of a SEC complaint on the misleading statements. In the emails, employees discussed that they had been warned that CA and other third parties were using Facebook's data, violating the company's policies, and that they were reaching out to those companies to investigate the situation. For instance, one employee spoke: "my hunch is that these app's data-scraping activity is likely non-compliant," mentioning various Facebook Platform Policies that these firms could have defied, namely, "Don't sell, license or purchase any data obtained from us or our services." (CNBC, 2019). Once these emails turned public, Facebook made a blog post on Facebook Newsroom, in a defensive tone, stating the company was standing by its initial position, that it was not aware that Kogan had sold the data to CA until December 2015. Stating the post: "In September 2015, a Facebook employee shared unsubstantiated rumors from a competitor of CA, which claimed that the data analytics company was scraping public data. (...) An engineer looked into this concern and was not able to find evidence of data scraping. Even if such a report had been confirmed, such incidents would not naturally indicate the scale of the misconduct that Kogan had engaged in." (*Appendix 12*). Again, how trustworthy are these words?

2.5. Conclusion

Facebook is the world's largest social media network, but, in recent years, its success has been harmed by critical privacy concerns. Since 2006 that Zuckerberg's company has been involved in controversies over the protection of its users' data. The March 2018 revelations of a major data breach, involving the data of more than 87 million people, were at the origin of a crisis that Facebook was not prepared to face. The CEO had a very hard time during this crisis, whose severe consequences could have been mitigated by a good communication strategy.

The way a company communicates to its stakeholders in a crisis scenario is key for softening the impact of its negative outcomes. To properly manage communications, it is important to establish ways-of-doing in the three communication phases.

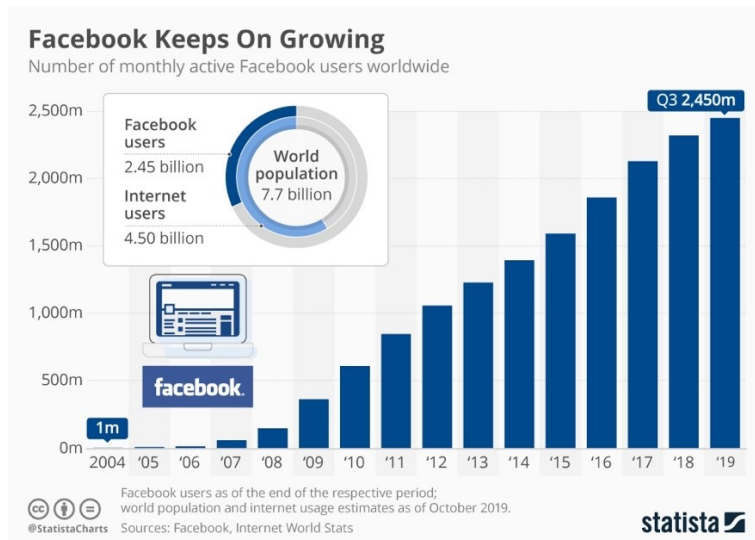
It is important to maintain good Issues Management (Coombs, 2010b), in order to prevent issues from developing into major problems. Facebook needs to review its management of issues so to avoid any data breaches and improper data sharing in days to come.

Moreover, during the crisis itself, it is crucial to respect and act accordingly to stakeholders' expectations of the way managers should deal with the situation, which are based on the attributions they made regarding the origins of the crisis. There are numerous strategies that can be selected, depending on the type of crisis, the veracity of evidence, the damage and a company's past performance (Coombs, 1995). Also, it is crucial to cover all media channels in which information could erroneously spread, namely social media. Facebook should have made an analysis a priori of the most appropriate response strategy to follow, which it has not, thus leading to a rapid reputation loss. When the CA story broke years ago, Mark Zuckerberg's initial response was a long and deafening silence. It took five days for the founder and CEO of Facebook, to emerge from his Menlo Park quarters and talk to the public. When he finally did, he did so with great enthusiasm, addressing several talking points, from his own Facebook page to the conventional press to Congress. He announced several initiatives in order to prevent such data leaks in the future. The young entrepreneur kept apologizing in what seemed to create a huge list of regrets, but the company's reputation was and is still at stake.

After the crisis, it is important to follow up with everyone involved, outside the company as well as inside, in an attempt to learn from previous mistakes. At this stage, Facebook has to look to what they've have done, determine mistakes and find ways to strengthen its communication strategy.

2.6. Case Appendices

Appendix 1. Monthly active Facebook users worldwide (Statista, 2019).



Appendix 2. Zuckerberg' FB post (Facebook, 2006).

Calm down. Breathe. We hear you.

6 de setembro de 2006 às 06:45

We've been getting a lot of feedback about Mini-Feed and News Feed. We think they are great products, but we know that many of you are not immediate fans, and have found them overwhelming and cluttered. Other people are concerned that non-friends can see too much about them. We are listening to all your suggestions about how to improve the product; it's brand new and still evolving.

We're not oblivious of the Facebook groups popping up about this (by the way, Ruchi is not the devil). And we agree, stalking isn't cool; but being able to know what's going on in your friends' lives is. This is information people used to dig for on a daily basis, nicely reorganized and summarized so people can learn about the people they care about. You don't miss the photo album about your friend's trip to Nepal. Maybe if your friends are all going to a party, you want to know so you can go too. Facebook is about real connections to actual friends, so the stories coming in are of interest to the people receiving them, since they are significant to the person creating them.

We didn't take away any privacy options. [Your privacy options remain the same.] The privacy rules haven't changed. None of your information is visible to anyone who couldn't see it before the changes. If you turned off your wall to non-friends, no one who is not your friend will be able to see a post on your wall. Your friends can still see it; it hasn't changed. Secret groups and secret events remain secret from other people. Pokes and messages remain as private interactions. Nothing you do is being broadcast; rather, it is being shared with people who care about what you do—your friends.

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. Use your privacy settings so you can feel most comfortable using the site.

We hear you, and we appreciate the feedback.

Stay tuned... Mark

   227

0 comentários 17 partilhas

Appendix 3. Zuckerberg' FB post (Facebook, 2007).

Thoughts on Beacon

5 de dezembro de 2007 às 16:00

About a month ago, we released a new feature called Beacon to try to help people share information with their friends about things they do on the web. We've made a lot of mistakes building this feature, but we've made even more with how we've handled them. We simply did a bad job with this release, and I apologize for it. While I am disappointed with our mistakes, we appreciate all the feedback we have received from our users. I'd like to discuss what we have learned and how we have improved Beacon.

When we first thought of Beacon, our goal was to build a simple product to let people share information across sites with their friends. It had to be lightweight so it wouldn't get in people's way as they browsed the web, but also clear enough so people would be able to easily control what they shared. We were excited about Beacon because we believe a lot of information people want to share isn't on Facebook, and if we found the right balance, Beacon would give people an easy and controlled way to share more of that information with their friends.

But we missed the right balance. At first we tried to make it very lightweight so people wouldn't have to touch it for it to work. The problem with our initial approach of making it an opt-out system instead of opt-in was that if someone forgot to decline to share something, Beacon still went ahead and shared it with their friends. It took us too long after people started contacting us to change the product so that users had to explicitly approve what they wanted to share. Instead of acting quickly, we took too long to decide on the right solution. I'm not proud of the way we've handled this situation and I know we can do better.

Facebook has succeeded so far in part because it gives people control over what and how they share information. This is what makes Facebook a good utility, and in order to be a good feature, Beacon also needs to do the same. People need to be able to explicitly choose what they share, and they need to be able to turn Beacon off completely if they don't want to use it.

This has been the philosophy behind our recent changes. Last week we changed Beacon to be an opt-in system, and today we're releasing a privacy control to turn off Beacon completely. You can find it [here](#). If you select that you don't want to share some Beacon actions or if you turn off Beacon, then Facebook won't store those actions even when partners send them to Facebook.

On behalf of everyone working at Facebook, I want to thank you for your feedback on Beacon over the past several weeks and hope that this new privacy control addresses any remaining issues we've heard about from you.

Thanks for taking the time to read this.

Mark

Appendix 4. Zuckerberg's FB post (Facebook, 2011).

Our Commitment to the Facebook Community

29 de novembro de 2011 às 18:39

I founded Facebook on the idea that people want to share and connect with people in their lives, but to do this everyone needs complete control over who they share with at all times.

This idea has been the core of Facebook since day one. When I built the first version of Facebook, almost nobody I knew wanted a public page on the internet. That seemed scary. But as long as they could make their page private, they felt safe sharing with their friends online. Control was key. With Facebook, for the first time, people had the tools they needed to do this. That's how Facebook became the world's biggest community online. We made it easy for people to feel comfortable sharing things about their real lives.

We've added many new tools since then: sharing photos, creating groups, commenting on and liking your friends' posts and recently even listening to music or watching videos together. With each new tool, we've added new privacy controls to ensure that you continue to have complete control over who sees everything you share. Because of these tools and controls, most people share many more things today than they did a few years ago.

Overall, I think we have a good history of providing transparency and control over who can see your information.

That said, I'm the first to admit that we've made a bunch of mistakes. In particular, I think that a small number of high profile mistakes, like Beacon four years ago and poor execution as we transitioned our privacy model two years ago, have often overshadowed much of the good work we've done.

I also understand that many people are just naturally skeptical of what it means for hundreds of millions of people to share so much personal information online, especially using any one service. Even if our record on privacy were perfect, I think many people would still rightfully question how their information was protected. It's important for people to think about this, and not one day goes by when I don't think about what it means for us to be the stewards of this community and their trust.

Facebook has always been committed to being transparent about the information you have stored with us – and we have led the internet in building tools to give people the ability to see and control what they share.

But we can also always do better. I'm committed to making Facebook the leader in transparency and control around privacy.

As we have grown, we have tried our best to listen closely to the people who use Facebook. We also work with regulators, advocates and experts to inform our privacy practices and policies. Recently, the US Federal Trade Commission established agreements with Google and Twitter that are helping to shape new privacy standards for our industry. Today, the FTC announced [a similar agreement with Facebook](#). These agreements create a framework for how companies should approach privacy in the United States and around the world.

For Facebook, this means we're making a clear and formal long-term commitment to do the things we've always tried to do and planned to keep doing -- giving you tools to control who can see your information and then making sure only those people you intend can see it.

In the last 18 months alone, we've announced more than 20 new tools and resources designed to give you more control over your Facebook experience. Some of the things these include are:

- An easier way to [select your audience](#) when making a new post
- [Inline privacy controls](#) on all your existing posts
- The [ability to review tags](#) made by others before they appear on your profile
- [Friend lists](#) that are easier to create and that maintain themselves automatically
- A [new groups product](#) for sharing with smaller sets of people
- A tool to view your profile as someone else would see it
- Tools to ensure your information stays secure like [double login approval](#)
- [Mobile versions](#) of your privacy controls
- An easy way to download all your Facebook data
- A [new apps dashboard](#) to control what your apps can access
- A [new app permission dialog](#) that gives you clear control over what an app can do anytime you add one
- Many more [privacy education resources](#)

As a matter of fact, privacy is so deeply embedded in all of the development we do that every day tens of thousands of servers worth of computational resources are consumed checking to make sure that on any webpage we serve, that you have access to see each of the sometimes hundreds or even thousands of individual pieces of information that come together to form a Facebook page. This includes everything from every post on a page to every tag in those posts to every mutual friend shown when you hover over a person's name. We do privacy access checks literally tens of billions of times each day to ensure we're enforcing that only the people you want see your content. These privacy principles are written very deeply into our code.

Even before the agreement announced by the FTC today, Facebook had already proactively addressed many of the concerns the FTC raised. For example, their complaint to us mentioned our Verified Apps Program, which we canceled almost two years ago in December 2009. The same complaint also mentions cases where advertisers inadvertently received the ID numbers of some users in referrer URLs. We fixed that problem over a year ago in May 2010.

In addition to these product changes, the FTC also recommended improvements to our internal processes. We've embraced these ideas, too, by agreeing to improve and formalize the way we do privacy review as part of our ongoing product development process. As part of this, we will establish a biennial independent audit of our privacy practices to ensure we're living up to the commitments we make.

Even further, effective today I am creating two new corporate officer roles to make sure our commitments will be reflected in what we do internally -- in the development of our products and the security of our systems -- and externally -- in the way we work collaboratively with regulators, government agencies and privacy groups from around the world:

- Erin Egan will become Chief Privacy Officer, Policy. Erin recently joined Facebook after serving as a partner and co-chair of the global privacy and data security practice of Covington & Burling, the respected international law firm. Throughout her career, Erin has been deeply involved in legislative and regulatory efforts to address privacy, data security, spam, spyware and other consumer protection issues. Erin will lead our engagement in the global public discourse and debate about online privacy and ensure that feedback from regulators, legislators, experts and academics from around the world is incorporated into Facebook's practices and policies.

- Michael Richter will become Chief Privacy Officer, Products. Michael is currently Facebook's Chief Privacy Counsel on our legal team. In his new role, Michael will join our product organization to expand, improve and formalize our existing program of internal privacy review. He and his team will work to ensure that our principles of user control, privacy by design and transparency are integrated consistently into both Facebook's product development process and our products themselves.

These two positions will further strengthen the processes that ensure that privacy control is built into our products and policies. I'm proud to have two such strong individuals with so much privacy expertise serving in these roles.

