Crisis dead – long live the crisis! Apple inc.: managing the post-pandemic and cargo thefts crises

Case

Crisis dead – long live the crisis! Apple inc.: managing the post-pandemic and cargo thefts crises

Jaweria Ahsan,
Aušrinė Šilenskytė

Abstract: Supply chain thefts have caused a crisis for companies in various industries multiple times. Thefts had been partially put on hold because of COVID-19, but companies should be ready to face the emergency when the lockdown eases. This case describes the challenges faced by Apple's international logistics manager, who needed to design preventative actions for the constantly repeating crisis caused by the theft of Apple's iPhone shipments and to ensure that the expected emergency in the post-COVID era would not hit the company. The case helps stimulate classroom/group discussions on all three phases (the pre-crisis, the crisis, and the post-crisis) of global crisis management. When solving the case, students are encouraged to apply holistic thinking for crisis assessment and management, and to evaluate the benefits of industry stakeholder collaboration and the role of technological innovations in long-term crisis prevention. The case offers a teaching plan that comprises two levels of complexity and can be used for undergraduate, MBA, or MSc-level studies.

Keywords

global smartphone industry
cargo thefts
crisis assessment and prevention
blockchain

15.1. Introduction

Crisis management (CM) requires holistic thinking and appreciating the future over current challenges in a volatile and ambiguous global environment (McNulty and Marcus, 2020). Leaders handling a crisis must consider issues beyond their organisation and collaborate with multiple stakeholders to find solutions (ibid.). Moreover, to tackle a global crisis, managers need to analyse the three CM phases: *the pre-crisis* (what were the preventative and preparatory

actions?), *the crisis* (what were the responses when the crisis occurred?), and *the post-crisis* (how to incorporate the takeaways from the crisis and its management?; Coombs and Laufer, 2018). Managers need to take action in the foreign country of operations or internationally in each of these phases (ibid.). Understanding how these phases of several simultaneous crises overlap and influence one another is also essential. The Apple case on the crises caused by cargo thefts and COVID-19 illustrates these issues and invites readers to find innovative solutions for the company and the entire ecosystem.

15.2. Preparing for a crisis during the pandemic at Apple Inc.[1]

The COVID-19 pandemic disrupted global supply chains. For a few months, these interruptions had shifted the attention of David Talbot,[2] the international logistics manager at Apple Inc., from concerns about other emergencies, such as cargo thefts. When supply chain flows were slowly normalising, David was anxious about the supply chain thefts again. The approximate value of cargo thefts before the pandemic was US$900 million in the USA alone and cost the broader mobile ecosystem US$30 billion annually (Farrell, 2015; Hodkinson, 2019). David's fear could not have been worse on hearing the warnings issued by Transported Asset Protection Association (TAPA) about organised crime groups (OCGs) and opportunist ad hoc cargo thieves planning to recover cargo theft "incomes" that they partially lost because of the Great Lockdown (BIFA, 2021).

David realised that cargo thefts account for a small percentage of Apple Inc.'s global costs. Nevertheless, the thefts had been seriously tarnishing the company's international brand image, threatening its security, and infringing its copyrights, as stolen phones were resold in the black market. David was responsible for mitigating supply chain disruptions and the prevention of related emergencies. Consequently, searching for a feasible solution to prevent cargo thefts and avoid thefts projected in the post-COVID era immediately topped David's agenda. Moreover, David was pondering on the insufficient collaboration among the stakeholders of the global smartphone industry, which seemed to be crucial to close the ecosystem loopholes that OCGs had been exploiting (cf. Farrell, 2015).

15.3. Global mobile phone industry and Apple Inc.

The mobile phone industry was oligopolistic, with six dominating players: Samsung, Apple, Xiaomi, Oppo, Vivo, and Huawei (Counterpoint Technology, 2022). The industry was fast growing – in 2019, smartphone manufacturers had sold 1,540 million units worldwide,

compared to 172 million in 2009, indicating an 895% increase in a decade (O'Dea, 2021). The global smartphone industry was expected to reach US$1,351.8 billion by 2026, with a compound annual growth rate of 11.2% over 2021–2026 (ibid.).