Today's announcement formalizes our commitment to providing you with control over your privacy and sharing -- and it also provides protection to ensure that your information is only shared in the way you intend. As the founder and CEO of Facebook, I look forward to working with the Commission as we implement this agreement. It is my hope that this agreement makes it clear that Facebook is the leader when it comes to offering people control over the information they share online.

Finally, I also want to reaffirm the commitment I made when I first launched Facebook. We will serve you as best we can and work every day to provide you with the best tools for you to share with each other and the world. We will continue to improve the service, build new ways for you to share and offer new ways to protect you and your information better than any other company in the world.

Important Message from Facebook's White Hat Program

21 de junho de 2013 às 21:50

At Facebook, we take people's privacy seriously, and we strive to protect people's information to the very best of our ability. We implement many safeguards, hire the brightest engineers and train them to ensure we have only high-quality code behind the scenes of your Facebook experiences. We even have teams that focus exclusively on preventing and fixing privacy-related technical issues before they affect you.

Even with a strong team, no company can ensure 100% prevention of bugs, and in rare cases we don't discover a problem until it has already affected a person's account. This is one of the reasons we also have a [White Hat program](#) to collaborate with external security researchers and help us ensure that we maintain the highest security standards for our users.

We recently received a report to our White Hat program regarding a bug that may have allowed some of a person's contact information (email or phone number) to be accessed by people who either had some contact information about that person or some connection to them.

Describing what caused the bug can get pretty technical, but we want to explain how it happened. When people upload their contact lists or address books to Facebook, we try to match that data with the contact information of other people on Facebook in order to generate friend recommendations. For example, we don't want to recommend that people invite contacts to join Facebook if those contacts are already on Facebook; instead, we want to recommend that they invite those contacts to be their friends on Facebook.

Because of the bug, some of the information used to make friend recommendations and reduce the number of invitations we send was inadvertently stored in association with people's contact information as part of their account on Facebook. As a result, if a person went to download an archive of their Facebook account through our Download Your Information (DYI) tool, they may have been provided with additional email addresses or telephone numbers for their contacts or people with whom they have some connection. This contact information was provided by other people on Facebook and was not necessarily accurate, but was inadvertently included with the contacts of the person using the DYI tool.

After review and confirmation of the bug by our security team, we immediately disabled the DYI tool to fix the problem and were able to turn the tool back on the next day once we were satisfied that the problem had been fixed.

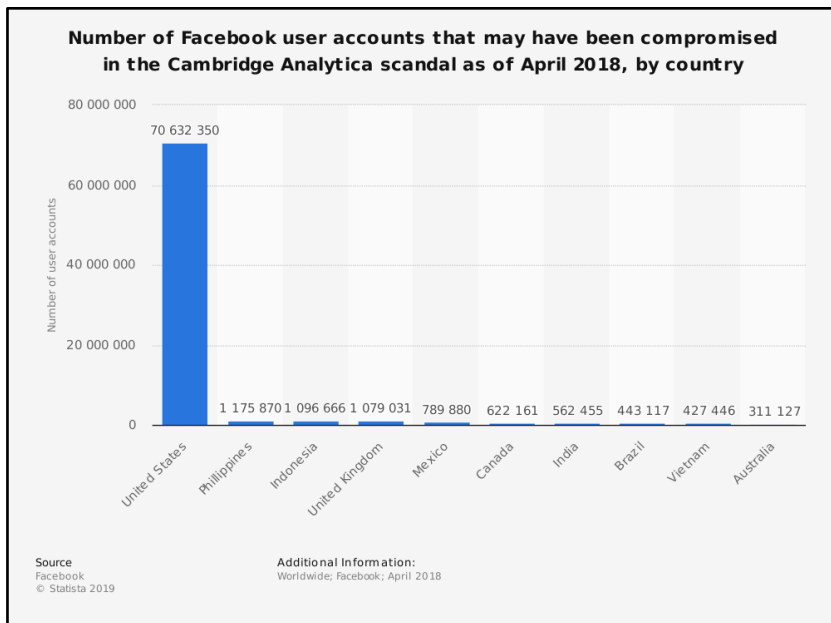
We've concluded that approximately 6 million Facebook users had email addresses or telephone numbers shared. There were other email addresses or telephone numbers included in the downloads, but they were not connected to any Facebook users or even names of individuals. For almost all of the email addresses or telephone numbers impacted, each individual email address or telephone number was only included in a download once or twice. This means, in almost all cases, an email address or telephone number was only exposed to one person. Additionally, no other types of personal or financial information were included and only people on Facebook – not developers or advertisers – have access to the DYI tool.

We currently have no evidence that this bug has been exploited maliciously and we have not received complaints from users or seen anomalous behavior on the tool or site to suggest wrongdoing. Although the practical impact of this bug is likely to be minimal since any email address or phone number that was shared was shared with people who already had some of that contact information anyway, or who had some connection to one another, it's still something we're upset and embarrassed by, and we'll work doubly hard to make sure nothing like this happens again. Your trust is the most important asset we have, and we are committed to improving our safety procedures and keeping your information safe and secure.


We have already notified our regulators in the US, Canada and Europe, and we are in the process of notifying affected users via email.

We appreciate the security researcher's report to our White Hat program, and have paid out a bug bounty to thank him for his efforts.

Appendix 6. Number of users affected (Statista, 2018).



Appendix 7. Mark Zuckerberg's post (Facebook, 2018a, March 21).



Mark Zuckerberg ✓
21 de março de 2018 · Menlo Park, Estados Unidos da América · 🌐

Seguir

I want to share an update on the Cambridge Analytica situation -- including the steps we've already taken and our next steps to address this important issue.

We have a responsibility to protect your data, and if we can't then we don't deserve to serve you. I've been working to understand exactly what happened and how to make sure this doesn't happen again. The good news is that the most important actions to prevent this from happening again today we have already taken years ago. But we also made mistakes, there's more to do, and we need to step up and do it.

Here's a timeline of the events:

In 2007, we launched the Facebook Platform with the vision that more apps should be social. Your calendar should be able to show your friends' birthdays, your maps should show where your friends live, and your address book should show their pictures. To do this, we enabled people to log into apps and share who their friends were and some information about them.

In 2013, a Cambridge University researcher named Aleksandr Kogan created a personality quiz app. It was installed by around 300,000 people who shared their data as well as some of their friends' data. Given the way our platform worked at the time this meant Kogan was able to access tens of millions of their friends' data.

In 2014, to prevent abusive apps, we announced that we were changing the entire platform to dramatically limit the data apps could access. Most importantly, apps like Kogan's could no longer ask for data about a person's friends unless their friends had also authorized the app. We also required developers to get approval from us before they could request any sensitive data from people. These actions would prevent any app like Kogan's from being able to access so much data today.

In 2015, we learned from journalists at The Guardian that Kogan had shared data from his app with Cambridge Analytica. It is against our policies for developers to share data without people's consent, so we immediately banned Kogan's app from our platform, and demanded that Kogan and Cambridge Analytica formally certify that they had deleted all improperly acquired data. They provided these certifications.

Last week, we learned from The Guardian, The New York Times and Channel 4 that Cambridge Analytica may not have deleted the data as they had certified. We immediately banned them from using any of our services. Cambridge Analytica claims they have already deleted the data and has agreed to a forensic audit by a firm we hired to confirm this. We're also working with regulators as they investigate what happened.

This was a breach of trust between Kogan, Cambridge Analytica and Facebook. But it was also a breach of trust between Facebook and the people who share their data with us and expect us to protect it. We need to fix that.

In this case, we already took the most important steps a few years ago in 2014 to prevent bad actors from accessing people's information in this way. But there's more we need to do and I'll outline those steps here:

First, we will investigate all apps that had access to large amounts of information before we changed our platform to dramatically reduce data access in 2014, and we will conduct a full audit of any app with suspicious activity. We will ban any developer from our platform that does not agree to a thorough audit. And if we find developers that misused personally identifiable information, we will ban them and tell everyone affected by those apps. That includes people whose data Kogan misused here as well.




Second, we will restrict developers' data access even further to prevent other kinds of abuse. For example, we will remove developers' access to your data if you haven't used their app in 3 months. We will reduce the data you give an app when you sign in -- to only your name, profile photo, and email address. We'll require developers to not only get approval but also sign a contract in order to ask anyone for access to their posts or other private data. And we'll have more changes to share in the next few days.

Third, we want to make sure you understand which apps you've allowed to access your data. In the next month, we will show everyone a tool at the top of your News Feed with the apps you've used and an easy way to revoke those apps' permissions to your data. We already have a tool to do this in your privacy settings, and now we will put this tool at the top of your News Feed to make sure everyone sees it.

Beyond the steps we had already taken in 2014, I believe these are the next steps we must take to continue to secure our platform.

I started Facebook, and at the end of the day I'm responsible for what happens on our platform. I'm serious about doing what it takes to protect our community. While this specific issue involving Cambridge Analytica should no longer happen with new apps today, that doesn't change what happened in the past. We will learn from this experience to secure our platform further and make our community safer for everyone going forward.

I want to thank all of you who continue to believe in our mission and work to build this community together. I know it takes longer to fix all these issues than we'd like, but I promise you we'll work through this and build a better service over the long term.

   272 mil

53 mil comentários 67 mil partilhas

Appendix 8. Sheryl Sandberg's post (Facebook, 2018b, March 21).



Sheryl Sandberg ✓
21 de março de 2018 · 🌐

Seguir

Sharing Mark's post addressing the Cambridge Analytica news. As he said, we know that this was a major violation of people's trust, and I deeply regret that we didn't do enough to deal with it. We have a responsibility to protect your data - and if we can't, then we don't deserve to serve you.

We've spent the past few days working to get a fuller picture so we can stop this from happening again. Here are the steps we're taking. We're investigating all apps that had access to large amounts of information before we changed our platform in 2014 to dramatically reduce data access. And if we find that developers misused personally identifiable information, we'll ban them from our platform and we'll tell the people who were affected.

We're also taking steps to reduce the data you give an app when you use Facebook login to your name, profile photo, and email address. And we'll make it easier for you to understand which apps you've allowed to access your data.

You deserve to have your information protected - and we'll keep working to make sure you feel safe on Facebook. Your trust is at the core of our service. We know that and we will work to earn it.



Mark Zuckerberg ✓
21 de março de 2018 · Menlo Park, Estados Unidos da América

I want to share an update on the Cambridge Analytica situation -- including the steps we've already taken and our next steps to address this important issue.

March 21, 2018

Cracking Down on Platform Abuse

“

We have a responsibility to everyone who uses Facebook to make sure their privacy is protected.

”

Protecting people’s information is the most important thing we do at Facebook. What happened with Cambridge Analytica was a breach of Facebook’s trust. More importantly, it was a breach of the trust people place in Facebook to protect their data when they share it. As Mark Zuckerberg [explained in his post](#), we are announcing some important steps for the future of our platform. These steps involve taking action on potential past abuse and putting stronger protections in place to prevent future abuse.

People use Facebook to connect with friends and others using all kinds of apps. Facebook’s platform helped make apps social — so your calendar could show your friends’ birthdays, for instance. To do this, we allowed people to log into apps and share who their friends were and some information about them.

As people used the Facebook platform in new ways, we strengthened the rules. We required that developers get people’s permission before they access the data needed to run their apps – for instance, a photo sharing app has to get specific permission from you to access your photos. Over the years we’ve introduced more guardrails, including in 2014, when we began [reviewing](#) apps that request certain data before they could launch, and introducing more granular controls for people to decide what information to share with apps. These actions would prevent any app like Aleksandr Kogan’s from being able to access so much data today.

Even with these changes, we've seen abuse of our platform and the misuse of people's data, and we know we need to do more. We have a responsibility to everyone who uses Facebook to make sure their privacy is protected. That's why we're making changes to prevent abuse. We're going to set a higher standard for how developers build on Facebook, what people should expect from them, and, most importantly, from us. We will:

1. **Review our platform.** We will investigate all apps that had access to large amounts of information before we changed our platform in 2014 to reduce data access, and we will conduct a full audit of any app with suspicious activity. If we find developers that misused personally identifiable information, we will ban them from our platform.
2. **Tell people about data misuse.** We will tell people affected by apps that have misused their data. This includes building a way for people to know if their data might have been accessed via "thisisyourdigitallife." Moving forward, if we remove an app for misusing data, we will tell everyone who used it.
3. **Turn off access for unused apps.** If someone hasn't used an app within the last three months, we will turn off the app's access to their information.
4. **Restrict Facebook Login data.** We are changing Login, so that in the next version, we will reduce the data that an app can request without app review to include only name, profile photo and email address. Requesting any other data will require our approval.
5. **Encourage people to manage the apps they use.** We already show people what apps their accounts are connected to and control what data they've permitted those apps to use. Going forward, we're going to make these choices more prominent and easier to manage.
6. **Reward people who find vulnerabilities.** In the coming weeks we will expand Facebook's [bug bounty program](#) so that people can also report to us if they find misuses of data by app developers.

There's more work to do, and we'll be sharing details in the coming weeks about additional steps we're taking to put people more in control of their data. Some of these updates were already in the works, and some are related to new data protection laws coming into effect in the EU. This week's events have accelerated our efforts, and these changes will be the first of many we plan to roll out to protect people's information and make our platform safer.

Facebook

Pursuing Forensic Audits to Investigate Cambridge Analytica Claims

March 19, 2018

“

We remain committed to vigorously enforcing our policies to protect people’s information.

”

Update on March 19, 2018, 3:25 PM PT: Independent forensic auditors from Stroz Friedberg were on site at Cambridge Analytica's London office this evening. At the request of the UK Information Commissioner's Office, which has announced it is pursuing a warrant to conduct its own on-site investigation, the Stroz Friedberg auditors stood down.

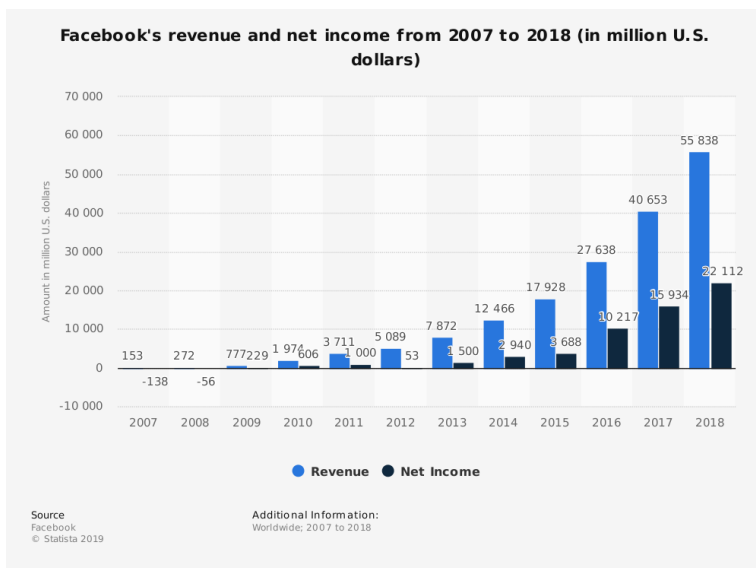
Originally published March 19, 2018, 11:40 AM PT:

We have hired a digital forensics firm, Stroz Friedberg, to conduct a comprehensive audit of Cambridge Analytica. Cambridge Analytica has agreed to comply and afford the firm complete access to their servers and systems. We have approached the other parties involved — Christopher Wylie and Aleksandr Kogan — and asked them to submit to an audit as well. Mr. Kogan has given his verbal agreement to do so. Mr. Wylie thus far has declined.

This is part of a comprehensive internal and external review that we are conducting to determine the accuracy of the claims that the Facebook data in question still exists. This is data Cambridge Analytica, SCL, Mr. Wylie, and Mr. Kogan certified to Facebook had been destroyed. If this data still exists, it would be a grave violation of Facebook's policies and an unacceptable violation of trust and the commitments these groups made.

We are moving aggressively to determine the accuracy of these claims. We remain committed to vigorously enforcing our policies to protect people's information. We also want to be clear that today when developers create apps that ask for certain information from people, we conduct a robust review to identify potential policy violations and to assess whether the app has a legitimate use for the data. We actually reject a significant number of apps through this process. Kogan's app would not be permitted access to detailed friends' data today.

Appendix 11. Facebook's numbers (Statista, 2018).



Appendix 12. Paul Grewal blog post (Facebook Newsroom, 2019).

By Paul Grewal, Vice President and Deputy General Counsel

Today we are agreeing with the District of Columbia Attorney General to jointly make public a September 2015 document in which Facebook employees discuss public data scraping. We believe this document has the potential to confuse two different events surrounding our knowledge of Cambridge Analytica. There is no substantively new information in this document and the issues have been previously reported. As we have said many times, [including last week](#) to a British parliamentary committee, these are two distinct issues. One involved unconfirmed reports of scraping — accessing or collecting public data from our products using automated means — and the other involved policy violations by Aleksandr Kogan, an app developer who sold user data to Cambridge Analytica. This document proves the issues are separate; conflating them has the potential to mislead people.

Facebook was not aware that Kogan sold data to Cambridge Analytica until December 2015. That is a fact that we have testified to under oath, that we have described to our core regulators, and that we stand by today.

Here is the timeline: In September 2015, a Facebook employee shared unsubstantiated rumors from a competitor of Cambridge Analytica, which claimed that the data analytics company was scraping public data. This was the kind of data that you can see on someone's Facebook profile even if you are not friends with them, a serious but frequent problem across the internet. An engineer looked into this concern and was not able to find evidence of data scraping. Even if such a report had been confirmed, such incidents would not naturally indicate the scale of the misconduct that Kogan had engaged in.

The first indication of Kogan's involvement didn't come until December 2015, three months later. That incident involved Kogan's now widely known and unauthorized sale of data to Cambridge Analytica.

Cambridge Analytica was a clear lapse for us, which we have worked hard to address. We've learned many lessons that will help us become a stronger company going forward.

3. Teaching Note

3.1. Teaching Objectives

The present case study is designed to present Master or MBA students with a real crisis event scenario, in the context of a Brand Management and Strategy course or, in less broad disciplines, for instance, Brand Communications and Digital Marketing. The mission is to trigger their analytical and problem-solving capabilities and to make them apply their theoretical expertise in practice.

The case study was outlined to fit in one academic hour lecture with length of up to three hours, which can be adapted depending on the questions chosen for discussion. For students to be able to participate in the in-class discussion actively, students should do their own preparation at home, starting by reading the case and make an attempt of answering to the suggested assignment questions, which intend to help meet the following objectives:

1. To familiarize students with a reputation crisis event.
2. To present the notion of “Crisis communication” and encourage the understanding of the three phases that integrate it.
3. To present the topic of “Attribution Theory”.
4. To present students with different types of corporate crisis response strategies.
5. To introduce a crisis communication tool – crisis teams, which should facilitate communication between companies and their stakeholders.
6. To highlight the importance of “Issue management” and identify paths to avoid future crisis events.

3.2. Introduction

The Facebook case study was prepared by Raquel Duarte, under Professor’s Daniela Langaro supervision, within the scope of the Brands in Digital and Social Media Marketing seminar at Católica-Lisbon School of Business and Economics.

The case was written for teaching purposes, aiming to assist instructors to achieve a set of learning goals, by placing each of their students in the role of a CMO of one of the largest companies worldwide, confronted with an intriguing marketing dilemma.

Even though all the events related in the case study are real, it should not be used as a source of primary data or as a reference.

3.3.Synopsis

Facebook's is a free social network that allows people to create profiles, upload image and video content, send messages and keep in touch. It was born in 2004 and since then has known nothing but growth. Nonetheless, due to the lack of regulations and inaccurate privacy policies, it has been the object of several controversies regarding its capability of protecting users' data. Recently the social media giant has faced one of the biggest reputation crises ever and was faced with a declining reputation and trust from stakeholders. Zuckerberg, the company's CEO, apologized innumerous times for what happened but there was a need to resort to stricter measures in order to respond to such an event.

3.4. Suggested assignment questions

The proposed assignment questions aim at leading students through their analysis of the case, in order to generate an in-class debate on crisis-related topics. To that end, students are expected to deal with the following questions:

1. How did Facebook manage communications along the crisis?
2. What was the level of Damage associated with this crisis? Who are the stakeholders affected, and how was the crisis perceived by them?
3. How would you react if you were the CMO of Facebook?
4. Who should be the spokesperson in this case?
5. How would you avoid that this repeats in the future?

3.5. Literature Review

3.5.1. Crisis

Various definitions of organizational crisis have been proposed by authors. Gillespie and Dietz (2009) describe an organizational crisis as an “organization-level failure, as a single major incident, or cumulative series of incidents, resulting from the action of organizational agents that threatens the legitimacy of the organization and has the potential to harm the well-being of [...] the organization’s stakeholders”. Similarly, crisis is defined as “the perception of an unpredictable event that threatens important expectancies of stakeholders and can seriously impact an organization’s performance and generate negative outcomes” (Coombs, 2014). Accordingly, crisis are negative events that can pollute the positive aspects of an organization’s image (Coombs, 1995).

3.5.2. Crisis Management

In the literature, crisis management refers to a “a set of factors designed to combat crisis and to lessen the actual damages inflicted”. Moreover, it is a process that aims to prevent or mitigate the bad outcomes of a crisis and by that protect the stakeholders, organization and even the industry from possible damage (Coombs, 2014). One of the many tasks of the crisis manager is to do its best to protect the existent positive facets of an organization’s image (Sturges, 1994).

A very important theory in conceptualizing the concept of “crisis management” is Attribution Theory. The latter postulates that individuals make judgements about the causes of crisis events based upon three dimensions: locus, stability and controllability (Weiner, 1974). Locus concerns the locus of control, whether the crisis was caused by an internal or external player. As for stability, it takes into consideration the permanence of the event. Regarding controllability, it refers to the ability of the actor to control or not the cause of the event.

The crisis management process can be organized around three phases: pre-crisis, crisis, and post-crisis. Good crisis communication is at the heart of an effective process, as any crisis event rises a need for information. The term has been used by Coombs (2010a) to refer to the “(...) collection, processing, and dissemination of information required to address a crisis situation.”.

Pre-crisis communication includes efforts to prevent, detect and prepare for crisis, such as the collection of information about crisis risks and training people who will be involved in the process (e.g., crisis spokespersons) (Coombs, 2010a). In this phase, another concept that pops up is “Issues management”, which has a reciprocal relationship with crisis management. It involves “a strategic set of functions used to reduce friction and increase harmony between organizations and their publics in the public policy arena” (Heath, 2005). As indicated by this definition, effective issues management is a form of crisis prevention (Coombs, 2014). By identifying embryonic issues, crisis managers can act before it develops into a mature crisis. “Risk Management” is another important concept in this phase, as it can help prevent a crisis. The majority of the analysis done by crisis managers is conceived to detect risks before they convert into something massive. On its side, crisis preparation is guided by risks assessments (Williams & Olaniran, 1998). Communicating risks among the organization is also a crucial element in the pre-crisis phase as organizations can demonstrate to risk bearers that they are taking responsibility for it and putting efforts on managing it (Coombs, 2010b).

The crisis communication phase is the recognition of the trigger event and the actual response to it (Coombs, 2010a). Risk communication is also needed in the crisis response phase (Coombs, 2010b), to enlighten all the involved players about the current situation. At this point, the goal is to act fast, to be accurate and consistent (Coombs, 2010a). Indeed, experts highlighted that a quick response is given within the first hour after the publics get knowledge of the crisis event (Barton, 2001). Moreover, the Web has only intensified the need for the rapid spread of news and information. A failure to comply with this opens space for others to control and frame the crisis event in their own way, affecting the perceptions of the stakeholders (Brummett, 1980). Likewise, research has validated that when the organization is the information source, there is less reputational harm than if media step in first in delivering the facts. This is called the “stealing thunder” effect (Arpan & Roskos-Ewoldsen, 2005) and proves that silence is not a way out. Moreover, providing accurate information and being consistent creates credibility and protects stakeholders.

As for post-crisis communication, it involves efforts to follow-up with stakeholders and learning from the crisis (Coombs, 2010a). Risk information and concerns are, here again, a part of the communicative needs after the crisis (Coombs, 2010b). Mitroff et al. (1996) have highlighted the need to learn from the crisis, but others have reported that organizations are averse to learn from these negative events (Roux-Dufort, 2000). In fact, people tend to get

watchful and to resist crisis investigations for the simple reason that they feel threatened by a possible attribution of blame or punishment. Thus, learning must not be blame oriented and be rewarded (Coombs, 2010a).

Besides the three mentioned phases, there are two types of crisis communication that are helpful to distinguish: crisis knowledge management, that is all about creating knowledge, going from identifying the crisis sources to decision making, and stakeholder reaction management, that involves communicative efforts (words and actions) to influence the perceptions of stakeholders about the crisis event (Coombs, 2010a).

3.5.3. Reputation management

Reputation is the “aggregate evaluation constituents make about how well an organization is meeting constituent expectations based on its past behaviors” (Wartick 1992). An organization is rewarded with a strong reputation depending on how well it meets certain criteria and/or stakeholder’s expectations. All interactions with an organization, whether in person or any other communication channel are integrated into stakeholder’s mind creating an album of memories that weight in their vision in unexpected events such as crisis. Therefore, reputation is a critical resource for any organization.

Maintaining a good reputation is thereby one of any organization’s main concerns. That is why Reputation Management is so important. In broad, it involves efforts to shape how stakeholders perceive the organization with the purpose of creating benign impressions. It may involve advertising “the good points” about an organization, for instance (Coombs, 2010b).

Any crisis menaces an organization’s reputation (Barton 2001). Part of the crisis phase is dedicated to reputation repair, the latter being a vital resource that must be protected. A persuasive crisis communication minimizes a crisis’ consequent reputational damage and sets the base for repairing the caused damage (Coombs, 2010b). Also, reputation building prior to a crisis is beneficial to an organization in this kind of scenario (Coombs & Holladay 2002). Indeed, a prior negative reputation just slows down the eventual positive outcomes of the reputation repair efforts. This reaction is called the Velcro effect (Coombs & Holladay, 2006). The inverse situation may also occur, a positive reputation favoring the recovery of an organization’s after the event. Here, the organization is given the benefit of the doubt.

3.5.4. Information breaches

Information breaches are here concerned. An information breach can be defined as the “malpractice of unauthorized access to personal information of a group of individuals” (Culnan & Williams, 2009). A recent review of literature on this matter found that from 2006 to 2015, according to the DatalossDB.org database, the number of breaches increased from 643 to over 1500 annually (Rasoulia et al., 2017).