Apple Inc. (further in the text 'Apple') was an American multinational corporation operating in the consumer electronics industry, with products ranging from computers, operating systems, applications, media players, tablets, smart TVs, smartwatches, and smartphones (Aljafari, 2016). Apple was the world's largest publicly traded company (ibid.) and had left a considerable footprint in the global mobile phone industry: it was the second-largest mobile phone producer globally and founded "iReligion" with fanatic followership (Pogačnik and Črnič, 2014).

The smartphone industry players envisioned many opportunities. Opportunities for phone manufacturing companies included but were not limited to expanding operations through the development of new Internet of Things devices and technologies, building sustainable relationships with consumers through solid trade-in programmes, and applying circular business models to offset the negative impact of a high rate of product obsolescence (Aljafari, 2016; Watson et al., 2017). However, in addition to growth and business opportunities, the global mobile phone industry, and Apple specifically, faced significant challenges (cf. Aljafari, 2016), cargo thefts being one of them. Apple's iPhones were among the most expensive smartphones on the market, and because of this, they were the most stolen worldwide (Hodkinson, 2019).

15.4. Cargo thefts and the global mobile phone industry

The threat posed by cargo thieves compromised supply chain security and raised concerns about supply chain vulnerabilities (Farrell, 2015; Justus et al., 2018). Cargo thefts – the illegal "subtraction of goods for resale when they are being transported" (Justus et al., 2018, pp. 297–323) – were a risk for economic losses, a concern for the safety of employees involved in logistics, and a matter of companies' brand images (IUMI, 2019).

Targeted products were CRAVED goods (concealable, removable, available, valuable, enjoyable, or disposable). Such products had a high demand in grey and black markets, driving the unanimous interest of OCGs in these items (ibid.). British Standards Institution and TT Club report (BSI and TT Club, 2021) indicated several global cargo theft trends: electronic goods, including smartphones, were the third most stolen commodity; most of the thefts were

committed from cargo-in-transit (71% of all thefts), and some were directly from warehouses (24%); cargo theft types included hijacking (30%), theft from container/trailer (11%), theft of vehicle (11%), theft from a facility (24%), and others; North America, Europe, and South America were the continents with the highest theft rates (ibid.).

15.4.1. Actions of various stakeholders to tackle cargo thefts

Some stakeholders had taken initiatives to mitigate cargo thefts. TAPA issued protective measures such as freight, truck, parking security requirements, and supply chain cyber security standard. German Insurance Association published a manual for high-security truck parks. The EU Commission launched a body that disseminated truck parking security and theft prevention strategies and funded "Project RoadSec", providing security toolkits (cf. European Commission, Directorate-General for Mobility and Transport, 2019). Besides these, several countries in Europe and South America had launched initiatives such as "Project CARGO", "Operation Grafton", "Fight Against Transport Crime," which attempted to target and neutralise OCGs (cf. IUMI, 2019). Furthermore, IUMI, TT Club and BSI had provided recommendations to authorities and the global logistics industry for reducing cargo thefts (e.g., IUMI, 2019; BSI and TT Club, 2021). However, these were general measures meant to prevent cargo thefts in all industries, and specific solutions for smartphone cargo thefts were needed.

Considering that the price of premium smartphones had increased by 490% over the last two decades, increasing OCGs' interest in them was understandable (Ali, 2020). Stakeholders of the global mobile phone ecosystem had to take necessary steps to ensure that there was little to no incentive to steal smartphones by rendering the device useless to thieves and/or significantly increasing the risk of failure of such cargo heists.

25.4.1. Ecosystem loopholes that allowed smartphone cargo thefts to thrive

Multiple stakeholders within the ecosystem had to collaborate to tackle smartphone cargo thefts. In addition to the phone manufacturers in the global mobile phone industry, other key stakeholders, such as mobile network operators (MNOs), freight forwarders, national and international law enforcement bodies, governments, retailers and e-commerce platforms, insurers, international institutions (e.g., GSMA, CTWA, International Telecommunication Union, TAPA), and an international transport and logistics body TT Club had to be involved

(Farrell, 2015; Moran, 2018). The stakeholders were interdependent, but each of them had a unique role in the ecosystem.