Any stakeholder’s basic expectation is that it can trust an organization to protect its data (Carroll 1991). Besides, data privacy protection is a key element of every organization’s service quality (Yang & Fang 2004). A gap in these expectations can lead to a huge service crisis, with substantial media attention. Due to its intangibility, it may take some time to figure out the nature of a breach, and once the information is revealed, there is no way back on restoring the loss of privacy (Malhotra & Malhotra, 2010), taking down an organization’s legitimacy and reputation.

Information breaches have enough magnitude to influence responses of investors (Campbell et al. 2003), one of the most important capital sources of an organization. An important concept is idiosyncratic risk (or unsystematic risk), which stands for the firm-specific volatility of stock return. This volatility is influenced by micro firm-level factors, such as marketing strategies (Goyal et al., 2003). Hence, besides being reflective of the effectiveness of an organization’s marketing strategies (Rust et al. 2004), idiosyncratic risk leads to understanding the financial impact of service crisis recoveries in investors’ investment portfolios.

3.5.5. Crisis classifications

In his paper of 1995, Coombs noted the existence of several elements that influence the way publics, i.e., the parties involved, react and perceive a crisis situation: the crisis type, the veracity of evidence, the damage, and the performance history. In broad, there are four types of crisis, that lean on two dimensions. The first dimension regards the internal or external origin of the crisis, meaning if it was caused by the organization itself or by a person or group outside it. The internal-external dimension relates to the locus of control dimension of AT. As for the second dimension, it encompasses whereas the crisis event was committed intentionally or unintentionally. The intentional-unintentional dimension relates to the controllability

dimension of AT. To summarize this, a matrix with the types of crisis was elaborated (*Table 1*).

	Unintentional	Intentional
External	Faux Pas	Terrorism
Internal	Accidents	Transgressions

Table 1. Types of Crisis (Coombs, 1995)

The “Faux Pas”, is an unintentional action that an external agent tries to transform into a crisis (e.g., a company is challenged by an outside group concerning the appropriateness of its products’ advertising). Accidents are another type of unintentional acts, that happen during the course of day-to-day operations and therefore lead to minimal organizational responsibility (e.g., employee injuries, natural disasters, product defects). On the other hand, transgressions are intentional actions incurred by an organization, placing publics at risk or harm (e.g., manipulating products in order to avoid governmental tests). Finally, there is “Terrorism”, which has the intentional side, except that the action is taken one or several external actors, with the objective of harming the organization directly (e.g., hurt employees) or indirectly (Ex: reduce sales) (Coombs, 1995).

As stated before, the type of crisis is not sufficient to affect the attribution publics make about a crisis. The term “**veracity of evidence**” (Coombs, 1995) usually refers to the proof of the actual existence of the crisis event. Such evidence can be either true, indicating that a crisis did happen, false (rumors), explained by the possible public circulation of crisis reports, and ambiguous. This last kind of evidence can only be found with faux pas, when questions of ethics and morality are at stake. For example, protests against an organization that legally conducts product testing on animals could create a faux pas. Here, there may be a disagreement on whether it is or is not acting appropriately and according to moral standards.

Another aspect that weights in crisis situations is the amount of **damage** associated with it, whether severe or minor (Coombs, 1995). Publics tend to ascribe more responsibility to the organizations when the level of damage is higher. This goes along with the notion that people hold others more personally responsible for negative actions than for positive ones (Griffin,

1997). Here, it is relevant to make a distinction between victims (those who suffer physically, mentally, or financially) and nonvictims.

Lastly, the organization's **performance history** (Coombs, 1995) is also an important factor in a crisis. An organization is worthy of trust if its past performance has been positive. Indeed, images are hard to change as publics attach to them (Grunig, 1993). Furthermore, publics are less likely to see the organization as guilty for the event since positive past actions make the cause of the crisis appear unstable (Griffin et al., 1991).

3.5.6. Impact of crisis on publics

The impact of the crisis should vary according to the importance publics give to the three AT dimensions. Depending on the level of responsibility each one gives to the organization, different feelings and behaviors will emerge among the ones that were affected by the crisis (Weiner, 1974). If larger responsibility is attributed to the organization, publics will have more negative images of it, and this will affect their actions towards it (Coombs, 1995). Therefore, it is crucial to identify who are the ones affected and define priorities concerning their importance and valence for the issue.

More and more, organizations collect and use customer data, but there is a growing resistance to these practices. This is because people feel vulnerable and this results in negative outcomes for organizations, such a negative stock performance and harming customer behaviors (e.g., faking information, disseminating negative word-of-mouth, switching behaviors, etc.) (Martin et al., 2017). In the context of a data breach, there is a complete violation of stakeholders' trust. The "Gossip Theory" may be introduced here. In broad, when people learn they are the target of gossip, they tend to react negatively (Baumeister et al., 2004). In the business context, applying this theory suggests that customer data vulnerability may lead to feelings of betrayal, emotional violation (Richman & Leary, 2009) and decreasing levels of trust (Turner et al. 2003). Transparency, i.e. the target's awareness of which information is being shared, and control, i.e. the extent to which the target believes (s)he can manage the flow of information, are two methods identified by the Gossip Theory, that help to eliminate the negative outcomes of unsanctioned transmissions of information.

Coombs and Holladay (2005) analyzed several crises and correlated the events with the generation of some feelings: anger, sympathy, and schadenfreude (taking joy in the pain of others). As expected, anger rises with attributions of crisis responsibility. The authors also examined the effect of these emotions on behavioral intentions, such as purchase intention and negative WOM. The latter is a troublemaker because its effects are very long-lasting. Messages posted online, for instance, can remain for years, while people's memory of a crisis fades after a few months.

3.5.7. Crisis recovery

There are a lot of difficulties associated with recovering from a service crisis. Crisis recovery can be broadly defined as an organization's attempts to amend and repair inconveniences to all the publics affected by the crisis. These will reassess the organization's trustworthiness, reputation and legitimacy based on their level of satisfaction with the recovery process (Aaker et al. 2004).

3.5.7.1 Crisis response strategies

Conforming to the RBT, effective crisis recoveries improve an organization's key resources, that is its relationships with its stakeholders, and/or enhances its capabilities (i.e., processes to protect data confidentiality). In turn, these stronger resources and capabilities balance the organization's future performance and cash flow.

Crisis situations diverge depending on how publics believe an organization is acting in the three dimensions of AT. Crisis response strategies aim to repair the damage caused by these attributions. A repertoire of crisis-response strategies, composed of messages that aim to repair organizational images, was mainly built on the works of Allen and Caillouet (1994). It is comprised of five categories: non-existence strategies, distance strategies, ingratiation strategies, mortification strategies and suffering strategies. Each of these strategies is composed of sub-strategies (*Table 2.*) that will be described below.

- **Non-existence strategies** attempt to eliminate the crisis. **Denial, clarification, attack** and **intimidation** are sub-types of non-existence strategies. Denying a crisis simply means stating that nothing happened, that there is no crisis at all (Coombs, 1995; Marcus & Goodman, 1991; Sharkey & Stafford, 1990). As for clarification, it undertakes the same

steps as in denial except that there an attempt of explaining why there is no crisis (Allen and Caillouet, 1994). With a more aggressive side, “attack” stems from confronting those who erroneously report that the non-existing crisis exists (Coombs, 1995; Metts & Cupach, 1989). Finally, intimidation is the most hostile strategy, knowing that it threatens to use organizational power (Ex: lawsuits or even physical violence) against the confronting players (Allen and Caillouet, 1994).

- **Distance strategies** recognize the crisis and attend to create public acceptance of the crisis while softening the connection between the organization and the crisis. “**Excuse**” is considered a DS as the organization minimizes its responsibility for the crisis through denial of intention and denial of volition (Coombs, 1995). On the same token, the **justification** strategy consists in minimizing the damage associated with the crisis (Metts & Cupach, 1989; Sharkey & Stafford, 1990). It may include denying the severity of an injury, alleging that the victim deserved what happened or that the event has been misinterpreted (Allen and Caillouet, 1994).
- **Ingratiation strategies** aspire to win public approval for the organization (Allen and Caillouet, 1994). **Bolstering** is about reminding publics of existing positive organization’s deeds (Ice, 1991), namely past charitable donations or a history of fair worker treatment. **Transcendence** strategy places the crisis in a preferable context (Coombs, 1995), appealing to values that the publics identify with (Allen and Caillouet, 1994). At last, **praising others** is also an IS as it refers to winning approval from publics, leading them to like the organization (Allen and Caillouet, 1994).
- **Mortification strategies’** goal is to win forgiveness and create acceptance for the crisis. **Remediation** is one way of pursuing this, that is offering some form of compensation or helping victims (money, goods, aid) (Marcus & Goodman, 1991; Sharkey & Stafford, 1990). Repentance implies asking for forgiveness (Sharkey & Stafford, 1990) and rectification means taking action to hinder a reoccurrence of the crisis in the future (Coombs, 1995).
- The **Suffering strategy** does not have any sub-strategy. The idea is to gain empathy from publics. Suffering represents the organization as an arbitrary victim of some malicious portrays the organization as an unfair victim of some outside actors.

Nonexistence Strategies	
<input type="checkbox"/>	Denial
<input type="checkbox"/>	Clarification
<input type="checkbox"/>	Attack
Distance Strategies	
<input type="checkbox"/>	Excuse
	○ Denial of intention
	○ Denial of volition
<input type="checkbox"/>	Justification
	○ Minimizing injury
	○ Victim deserving
	○ Misrepresentation of the crisis event
Ingratiation Strategies	
<input type="checkbox"/>	Bolstering
<input type="checkbox"/>	Transcendence
<input type="checkbox"/>	Praising Others
Mortification Strategies	
<input type="checkbox"/>	Remediation
<input type="checkbox"/>	Repentance
<input type="checkbox"/>	Rectification
Suffering Strategy	

Table 2. Crisis-Response Strategies (Coombs, 1995)

3.5.7.2. Select the correct crisis response strategy

Crisis response strategies are a very important source for crisis managers, they must select the most appropriate one. The decision process begins by identifying the crisis type, then the evidence, followed by the damage caused (victim status) and ending by analyzing the organization's performance history. In his work (Coombs, 1995), Coombs has provided a series of flowcharts for selecting crisis response strategies for each specific crisis situation (*Figures 1, 2, 3, 4*).

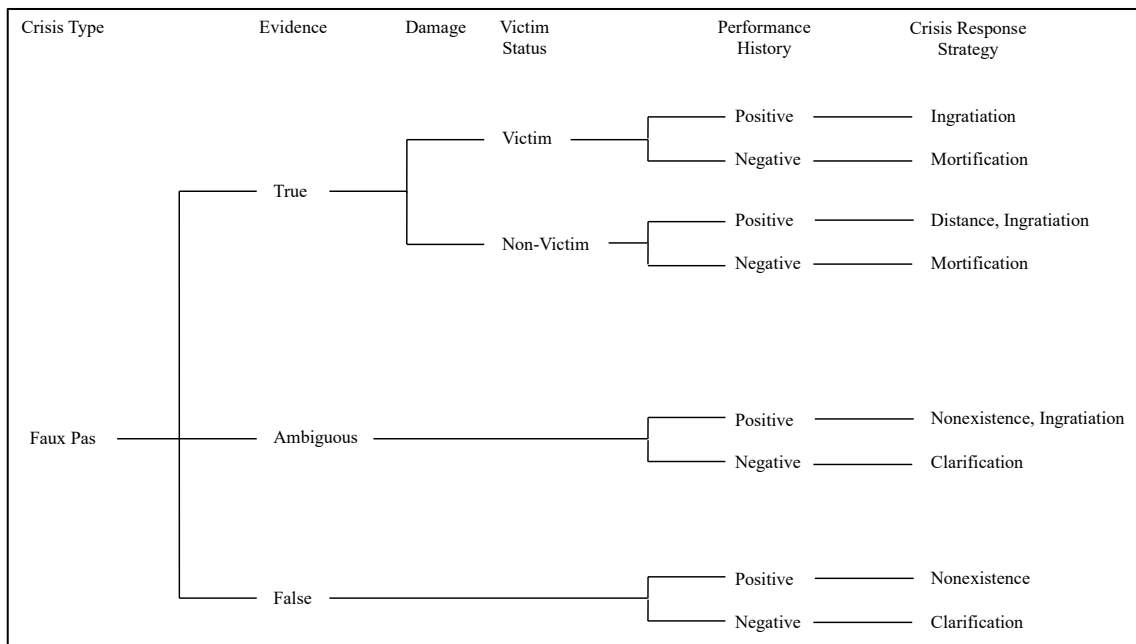


Figure 1. Faux Pas decision flowchart (Coombs, 1995, p.463)