For example, GSMA was a member-led organisation representing the global mobile phone industry and included over 1,050 MNOs, phone manufacturers, vendors, and suppliers of the mobile phone ecosystem. Using Unique Device Identification system, GSMA assigned an International Mobile Equipment Identity (IMEI) number to each phone. IMEI could be tracked as it was added to GSMA's centralised database of IMEI (GSMA IMEI DB) that was accessible only to members. GSMA IMEI DB contained a "blacklist" of IMEIs that should have been denied access to networks. MNOs could use this "blacklist" worldwide to prevent stolen phones from accessing the network even if the SIM card was changed. Members of the ecosystem with information on the IMEIs of stolen phones had to update the GSMA IMEI DB to make this information available to other members, including MNOs in countries where stolen phones were shipped and sold in the black market.

However, GSMA IMEI DB was not universally used or updated for numerous reasons, such as procedural barriers and a lack of incentive for stakeholders to become members of GSMA (cf. Farrell, 2015; Romero, 2018). Thus, Apple and some other phone manufacturers or MNOs were not members of GSMA (GSMA, n.d.). Less than 5% of the countries in Asia and Africa were connected to the GSMA IMEI DB and could access this "blacklist" (Romero, 2018). Instead, MNOs in each country had their databases of blacklisted IMEIs that they may or may not have shared with other MNOs or the national Central Equipment Identity Register (CEIR) maintained by the government. Several governments did not even possess a CEIR. Therefore, local MNOs that were not a part of GSMA did not have the opportunity to share their private databases with other stakeholders at the national or international levels using CEIRs (Moran, 2018). Such a situation was problematic because it was estimated that most of the stolen cargo from North America and Europe was shipped to emerging markets (Romero, 2018). Moreover, maintenance of just a blacklist was ineffective because of several other loopholes that OCGs had used to ensure that the "fingerprint" or the IMEI of the blacklisted device was untraceable (ibid.).

Due to these loopholes, the implementation of blacklisting IMEIs of stolen devices had been problematic, owing to which demand in the black market was thriving (Farrell, 2015). OCGs used these loopholes to their advantage by shipping the stolen cargo to other countries, where devices could easily access the local networks and remain operational, deepening the crisis in

the smartphone industry. Thus, a global solution involving a database with widespread acceptance and ease of access had been required for some time. Moreover, the feasibility of restricting network access to unauthorised IMEIs (locally and globally) was critical for the successful implementation of the said solution.

15.5. Effects of the global pandemics on Apple and the smartphone industry

The pandemic affected the global smartphone industry from Q1-2020 when the market declined 13% year-on-year (YoY). In Q2-2020, there was a 20% decline in global smartphone sales. Smaller brands relying majorly on offline channels struggled the most. However, Q1-2021 saw global shipment growth of 20% YoY (Counterpoint Technology, 2022).

The pandemic impacted the largest players in the industry as well, but differently. In Q1-2020, Samsung secured market leadership, and Apple remained stable with only a 5% decline in iPhones shipment. In Q2-2020, the USA, Latin America, Europe, and India struggled with the national lockdowns, which severely affected Samsung, whose sales declined 29% YoY. Whereas Apple shipments and revenues grew because the iPhone 11 sales gained momentum and the long-awaited iPhone SE was launched. In Q3-2020, Samsung regained the first rank, and the top ten companies saw growth attributed to 5G technology, for which a strong demand was present despite the pandemic. Recovery had been in full swing since Q4-2020, with fierce competition between the two players, Apple and Samsung (Counterpoint Technology, 2022).

15.5.1. Cargo thefts in the smartphone industry during the COVID-19

During the COVID-19 pandemic, consumer electronics remained the third most stolen category (BSI and TT Club, 2021), but the nature of and the possibilities for cargo theft changed. Continuous lockdown meant that the ability to perform in-transit crime operations had reduced (BSI and TT Club, 2021). Consequently, smartphone cargo thefts were projected to spike in the post-lockdown era, as OCGs were expected to reclaim their delayed “income” (BIFA, 2021). However, during the Great Lockdown, goods were stockpiled in warehouses with minimum security. This increased criminals’ access to goods and resulted in increased thefts from facilities from Q1-2020 through Q3-2020 (BSI and TT Club, 2021). In Q4-2020, trade and shipments resumed worldwide, explaining the trend shift of most thefts from facilities to cargo-in-transit. Furthermore, truck drivers parked in unsecured locations because of the

lockdown, increased regulations, border controls, and COVID-19 testing. The latter increased the vulnerability of cargo-in-transit and opened new opportunities for organised thefts (ibid.).