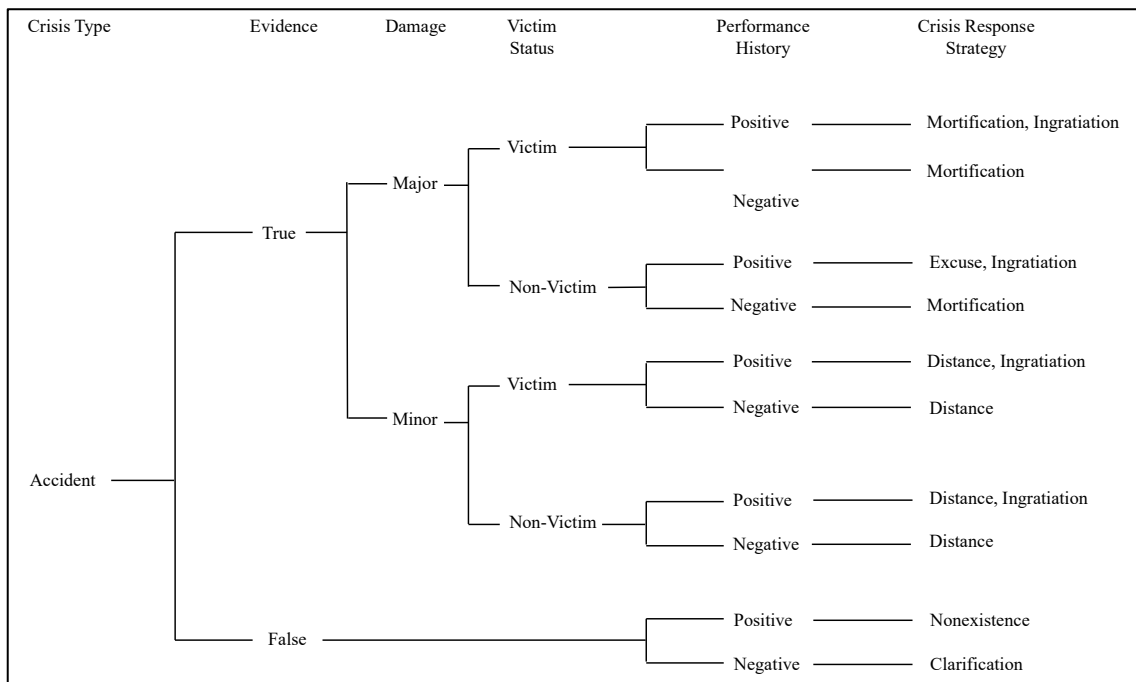


Figure 2. Accident decision flowchart (Coombs, 1995, p.465)

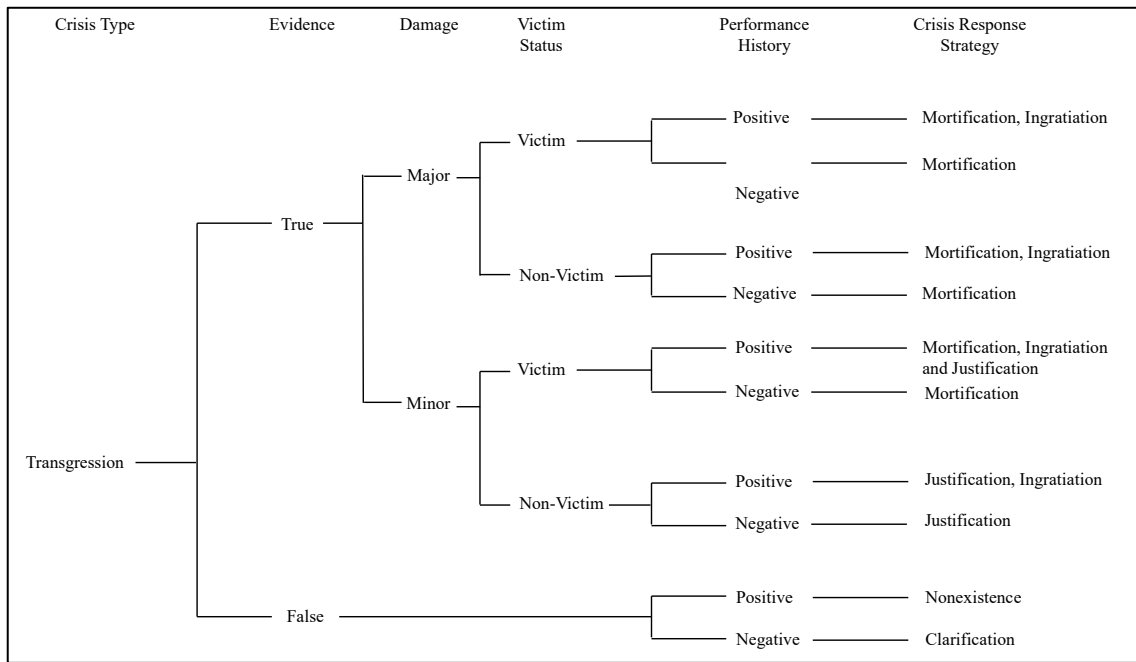


Figure 3. Transgression decision flowchart (Coombs, 1995, p.467)

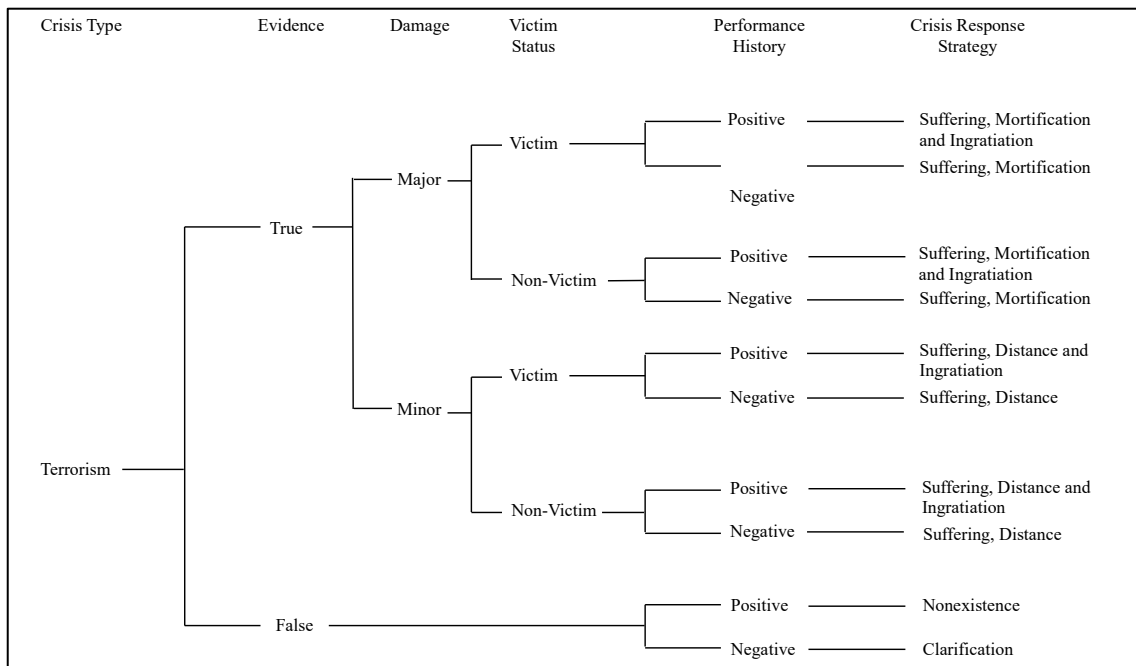


Figure 4. Terrorism decision flowchart (Coombs, 1995, p.468)

Crisis managers have to bear in mind that some strategies may directly affect the behavior of a specific type of stakeholder: investors. If a company's primary focus is to regain investor's trust during and after a crisis, it has to understand the payoffs of the following strategies: compensation, process improvement and apologies (Gelbrich & Roschk, 2011).

Justice theory advances that compensations increase stakeholders' satisfaction because of their perception of distributive justice. The term "distributive justice" means the appropriateness of the outcomes received by stakeholders after a service crisis (Gelbrich & Roschk, 2011). Hence, offering compensation helps to rebuild the relationships between the public and the organization. In the long-term, this has a positive effect on the organization's performance, that offsets the short-term costs of the compensation. Investors should interpret this as an effort of the organization of solidifying an important resource, the relationship with its stakeholders, that in the future will lead to cash flow stability, meaning lower idiosyncratic risk.

Regarding process improvement, it embodies a series of organization's actions that intend to reform its bad procedures in a way to avoid future failures (Gelbrich & Roschk, 2011).

In their analysis, Rasoulia et al. (2017) outline that an improvement of the process should lead to a competitive advantage, resulting in improved performance. Besides, it should improve stakeholder's perception of the organization's procedural justice, i.e., the appropriateness of the practices and policies put in place to serve the stakeholders. Investors should recognize that by improving processes, an organization is increasing the chances of better future performance and steadier cash flows.

In general, apologies are "messages containing the acknowledgement of blameworthiness for a negative event" (Rasoulia et al., 2017). Remorse, sorrow and regret can be part of an apology message. By apologizing, a firm shows regret and accepts responsibility for failure. In this case, investors should worry about an organization's apology for a double reason. First, an apology may be viewed as a poor measure to restore broken relationships between the stakeholders and the organization, leading to falling performance, and second, apologies can be interpreted as an admission of guilt, rising the fear among investors that don't want to face lawsuits against the organization for instance.

3.5.7.3 Online response tools

Given that the crisis in questions took place in a digital context, it is important to bring up some advice on how to recover from it in the online background.

Two tones of voice exist in online communications when keeping a conversation with users (Langaro et al., 2019). Organizations can adopt a “corporate tone of voice” (CV) or a “conversational human voice” (CHV). In CV, organizations “speak as one voice”, whether in CHV, they use a “more humanized voice” (Langaro et al., 2019). Specifically, CHV can be described as “an engaging and natural style of organizational communication as perceived by an organization’s public, based on interactions between individuals in the organization and individuals in public” (Kelleher, 2009).

To handle negative comments and complaints in social media, organizations have set up web care teams, whose job is to control and mediate the online discussions (Van Noort & Willemsen, 2012). Van Noort et al. (2014) proposed guidelines for web care teams to follow when dealing with complaints. Recommendations involve that teams should be attentive and empathic in their messages, as well as they should facilitate complaint handling. As for the exact crisis response strategy, it all depends on the dimensions presented in the above section. Moreover, web care teams should proceed in the fastest manner in response to complaints, to prevent further negative eWOM (Balaji et al., 2016).

3.6. Answers to Assignment Questions

This section of the Teaching Note is composed of a detailed discussion guide, intended to manage the group discussion, based on the mentioned case study facts and events and on the theory and frameworks of the literature review. In order to maximize the effectiveness of the discussion, it is important that the instructor follows the same order of questions as proposed in the Suggested Assignment Questions section.

To start the discussion, students should be capable of summarizing the case study presenting a brief overview of the scene and highlighting relevant information for the main problem. Once verified that the case study had been perfectly understood by students, the instructor may proceed with the coming debate:

1. How did Facebook manage communications along the crisis?

Sample answer:

The basis for effective crisis management goes through good communication management before, during and after the crisis. As such, there are three phases in the crisis communication process: pre-crisis, crisis and post-crisis (Coombs, 2010a).

In the pre-crisis communication phase, a company should put effort in preventing, identifying and get ready for potential crisis events (Coombs, 2010a). This includes identifying risks and train people who will be involved. Back in 2014, when the “thisisyourdigitallife” was created and put in place, the social network’s privacy policies did not protect Facebook’s users’ and their friend’s private information. Instead, they let the app collect data such as users’ likes and sometimes private messages in order to create their psychographic profile and target them politically. Therefore, the company did not prevent the data to be harvested and used for other purposes. Moreover, when Facebook first knew, in 2015, that CA had sold their user’s data, they did little to make sure that the consulting firm had really deleted all the information as previously requested by the company. Zuckerberg later stated in his testimony that he just “shouldn’t have taken their word for it”. In 2015, Zuckerberg and his company “considered that a closed case”, clearly not assessing the risks of such data not having been eliminated. Later, in 2019, when it came to know that Facebook had known about the CA’s collection of its users’ data earlier than it claimed, according to an email exchange between the company’s employees, it was shown that the company indeed communicated there were issues with the data. However, certainly out of shame and guilt, the company did not want to admit that it had knowledge about, given the scandal that followed.

In the crisis communication phase, the aim is to identify the cause of the crisis and to respond to it by coming up with a well-thought solution (Coombs, 2010a). Definitely, the beginning of the crisis was triggered by the newspapers’ publications (The Guardian and The New York Times) that revealed that data of 87 million people had been collected and used for targeting U.S. voters in the 2016 elections, as well as in the Vote Leave Brexit campaign. Facebook clearly identified the source who originated the scandal, so much that it threatened to take legal action against the publishers. In this phase, a company should act fast, accurately and consistently. Nevertheless, Facebook did not act fast. Indeed, it took five long days to react to the revelations, and it did through a Facebook post, something it could have done the same day

the scandal was revealed, mainly due to the need of the rapid spread of news and information. The company could have done more and alerted the users that their private information had been spread by the time it learned about it, in 2015. The fact that they “ignored” this need to notify the most affected stakeholders opened a window for other players to disclose everything they found about the whole situation and frame the crisis in their own way. In terms of providing accurate information, Facebook failed without any doubt, from the moment it kept from its users that they were being target of a scheme to favor politicians. Being consistent is also not Facebook main communication skills. In fact, the company had already promised to protect its users in previous data breaches situations mentioned, but until now, it has failed to comply with its previous speeches and commitments.

As for the post-crisis communication phase, which involves efforts to follow-up with the stakeholders and to learn from the crisis (Coombs, 2010a), Facebook showed willingness to communicate with the stakeholders affected and to put in place measures that would help prevent such incidents from happening again.

2. What was the level of Damage associated with this crisis? Who are the stakeholders affected and how was the crisis perceived by them?

Sample answer:

According to theory, the level of damage may be defined as severe or minor (Coombs, 1995). In the Facebook data breach case, around 87 million worldwide Facebook users were affected (*Appendix 6*), becoming severe damage. Among these thousands and thousands of users, were included the ones who downloaded the app and did the survey but also all of their Facebook friends’. Both can be considered a direct victim of the crisis (Coombs, 1995). Indeed, they trusted Facebook with their private information (such as name, gender, hometowns, etc.) and did not expect their privacy to be invaded the way it was. Moreover, they certainly expected to be notified in situations like this one, in which they are directly affected by a lack of data protection.

Among the stakeholders affected were Facebook’s employees and its high representatives. First of all, the trust of the employees in the company surely decreased. In fact, who wants to work in a company that breaks the trust of those who contributed to its growth? Besides, their own private information might have been collected and sold to CA. As for the top representatives,

Mark Zuckerberg, whose own data was admitted being harvested too, and Sheryl Sandberg, were negatively affected by the crisis. Both are considered the face of Facebook, especially Zuckerberg, being expected to act fast and effectively in such an event. Therefore, in addition to being blamed for the breach of trust, they were also pointed the finger for not acting according to what was expected by other stakeholders, fast and insightfully.

Other important stakeholders that were troubled by the crisis were investors. The latter saw their trust in Facebook decrease, which was reflected in the company's number, namely the price of the shares and the total value of the company.

Facebook advertisers were also affected by the crisis. Indeed, fake news was one of the big topics that came up due to fake political advertising in the social media during the U.S. presidential elections. This had and has consequences in what people believe or fail to believe in what comes to advertisements in these digital channels. This reflects on the effectiveness of the advertising and on the payoffs of all the companies that advertise through Facebook.

Trust between Lawmakers and the social media giant was also broken, after so many failures to protect the privacy of its users. Democracy does not work anymore on social media. It is not correctly regulated.

It is also important to mention the nonvictims (Coombs, 1995), i.e. those who were not directly affected by the crisis but are now afraid that their privacy might be invaded in another data breach. Among these are all Facebook users, many having already deleted their account, and potential Facebook users.

People assign more responsibility to organizations when the level of damage caused by a crisis is higher. This was Facebook's case, that besides being considered the biggest culprit of the data harvesting, also lost moral legitimacy for not disclosing everything they knew by the time they learned about the situation. In the end, it all translated into a loss of brand reputation and a drop in financial results. Recovering from this is about acting to fight people and stakeholders' perceptions, which are based on three dimensions, according to Attribution Theory (Weiner, 1974). These are: locus of control, stability and controllability.

As regards locus of control, the Facebook data breach was perceived to being caused by both internal issues, inaccurate privacy policies and the attempt to hide the illegal collection of user's data, and external players, i.e., a consulting and marketing firm which proceeded to that collection of data without users' consent. Concerning the stability of the crisis, information was made public that CA had collected people's data from 2014 to 2018, increasing the impact of the crisis and creating a large time frame so the data was spread even wider and used for other purposes. As for controllability, it was perceived that Facebook could have done much better to protect its users and their privacy, and more, it could have alerted the users before other media channels took the lead and spread the news themselves, eventually having a much larger impact.

3. How would you react if you were the CMO of Facebook?

Sample answer:

As Facebook's CMO, the goal is to regain people's trust in the company and rebuild the reputation, as well as improving results. Crisis response strategies serve this goal, aiming to repair the damage caused by the attributions made by the community. The most appropriate strategy must be selected in order to achieve the desired end. The selected strategy must be based on the crisis type, the evidence, the damage caused and the company's performance history (Coombs, 1995).

There are four crisis types, namely Faux Pas, terrorism, accidents and transgressions (Coombs, 1995). The Facebook data breach crisis may be considered an accident, considering that, due to the company's policies, it unintentionally allowed a third-party player to collect its users' private data. Nevertheless, it may also be considered to be the result of an act of "terrorism" from the creators of the "thisisyourdigitallife" app and also CA, which took advantage of the data for commercial and political purposes. Regarding the evidence of the existence of the crisis, it was proven to be true not only by third parties, such as Christopher Wylie but also by Facebook itself, who admitted the situation. As for the damage caused, the affected stakeholders were mentioned in a previous analysis (Question 2). Regarding the company's performance history, it is important to state that Facebook had already suffered from leaks of information and non-consented data-sharing issues due to several malfunctions (in 2006, 2007, 2011 and 2013). Therefore, the firm's past performance carried a negative sign. Taking all this into

consideration, Facebook should follow the correct path in the decision flowchart of Accidents (*Figure 2*) and Terrorism (*Figure 4*).

People's perceptions of the Facebook crisis raised the need of adopting different response strategies, as mentioned above. Indeed, Facebook would need to implement mortification strategies, whose goal is to earn forgiveness and build, in some way, acceptance for the critical situation. There exist three sub-strategies among the mortification strategies: remediation, repentance and rectification. Remediation is about offering some form of compensation to help the victims of the crisis. Indeed, Facebook should offer monetary compensation to all those users affected by the breach, whose privacy was completely attacked. The company should, therefore, provide an indemnity for non-compliance with users' rights. This would increase stakeholder's perception of distributive justice, being interpreted by investors as an effort of the company to solidify an important resource, i.e. the relationships with its stakeholders, which in the future would lead to more financial stability. Regarding repentance, a strategy already embraced by Facebook in every post, implies apologizing and asking for forgiveness. The spokespersons should definitely reinforce this strategy but complement it with others, namely with rectification. The latter involves a restructuring, taking action to prevent a recurrence of the crisis. As Facebook's CEO claimed, measures have already been implemented, regarding both the privacy policies and third-party apps. This should improve stakeholder's perceptions of procedural justice that investors should interpret as an effort to guarantee better future performance.

This crisis can also be considered an act of terrorism and so, Facebook should and did integrate to its reputation recovery approach a suffering strategy, presenting itself as a victim of actions of outside actors. However, a suffering strategy should have been applied from the very first moment they learned about the deeds of CA back in 2015, and after warning all affected users that their data have been stolen. This would help the organization gain some empathy from the people.

There is a discrepancy between the adopted strategies and the ones that the company should, in fact, have used. For instance, they used intimidation by threatening to sue the newspapers if they published. This non-existence strategy may only be used in a "Faux Pas" crisis, when an external agent tries to transform an unintentional act of the company into a crisis. Furthermore, Facebook resorted to an excuse strategy, trying to distance itself from guilt. By denying their

intention and volition of leaking the data, Facebook tried to minimize its responsibility in the crisis.

4. Who should be the spokesperson in this case?

Sample answer:

In the Facebook crisis, several spokespersons are required. There should be a face-to-face spokesperson but also online spokespeople, given the size of the organization and the impact of the crisis itself.

There are several important points to consider when choosing a crisis spokesperson. For instance, the person should be compelling and enigmatic, but also remain calm under pressure and at the same time connect with the audience, using a conversational human voice. That person should also have expert knowledge of both the organization and what led to the crisis. In a real-life conversation with a reporter (or others), besides needing to show humility and compassion, (s)he should maintain strong eye contact with the interviewer and avoid nodding their head so not to show agreement with what is being spoken. As for behind the screen representatives, that can be the same as face-to-face, or specialized web care teams, whose job is to control and mediate online discussions, in a fast, attentive and empathetic manner.

In this case, Mark Zuckerberg should be the spokesperson and indeed, he was. He fulfills the above recommendations of how to communicate in a crisis. As for the online crisis teams, they should be composed of experienced workers, who had pre-planned how to act and what to say in these types of situations, always adapting to each crisis event.

Therefore, preparation for crisis is crucial and essential for every organization, leading them to adopt a well thought out posture.

5. How would you avoid that this repeats in the future?

Sample answer:

Avoiding a reoccurrence of such a crisis goes through having a good Issues and Risk Management. It is important to bear in mind that an issue is not a crisis but, if not properly

corrected, it may develop into it. The same goes for risks, whose lack of attention and control may lead to an actual crisis. This is why issue management and risk management are so important for the proper functioning of an organization.

Part of the function of crisis managers is to assess which undeveloped risks and issues may evolve into major affairs. Facebook failed to manage this, as the company did not cut the bonds it had with Kogan's app that originated the illegal data collection, a mistake that Zuckerberg will forever regret. The lesson to take from the 2018 scenario, is that prevention is never too much and may help a company to survive in difficult conditions.

Every company should be proactive and prepare for a crisis. Crisis managers should gather and brainstorm about potential crisis that may occur in the organization. This has benefits because they may find that some of the issues and risks are avoidable by modifying certain methods and behaviors. Moreover, better answers to different sorts of scenarios will pop up in a calm discussion setting than under the pressure of a real crisis.

Crisis managers should create a crisis plan, in the case an issue comes up. This involves identifying the issue itself, namely through notifications systems, and the different scenarios to which it may develop. It also implies identifying the stakeholders, that are or can be affected by the potential deployment of the issue. Moreover, it includes the identification of the crisis management team and the spokespeople for internal and external communications in each situation.

3.6. Suggestions for the Animation of the Case Study

A proposition of slides to be used in class for teaching is available in the appendix (**Appendix**).

4. Reference List

Allen, M. W., & Caillouet, R. H. (1994). Legitimation endeavors: Impression management strategies used by an organization in crisis. *Communication Monographs*, 61(1), 44–62.

doi: 10.1080/03637759409376322.

Aaker, J., Fournier, S., & Brasel, S. A. (2004). When Good Brands Do Bad. *Journal of Consumer Research*, 31(1), 1–16.

doi: 10.1086/383419

Amazon Mechanical Turk. Retrieved from <https://www.mturk.com/>

Arpan, L. M., & Roskos-Ewoldsen, D. R. (2005). Stealing thunder: Analysis of the effects of proactive disclosure of crisis information. *Public Relations Review*, 31(3), 425–433.

doi: 10.1016/j.pubrev.2005.05.003

Balaji, M., Khong, K. W., & Chong, A. Y. L. (2016). Determinants of negative word-of-mouth communication using social networking sites. *Information & Management*, 53(4), 528–540.

doi: 10.1016/j.im.2015.12.002

Barton, L. (2001). *Crisis in organizations II*. Cincinnati, OH: South-Western College Pub.

Baumeister, R. F., Zhang, L., & Vohs, K. D. (2004). Gossip as Cultural Learning. *Review of General Psychology*, 8(2), 111–121.

doi: 10.1037/1089-2680.8.2.111

BBC News (2012). Google and Facebook top 2011's most visited sites in US. Retrieved from <https://www.bbc.com/news/technology-16356066>

Brummett, B. (1980). Towards a theory of silence as a political strategy. *Quarterly Journal of Speech*, 66(3), 289–303.

doi: 10.1080/00335638009383527

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market*. *Journal of Computer Security*, 11(3), 431–448.

doi: 10.3233/jcs-2003-11308

Carroll, A. B. (1991). The pyramid of corporate social responsibility: Toward the moral management of organizational stakeholders. *Business Horizons*, 34(4), 39–48.

doi: 10.1016/0007-6813(91)90005-g

CNBC. (2018, March 21). Zuckerberg on Cambridge Analytica: 'We have a responsibility to protect your data, and if we can't then we don't deserve to serve you'. Retrieved from <https://www.cnbc.com/2018/03/21/zuckerberg-statement-on-cambridge-analytica.html>

CNBC. (2018, November 20). Here are the scandals and other incidents that have sent Facebook's share price tanking in 2018.

Retrieved from <https://www.cnbc.com/2018/11/20/facebooks-scandals-in-2018-effect-on-stock.html>

CNBC. (2019). Facebook learned about Cambridge Analytica as early as September 2015, new documents show.

Retrieved from <https://www.cnbc.com/2019/08/23/facebook-releases-new-cambridge-analytica-documents.html>

CNN (2012) Facebook reaches one billion users. Retrieved from <https://money.cnn.com/2012/10/04/technology/facebook-billion-users/>.

CNN (2018) CNN Exclusive: Zuckerberg apologizes – CNN Video. Retrieved from <https://edition.cnn.com/videos/cnnmoney/2018/03/22/facebook-zuckerberg-cambridge-analytica-long.cnnmoney>.

Coombs, W. T. (1995). Choosing the Right Words. *Management Communication Quarterly*, 8(4), 447–476.

doi: 10.1177/0893318995008004003

Coombs, W. T. (2010a). Parameters for Crisis Communication. *The Handbook of Crisis Communication*, 17–53.

doi: 10.1002/9781444314885.ch1

Coombs, W. T. (2010b). Crisis Communication and Its Allied Fields. *The Handbook of Crisis Communication*, 54–64.

doi: 10.1002/9781444314885.ch2

Coombs, W. T. (2014). *Ongoing crisis communication: planning, managing, and responding*. Los Angeles: SAGE.

Coombs, W. T., & Holladay, S. J. (2002). Helping Crisis Managers Protect Reputational Assets. *Management Communication Quarterly*, 16(2), 165–186.

doi: 10.1177/089331802237233

Coombs, W. T., & Holladay, S. J. (2005). An Exploratory Study of Stakeholder Emotions: Affect and Crises. *Research on Emotion in Organizations The Effect of Affect in Organizational Settings*, 263–280.

doi: 10.1016/s1746-9791(05)01111-9

Coombs, W. T., & Holladay, S. J. (2006). Unpacking the halo effect: Reputation and crisis management. *Journal of Communication Management*, 10(2), 123–137.

doi: 10.1108/13632540610664698

Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: Lessons from the Choicepoint and TJX data breaches. *MIS Quarterly*, 33(4), 673–687. doi: 10.2307/20650322

Facebook (2006). *Calm down. Breathe. We hear you.*

Retrieved from <https://www.facebook.com/notes/facebook/calm-down-breathe-we-hear-you/2208197130/>.