Finally, COVID-19 affected the incomes of employees, including those working in the logistics industry. Because of this income decline, employees were more likely to give internal company information to thieves in exchange for money. Such conditions reinforced the commonly used mode of operations when crime groups recruit company employees to leak information about the cargo planned to be stolen (BSI and TT Club, 2021).

Amid the pandemic, in June 2020, Apple's competitor Samsung announced joining forces with Trustonic, a cybersecurity company, and planning to adopt Asset Lifecycle Protection Service to secure Samsung's phones from thefts (Samsung Knox News, 2020). LG was also collaborating with Trustonic for this purpose (BusinessWire, 2020). However, Apple did not take any measures to tackle cargo thefts. In November 2020, £5 million worth of iPhones were stolen from a truck (BBC, 2020) again, reminding us of Apple's need to tackle two interacting crises.

15.6. Taming the crises

David began drafting issues needed to prevent multiple crises caused by cargo thefts and the pandemic. David was seeking short- and long-term solutions. It was evident that re-imagination and reform were required within the company and the ecosystem, otherwise resolution could not be reached, questioning Apple's resilience. What actions should Apple take to ensure the security of its shipments? How to protect the company's brand from the damage caused by illegal sales of Apple's stolen products? How to prepare for a potential increase in thefts in a post-pandemic era? David leaned back in his chair and sighed, desperately thinking about possible solutions.

David wanted to remain open-minded but systematic (McNulty and Marcus, 2020) when envisioning solutions. Thus, David adopted a multi-disciplinary approach for CM (Pearson and Clair, 1998) and searched for solutions across the research disciplines. For example, David was investigating how takeaways from companies' coopetition (a collaboration of competitors) in marketing to cope with the crises caused by COVID-19 (Crick and Crick, 2020) could be helpful in CM at Apple. Similarly, David was ready to consider *technological-structural* (e.g., blockchain innovations for supply chain management; Lim et al. 2018; Sissman and Sharma,

2018; Kshetri, 2021), *socio-political* (e.g., industry norms and interactions of stakeholders in the ecosystem), and *psychological aspects* (e.g., biases that prevent rational decision-making; Pearson and Clair, 1998) in CM. These considerations would have supported David in realising what *types* of crises Apple is facing, what *systems* are relevant to manage the crises, and which *stakeholders* should be involved in the solution (cf., Pearson and Mitroff, 1993).

15.7. The teaching note

This teaching note comprises three parts. First, we briefly summarise the case from the instructor's point of view. Second, we introduce learning objectives and suggest readings to support the instructor and students when analysing this case. Finally, we provide teaching strategies for in-class or online courses and elaborate on the potential discussions that should enhance learning from this case.

15.7.1. Instructor's summary

This teaching case is designed to provide an overview of the conditions in which a crisis of a case company – Apple – occurs. The primary goal of this case is to demonstrate that crisis does not happen in a vacuum. Instead, it involves managing multiple stakeholders (McNulty and Marcus, 2020) in various countries through different stages of crisis (Coombs and Laufer, 2018). Thus, if the company wishes to regain resilience and succeed in managing crisis, it has to adopt holistic, multi-disciplinary thinking (Pearson and Clair, 1998) and re-imagine the future in its ecosystem in addition to taking present company-level actions (McNulty and Marcus, 2020).

The case elaborates on two situations that cause crises for Apple. First is the ongoing challenge – cargo thefts – that Apple and other mobile producers in the industry have been experiencing for decades (Farrell, 2015). Second, the case presents a recent disaster: the COVID-19 pandemic. The pandemic creates disruptions in global supply chains and worsens economic conditions, elevating the ongoing cargo theft challenge. Thus, being a highly successful company that managed to demonstrate growth in shipments and revenues even during the pandemic, Apple has not yet tackled the crisis caused by cargo thefts.

David, Apple's international logistic manager and the protagonist in the case, realises that crises caused by cargo thefts need to be managed, especially now, when its elevation is likely after the pandemic. David also understands that specific solutions are within Apple's hands, but best and long-term solutions require collaboration across stakeholders in the industry. The case provides a detailed account of how the critical stakeholders in the global mobile phone

industry interact to illustrate the reasons behind David's thinking. However, the current stakeholder efforts are insufficient. Thus, by the end of this case, students are invited to systematically analyse conditions in the industry and the effects of multiple factors that cause crises for Apple. Moreover, students are invited to create solutions, which would allow Apple to gain back its resilience and mitigate cargo thefts. Students' analysis is directed by suggesting some core CM principles available in the academic literature.

25.7.1. Learning objectives and study material

The case has several learning objectives. The learning objectives for *undergraduate*-level studies are as follows:

1. To learn analysing crisis causes and consequences, also crisis caution (steps taken to prevent crisis) and coping (steps taken to address the crisis that occurred);
2. To explore three phases (the pre-crisis, the crisis, and the post-crisis) of global CM and understand how these phases interact; and
3. To learn designing crisis prevention and management solutions that a single company can implement.

The readings that could support the instructor when teaching this case for undergraduate students (these readings can also be assigned for students): Pearson and Mitroff (1993); Pearson and Clair (1998); Coombs and Laufer (2018).

The additional learning objectives for *MBA and MSc*-level studies (learning goals 1–3 stated earlier also apply to MBA and MSc-level) are as follows:

4. To learn envisioning possibilities of industry stakeholder collaboration and adoption of technological innovations for crisis prevention in long-term; and
5. To learn evaluating factors that define CM success or failure.

The additional readings for the instructor and the students in master's degree programmes could be Lim et al. (2018), Sissman and Sharma (2018), Crick and Crick (2020), and Kshetri (2021). These studies would help re-imagining the way stakeholders in the ecosystem operate.

35.7.1. Teaching strategies and questions for case analysis

When discussing the following questions, the case can be taught in a classroom (60 or 90 minutes, depending on the study level). On the other hand, the case can be assigned as a group assignment. Every group (consisting of four to five students) could analyse the questions and design a potential solution for Apple. In the later teaching strategy, in the synchronous course,

students can be asked to make a group presentation followed by a question-and-answer session for each group. Alternatively, in the asynchronous course, students can be asked to record their presentation with the company's analysis and solution and place this recording in a virtual forum for further virtual discussions with their classmates.

Regardless of the teaching strategy applied, we present the questions that can be used when analysing this case. The list is not exclusive, and instructors are welcome to incorporate additional questions that are appropriate for their course.

- According to the case, what kinds of crises is Apple experiencing? What are the reasons for these crises?

Potential answer: Apple is experiencing two critical situations. One is ongoing (cargo thefts), and the other one has recently emerged (COVID-19). These critical situations create crises related to the company's security, infringement of its copyrights, and, therefore, damage to Apple's brand. The two critical situations interact, and COVID-19 escalates cargo theft challenges. Reasons for cargo theft-related crises are the premium price of Apple phones, loopholes in the industry ecosystem, the insufficient collaboration of stakeholders in the industry, and limitations of technological solutions currently applied. Reasons why COVID-19 escalates the crisis caused by cargo thefts: effects of lockdown (new opportunities for thefts, diminished cargo security, "lost" criminal incomes due to lack of mobility) and increased probability of leaking information for money due to reduced income of employees working with cargo.

- How did COVID-19 affect Apple's operations? In your opinion, what has caused more harm for Apple, cargo thefts or COVID-19? Why do you think so?

Potential answer: COVID-19 has disrupted the flow of supply chains for Apple and reduced the overall purchasing power of its potential customers. However, in Q2-2020, Apple managed to show growth in shipments and revenues. COVID-19 was a shared, temporary challenge for all industries. Its presence did not create any specific damage for Apple's business, as the need for a mobile phones due to an ongoing isolation has only increased during the pandemic. COVID-19, however, had indirect effects. Pandemics made other problems, such as cargo thefts, in the mobile phone industry acute.