Facebook (2007). *Thoughts on Beacon*. Retrieved from

<https://www.facebook.com/notes/facebook/thoughts-on-beacon/7584397130/>

Facebook (2011). *Our commitment to the Facebook Community*. Retrieved from <https://www.facebook.com/notes/facebook/our-commitment-to-the-facebook-community/10150378701937131/>

Facebook (2013). *Important Message from Facebook White Hat Program*. Retrieved from <https://www.facebook.com/notes/facebook-security/important-message-from-facebooks-white-hat-program/10151437074840766>

Facebook (2018a, March 21). Retrieved from <https://www.facebook.com/zuck/posts/10104712037900071>.

Facebook (2018b, March 21). Retrieved from <https://www.facebook.com/sheryl/posts/10160055807270177?pnref=story>

Facebook Newsroom (2018, March 17). Retrieved from <https://about.fb.com/news/2018/03/suspending-cambridge-analytica/>

Facebook Newsroom (2018, March 19). Retrieved from <https://newsroom.fb.com/news/2018/03/forensic-audits-cambridge-analytica/>

Facebook Newsroom (2018, March 21). Retrieved from <https://newsroom.fb.com/news/2018/03/cracking-down-on-platform-abuse/>

Facebook Newsroom (2019). *Document Holds the Potential for Confusion*. Retrieved from <https://newsroom.fb.com/news/2019/08/document-holds-the-potential-for-confusion/>.

Facebook Platform - Definition from Techopedia. Retrieved from <https://www.techopedia.com/definition/27916/facebook-platform>.

FTC (2011). *Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises*. Retrieved from <https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep>.

Gelbrich, K., & Roschk, H. (2011). A Meta-Analysis of Organizational Complaint Handling and Customer Responses. *Journal of Service Research*, 14(1), 24–43.

doi: 10.1177/1094670510387914

Gillespie, N., & Dietz, G. (2009). Trust Repair After An Organization-Level Failure. *Academy of Management Review*, 34(1), 127–145.

doi: 10.5465/amr.2009.35713319

Goyal, A., Santa-clara, P., Subrahmanyam, A., Torous, W., Valkanov, R., Campbell, E. J., & Roll, R. (2003). Idiosyncratic risk matters. *Journal of Finance*, 58(3), 975–1007. Retrieved from http://www.hec.unil.ch/agoyal/docs/IdiosyncraticRisk_JoF.pdf

Griffin, E. A. (1997). *A first look at communication theory*. New York: McGraw-Hill.

Griffin, M., Babin, B. J., & Attaway, J. S. (1991). An empirical investigation of the impact of negative publicity on consumer attitudes and intentions. *Advances in Consumer Research*, 18, 121-140.

Grunig, J. E. (1993). Image and substance: From symbolic to behavioral relationships. *Public Relations Review*, 19(2), 121–139.

doi: 10.1016/0363-8111(93)90003-u

Heath, R. (2005). Issues Management. *Encyclopedia of Public Relations*.

doi: 10.4135/9781452276236.n274

Ice, R. (1991). Corporate Publics and Rhetorical Strategies. *Management Communication Quarterly*, 4(3), 341–362.

doi: 10.1177/0893318991004003004

Independent (2018). People are trying to leave Facebook. But it might not actually be possible. Retrieved from <https://www.independent.co.uk/life-style/gadgets-and-tech/news/delete-facebook-cambridge-analytica-campaign-deactivate-data-remove-hide-privacy-a8266671.html>.

Kelleher, T. (2009). Conversational Voice, Communicated Commitment, and Public Relations Outcomes in Interactive Online Communication. *Journal of Communication*, 59(1), 172–188.

doi: 10.1111/j.1460-2466.2008.01410.x

Langaro, D., Loureiro, S. M. C., & Soares, A. (2020). When Consumers Complaints Fall Into Public Domain. *Exploring the Power of Electronic Word-of-Mouth in the Services Industry Advances in Marketing, Customer Relationship Management, and E-Services*, 124–137.

doi: 10.4018/978-1-5225-8575-6.ch008

Malhotra, A., & Malhotra, C. K. (2010). Evaluating Customer Information Breaches as Service Failures: An Event Study Approach. *Journal of Service Research*, 14(1), 44–59. doi: 10.1177/1094670510383409

Marcus, A. A., & Goodman, R. S. (1991). Victims And Shareholders: The Dilemmas Of Presenting Corporate Policy During A Crisis. *Academy of Management Journal*, 34(2), 281–305.

doi: 10.2307/256443

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data Privacy: Effects on Customer and Firm Performance. *Journal of Marketing*, 81(1), 36–58.

doi: 10.1509/jm.15.0497

Metts, S., & Cupach, W. R. (1989). Situational influence on the use of remedial strategies in embarrassing predicaments. *Communication Monographs*, 56(2), 151–162.

doi: 10.1080/03637758909390256

Mitroff, I. I., Pearson, C. M., & Harrington, L. K. (1996). *The essential guide to managing corporate crises: a step-by-step handbook for surviving major catastrophes*. New York: Oxford University Press.

NBC News (2013). Supreme Court won't review Facebook's notorious 'Beacon' case. Retrieved from <https://www.nbcnews.com/technolog/supreme-court-wont-review-facebooks-notorious-beacon-case-8C11522153>

Rasoulilian, S., Grégoire, Y., Legoux, R., & Sénécal, S. (2017). Service crisis recovery and firm performance: insights from information breach announcements. *Journal of the Academy of Marketing Science*, 45(6), 789–806.

doi: 10.1007/s11747-017-0543-8

Reuters. (2018). Factbox: Who is Cambridge Analytica and what did it do? Retrieved from <https://www.reuters.com/article/us-facebook-cambridge-analytica-factbox/factbox-who-is-cambridge-analytica-and-what-did-it-do-idUSKBN1GW07F>.

Richman, L. S., & Leary, M. R. (2009). Reactions to discrimination, stigmatization, ostracism, and other forms of interpersonal rejection: A multimotive model. *Psychological Review*, 116(2), 365–383.

doi: 10.1037/a0015250

Roux-Dufort, C. (2000). Why organizations don't learn from crises: The perverse power of normalization. *Review of Business*, 21, 25–30. Retrieved from <https://www.questia.com/library/journal/1G1-73183464/why-organizations-don-t-learn-from-crises-the-perverse>

Rust, R. T., Ambler, T., Carpenter, G. S., Kumar, V., & Srivastava, R. K. (2004). Measuring Marketing Productivity: Current Knowledge and Future Directions. *Journal of Marketing*, 68(4), 76–89.

doi: 10.1509/jmkg.68.4.76.42721

Sharkey, W. F., & Stafford, L. (1990). Responses to Embarrassment. *Human Communication Research*, 17(2), 315–335.

doi: 10.1111/j.1468-2958.1990.tb00235.x

Statista (2018). Facebook accounts affected by Cambridge Analytica by country. Retrieved from <https://www.statista.com/statistics/831815/facebook-user-accounts-affected-cambridge-analytica-by-country/>.

Statista (2018). Facebook's annual revenue and net income from 2007 to 2018. Retrieved from <https://www.statista.com/statistics/277229/facebooks-annual-revenue-and-net-income/>

Statista (2019). Infographic: Facebook Keeps on Growing. Retrieved from <https://www.statista.com/chart/10047/facebooks-monthly-active-users/>

Sturges, D. L. (1994). Communicating through Crisis. *Management Communication Quarterly*, 7(3), 297–316.

doi: 10.1177/0893318994007003004

Techcrunch (2011). The Rise of Facebook's Valuation From 2004-2011 [Graphic]. Retrieved from <https://techcrunch.com/2011/01/10/facebook-5/>

TechRepublic (2019). Facebook data privacy scandal: A cheat sheet. Retrieved from <https://www.techrepublic.com/article/facebook-data-privacy-scandal-a-cheat-sheet/>.

TED (2018). O papel do Facebook no Brexit - e a ameaça à democracia. Retrieved from https://www.ted.com/talks/carole_cadwalladr_facebook_s_role_in_brexit_and_the_threat_to_democracy?language=pt

The Telegraph (2009). Facebook shuts down Beacon. Retrieved from <https://www.telegraph.co.uk/technology/facebook/6214370/Facebook-shuts-down-Beacon.html>.

The Guardian (2015). Ted Cruz campaign using firm that harvested data on millions of unwitting Facebook users. Retrieved from <https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data>.

The Guardian (2018, March 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach.

Retrieved from <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>.

The Guardian (2018, March 18). 'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower. Retrieved from

<https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump>.

The Guardian (2018, March 22). Mark Zuckerberg apologizes for Facebook's 'mistakes' over Cambridge Analytica. Retrieved from <https://www.theguardian.com/technology/2018/mar/21/mark-zuckerberg-response-facebook-cambridge-analytica>.

The Guardian (2018a, April 11). Mark Zuckerberg vows to fight election meddling in marathon Senate grilling. Retrieved from <https://www.theguardian.com/technology/2018/apr/10/zuckerberg-facebook-testimony-latest-news-regulation-congress>

The Guardian (2018b, April 11). Zuckerberg put on back foot as House grills Facebook CEO over user tracking. Retrieved from <https://www.theguardian.com/technology/2018/apr/11/zuckerberg-hearing-facebook-tracking-questions-house-back-foot>

The New York Times (2011). F.T.C. Settles Privacy Issue at Facebook. Retrieved from <https://www.nytimes.com/2011/11/30/technology/facebook-agrees-to-ftc-settlement-on-privacy.html>

The New York Times (2012). Facebook Raises \$16 Billion in I.P.O. Retrieved from <https://dealbook.nytimes.com/2012/05/17/facebook-raises-16-billion-in-i-p-o/>

Time (2006). Inside the Backlash Against Facebook. Retrieved from <http://content.time.com/time/nation/article/0,8599,1532225,00.html>

Turner, M. M., Mazur, M. A., Wendel, N., & Winslow, R. (2003). Relational ruin or social glue? The joint effect of relationship type and gossip valence on liking, trust, and expertise. *Communication Monographs*, 70(2), 129–141.
doi: 10.1080/0363775032000133782

Turkopticon.com. Retrieved from <https://turkopticon.ucsd.edu/>.

Twitter (2018). Yesterday @facebook threatened to sue us. Today we publish this. Meet the whistleblower blowing the lid off Facebook & Cambridge Analytica. Retrieved from <https://twitter.com/carolecadwalla/status/974995682124804099>

Noort, G. V., & Willemsen, L. M. (2012). Online Damage Control: The Effects of Proactive Versus Reactive Webcare Interventions in Consumer-generated and Brand-generated Platforms. *Journal of Interactive Marketing, 26*(3), 131–140.

doi: 10.1016/j.intmar.2011.07.001

Noort, G. V., Willemsen, L. M., Kerkhof, P., & Verhoeven, J. W. M. (2015). Webcare as an Integrative Tool for Customer Care, Reputation Management, and Online Marketing: A Literature Review. *Integrated Communications in the Postmodern Era, 77–99*.

doi: 10.1057/9781137388551_4

Wartick, S. L. (1992). The Relationship between Intense Media Exposure and Change in Corporate Reputation. *Business & Society, 31*(1), 33–49.

doi: 10.1177/000765039203100104

Weiner, B. (1974). *Achievement motivation and attribution theory*. Morristown, NJ: General Learning Press.

Williams, D. E., & Olaniran, B. A. (1998). Expanding the crisis planning function: Introducing elements of risk communication to crisis communication practice. *Public Relations Review, 24*(3), 387–400.

doi: 10.1016/s0363-8111(99)80147-7

Yahoo! Finance (2012). SEC, FINRA to review Facebook issues, Nasdaq sued. Retrieved from <https://web.archive.org/web/20120528230445/https://finance.yahoo.com/news/facebook-shares-fall-valuation-doubts-134021024.html>

Yang, Z., & Fang, X. (2004). Online service quality dimensions and their relationships with satisfaction. *International Journal of Service Industry Management, 15*(3), 302–326.

doi: 10.1108/09564230410540953

ZDNet (2013). Facebook bug exposed personal data of six million accounts.

Retrieved from <https://www.zdnet.com/article/facebook-bug-exposed-personal-data-of-six-million-accounts/>

Appendix



Topic: Crisis Management

Case Study: Facebook In Face Of Crisis

CATOLICA LISBON
FACULDADE DE CIÊNCIAS

The instructor is supposed to ask who read the case and then surprise students with... a small quiz! (see next slide)

Grab your phones! It's Quizz time!



Case Discussion


CATOLICA LISBON
FACULDADE DE CIÊNCIAS

2

The instructor is supposed to ask students to grab their phones and download the Kahoot app, in order to play the quiz.

Answers to the Quiz

1 - Quiz
Who was the creator of the "thisisyourdigitallife" app?

 10 sec

- Christopher Wylie
- Robert Mercer
- Carole Cadwalladr
- Alexander Kogan

2 - Quiz
What is the name the whistleblower that revealed the Cambridge Analytica scheme?

 10 sec

- Alexander Kogan
- Mark Zuckerberg
- Christopher Wylie
- Sheryl Sandberg

Slide for the Instructor



3


Answers to the Quiz

3 - Quiz
How many millions of people were affected by the Facebook data breach?