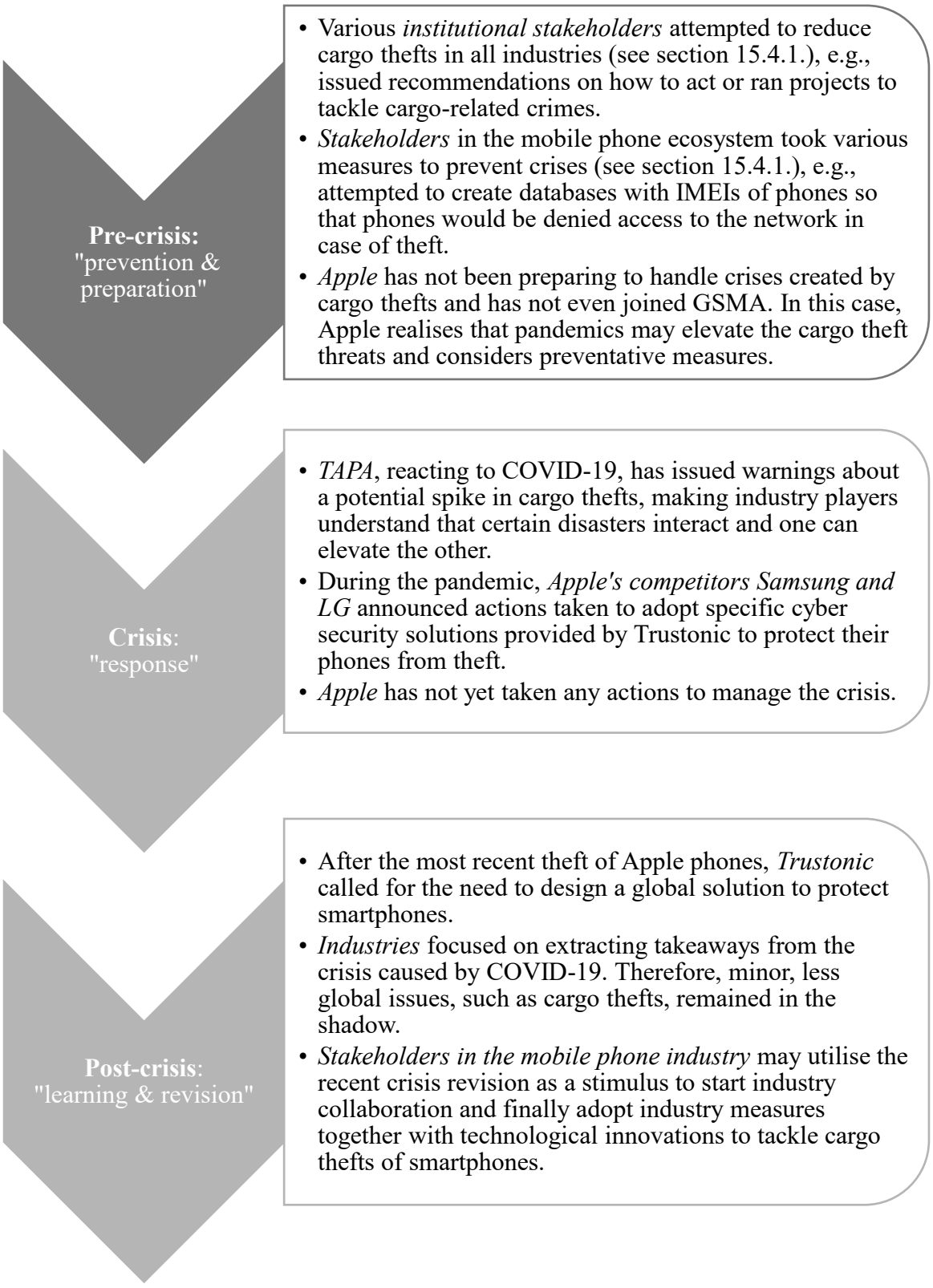
Cargo thefts constantly harm Apple's business. When theft is committed, Apple faces short-term damages: loss of assets, unwanted negative media coverage, and security-related concerns

from its stakeholders. Cargo thefts create long-term damages, too, such as infringement of its copyrights (when products are resold on the black market) and, therefore, harm to its brand, increased consumer dissatisfaction, and doubts about Apple's technological capabilities. Cargo thefts may also reduce supply chain partners' interest to work with Apple, given that Apple's phones are stolen the most. Thus, despite the extensive debates about the crisis caused by COVID-19, crises caused by cargo thefts are very likely to harm Apple more in both the short and long term.

- How have Apple and various other stakeholders in the ecosystem behaved during the three phases of the global crisis (Coombs and Laufer, 2018)? How were all stakeholders attempting to manage: *the pre-crisis*, *the crisis*, and *the post-crisis*? How can Apple's behaviour in CM be explained?

A potential answer is provided in Figure 15.1.

Figure 15.1 CM by Apple and the ecosystem in different phases (framework adapted from Coombs and Laufer, 2018)



Apple's inaction in CM can be explained in several ways. Apple may *perceive* that harm caused by cargo thefts is smaller than the efforts and investments needed to mitigate cargo crimes. Apple may use the publicity created by cargo thefts to strengthen the perception of the

desirability of Apple phones. Apple may not be aware of the ways to manage these crises and is postponing the decision until an easy and cost-effective solution is available. Apple may be designing a solution to secure its phones internally without communicating about it to the public.