 10 sec

- 17 Million
- 43 Million
- 87 Million
- 92 Million

4 - Quiz
How many days did Mark Zuckerberg take to break his silence on the data breach scandal?

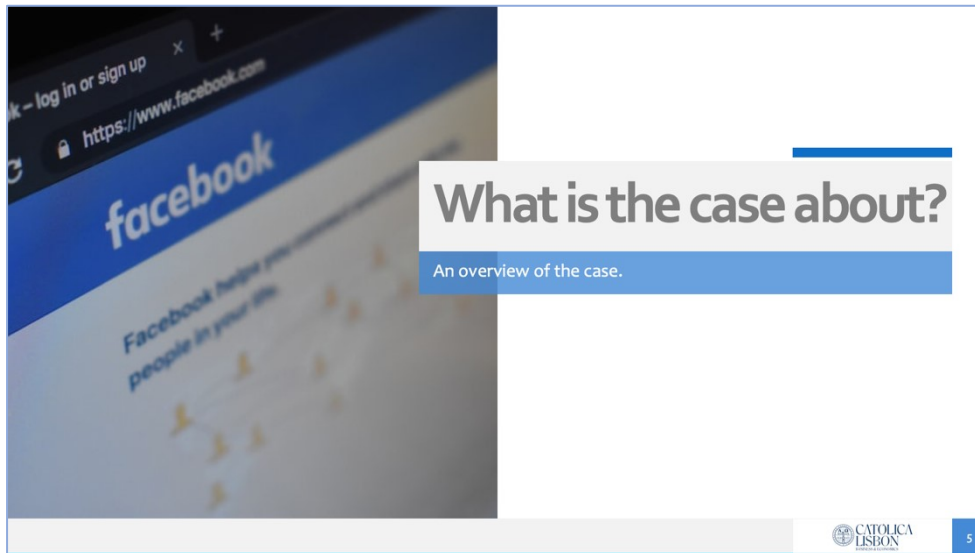
 10 sec

- 1 day
- 2 days
- 4 days
- 5 days

Slide for the Instructor



4

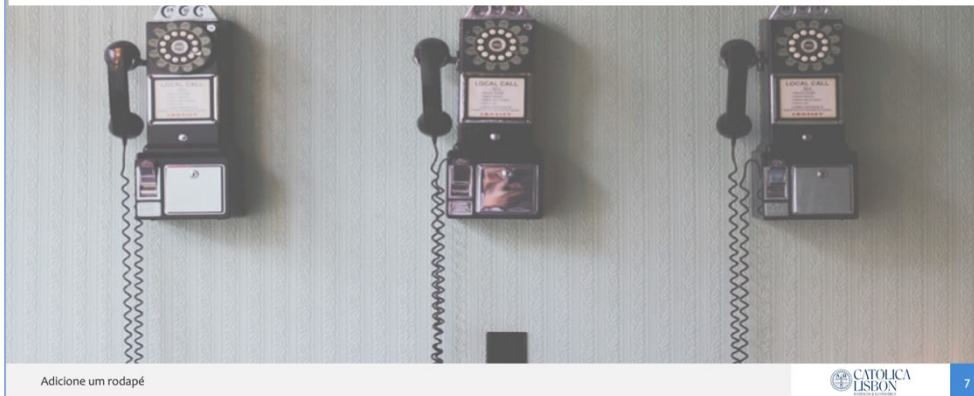


Here the instructor is supposed to ask students for an overview of the case.



The instructor is now supposed to incentivize students' participation in the answers of the questions and to take notes.

1. How did Facebook manage communications along the crisis?



The instructor is supposed to write down student's ideas on the board, making room for various ideas.

1. How did Facebook manage communications along the crisis?

Crisis Communication phases:



Pre-crisis communication

Includes efforts to prevent, detect and prepare for crisis, such as collection information about crisis risks and training people who will be involved in the process (e.g., crisis spokespersons) (Coombs, 2010a).

Crisis communication

The recognition of the trigger event and the actual response to it (Coombs, 2010a).

Post-crisis communication

Involves efforts to follow-up with stakeholders and learn from the crisis (Coombs, 2010a).

The instructor is supposed to present the three crisis communication phases, theorized by Timothy Coombs (in the picture), in his book "The Handbook of Crisis Communication" (2010).

The idea is to assign each step taken by the company, in the way it managed communications, to each one of the phases, and conclude what have they done right or wrong, and what could be improved.

2. What was the level of Damage associated with this crisis? Who are the stakeholders affected and how was the crisis perceived by them?



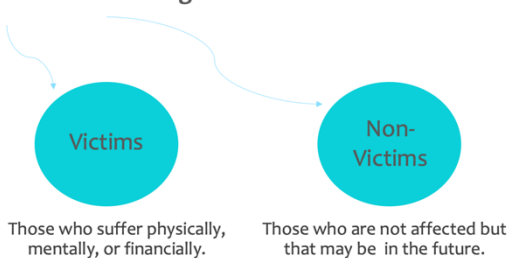
Adicione um rodapé

CATOLICA LISBON

9

2. What was the level of Damage associated with this crisis? Who are the stakeholders affected and how was the crisis perceived by them?

Level of damage:
Minor VS Severe damage



Victims
Those who suffer physically, mentally, or financially.

Non-Victims
Those who are not affected but that may be in the future.

Stakeholder's perceptions of a crisis:

ATTRIBUTION THEORY

- Locus of control
- Stability
- Controllability

CATOLICA LISBON

10

The instructor is supposed to present another Timothy Coombs theory (1995), that states that a crisis has either a minor or a severe level of damage. Damage also raises the question of Victims. It is important to define who are the victims and non-victims, i.e., the stakeholders. Stakeholder perceive the causes of an event according to three dimensions: locus of control, stability and controllability. This is called the Attribution Theory.

3. How would you react if you were the CMO of Facebook?



Adicione um rodapé

3. How would you react if you were the CMO of Facebook?

Four types of crisis (Coombs, 1995)

	Unintentional	Intentional
External	Faux Pas	Terrorism
Internal	Accidents	Transgressions

Five types of crisis-response strategies (Coombs, 1995)



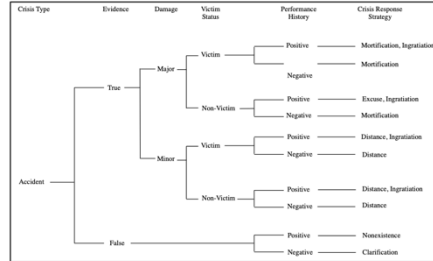
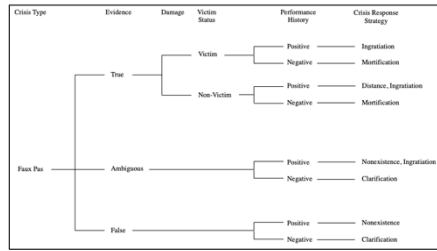
Crisis-response strategies decision flowcharts

<ul style="list-style-type: none"> Denial Clarification Attack
<ul style="list-style-type: none"> Excuse <ul style="list-style-type: none"> Denial of intention Denial of volition Justification <ul style="list-style-type: none"> Minimizing injury Victim deserving Misrepresentation of the crisis event
<ul style="list-style-type: none"> Bolstering Transcendence Praising Others
<ul style="list-style-type: none"> Remediation Repentance Rectification
Suffering Strategy

Here the instructor needs to present the several crisis-response strategies (Coombs, 1995). There are four types of crisis and for each one, there is a decision flowchart that the Company should follow. The class should do the exercise for the Facebook crisis.

3. How would you react if you were the CMO of Facebook?

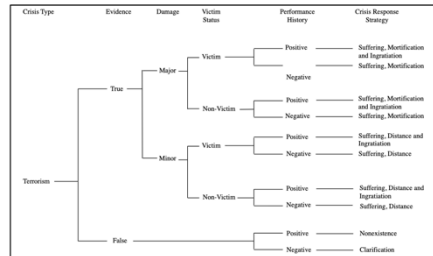
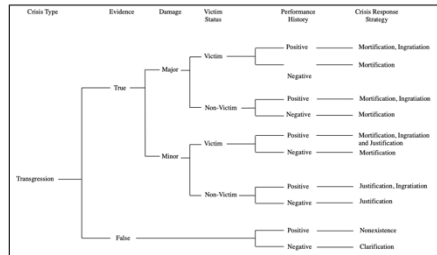
Crisis-response strategies decision flowcharts (Coombs, 1995)



Here the instructor needs to present the several crisis-response strategies (Coombs, 1995). There are four types of crisis and for each one, there is a decision flowchart that the Company should follow. The class should do the exercise for the Facebook crisis.

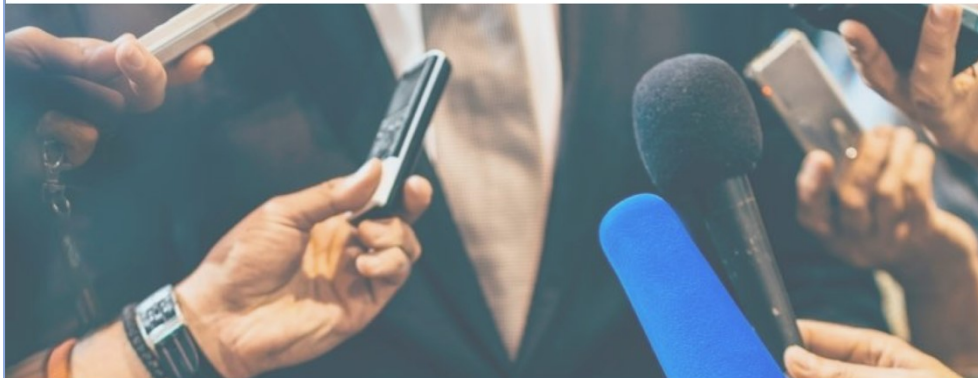
3. How would you react if you were the CMO of Facebook?

Crisis-response strategies decision flowcharts (Coombs, 1995)



Here the instructor needs to present the several crisis-response strategies (Coombs, 1995). There are four types of crisis and for each one, there is a decision flowchart that the Company should follow. The class should do the exercise for the Facebook crisis.

4. Who should be the spokesperson in this case?



Adicione um rodapé

4. Who should be the spokesperson in this case?

Face to face spokesperson

- Characteristics:
- Compelling and enigmatic
 - Humility and compassion
 - Calm under pressure
 - Connect with the audience
 - Conversational human voice
 - Expert knowledge on the organization and the crisis itself
 - Maintain eye contact
 - Avoid nodding head

Online spokespeople

- Specialized web-care teams
- Expert knowledge on the organization and the crisis itself
- Fast
- Attentive
- Empathetic

The instructor needs to explain to students the several characteristics of a crisis spokesperson/people. Then, students must suggest who should be the spokesperson in Facebook's case.

5. How would you avoid that this repeats in the future?



Adicione um rodapé

CATOLICA LISBON

17

5. How would you avoid that this repeats in the future?

Issues Management

It involves “a strategic set of functions used to reduce friction and increase harmony between organizations and their publics in the public policy arena” (Heath, 2005).

Risk Management

Analysis done by crisis managers in order to detect risks before they convert into something massive (Coombs, 2010b).

→ Prevention ←

↑
CRISIS PLAN

CATOLICA LISBON

18

Here the instructor is supposed to introduce the topics of issues management and risk management in order to show the importance of preventing a crisis.

You may want to check these out...

Videos

- Christopher Wylie interview
Source: <https://youtu.be/EXdYSQ6nu-M>
- Carole Cadwalladr Ted Talk
Source:
https://www.ted.com/talks/carole_cadwalladr_face_book_s_role_in_brexit_and_the_threat_to_democracy?utm_campaign=tedsread&utm_medium=referral&utm_source=tedcomshare
- Marz Zuckerberg CNN interview
Source: CNN (2018) CNN Exclusive: Zuckerberg apologizes – CNN Video. Retrieved from <https://edition.cnn.com/videos/cnnmoney/2018/03/22/facebook-zuckerberg-cambridge-analytica-long.cnnmoney>.
- The Great Hack (2019), Netflix documentary

Books

- The Handbook of crisis communication (Coombs, 2010)
Source: Coombs, W. T., Holladay, S. J. (2010). *The Handbook of Crisis Communication*. Hoboken, NJ: Wiley-Blackwell, 17-64.
- Choosing the right words (Coombs, 1995)
Source: Coombs, W. T. (1995). Choosing the Right Words: The Development of Guidelines for the Selection of the “Appropriate” Crisis-Response Strategies. *Management Communication Quarterly*, 8(4), 447-476.

Adicione um rodapé



19



Thank you!
See you next class!



20

References

- The images were retrieved from <https://unsplash.com/>
- Image of Timothy Coombs, retrieved from https://www.google.pt/search?q=w:timothy+coombs&sa=X&biw=1259&bih=587&sxsf=ACYBGNO73ZUC_ElSZ_ALcYOpJHcTv1q_1575991523472&tbm=isch&source=iu&icb=1&fir=HmFsw0DLUTdIXM%252A%252CrlLp33BHUwJlyM%252C%252Fg%252F11f35y1sf&vet=1&usq=Al4_-kR7TMRfwtFOnA6Ehdgse74E_EOgA&ved=2ahUKEwitHsbP3savmAhUHfBoKHQ-DUgQ_BowC3oECAwOAw#imgrc=HmFsw0DLUTdIXM

Adicione um rodapé



21