- What potential solutions could Apple implement to manage the crises caused by cargo thefts and prevent its elevation after the pandemic? Discuss possible solutions that Apple could implement (a) as a single company and (b) as an industry player.

(a) *Potential company-level solution "security measures":* Apple can take internal measures towards the protection of trucks, thereby reducing the probability of thefts occurring and increasing the risk of failure of thefts when they are carried out. This option does not directly tackle the demand in the black market, but it is one that all companies can implement. Criminal opportunity can be reduced by ensuring loaded vehicles are always secure, attended, and never parked in vulnerable locations. Additionally, due diligence in the employment process for Apple is imperative to reduce the likelihood of "insider jobs" occurring. Apple could ensure that working conditions in its supply chain are at the highest standard, lessening employee motivation to seek extra income. Employees should be trained about needed security measures.

Strategies must be in place to deflect criminals from storage areas by upgrading security. Apple could incorporate blockchain technology in logistics, moving towards Supply Chain 4.0, to ensure that confidential information is not leaked and that operations are faster, transparent, and secure (DHL Trend Research, 2018). Furthermore, Apple could follow the lead of Samsung and LG in collaborating with a cybersecurity company, Trustonic (BusinessWire, 2020; Samsung Knox News, 2020), i.e., Apple could subscribe to Asset Lifecycle Protection Service (ALPS) to prevent thefts. Trustonic's ALPS binds the IMEI in the device's chipset cryptographically. Such binding means that illegally reprogramming the IMEI would not be possible, and the device would remain blocked from networks worldwide. This embedded cybersecurity measure would prevent street crimes and would partially reduce organised supply chain thefts. However, the downsides of this solution are (i) hardware modifications in phones must be made during production, so (ii) it would not work on stolen smartphones that are already in use, and (iii) this solution would entail the global industry's heavy

reliance on one single for-profit corporation: Trustonic, and would require that companies pay vast sums of money to Trustonic to avail ALPS.

(b) *Potential ecosystem-level solution "GSMA membership":* This solution tackles many of the shortcomings listed earlier. However, it is more challenging to implement because of the need to proactively involve many stakeholders. Nevertheless, if implemented, the solution would directly slash existing demand for stolen phones in the black market, leaving crime groups with no incentive to carry out cargo thefts. Apple could lead industry debate encouraging as many as possible stakeholders to join the GSMA and subscribe to existing IMEI databases. Nonetheless, governments would have to mandate all stakeholders' membership and subsequent participation in this centralised database maintained by GSMA. Governments would also have to maintain national CEIRs, which would then be continually synchronised with GSMA's database. Stakeholders, including GSMA, would need to understand that maintaining just a blacklist is not sufficient, and the need for comprehensive and updated white- and grey-lists is also necessary to avoid illegal reprogramming of IMEI. These actions would ensure no duplication of active IMEIs and that invalid IMEIs not assigned by GSMA were not operating in any network (cf. Romero, 2018). Once these steps are taken, only then would this solution prove to be effective.

- (If taught in MBA, MSc. class) How could technological innovations, such as increasing blockchain adoption, support Apple in re-imagining the global mobile phone ecosystem and preventing cargo thefts?

(c) *Potential ecosystem-level solution of the near future "blockchain database":* blockchain technology provides an innovative solution for IMEI authentication through a common, easily accessible, exhaustive database of IMEI white, grey, and blacklists. Owing to blockchain technology's distributed peer-to-peer nature, all the stakeholders could directly participate in a blockchain network to store and share information about stolen devices worldwide. Such a blockchain-based global database would help overcome the loopholes by reducing costs, preventing duplication of data, avoiding downsides of bureaucracy by removing layers of intermediaries, improving *accessibility* for stakeholders, and ensuring that the threat of data breach is negligible due to blockchain consensus mechanisms (cf. Deloitte, 2017; Lim et al., 2018).

As a first step towards a safe ecosystem with increased trust and data security for stakeholders, a Consortium Blockchain (CB) concept could be applied. CB is a hybrid between "low-trust" public blockchains and a "single highly-trusted entity" model of private blockchains. Therefore, CB could be used to create a decentralised global database of IMEI that is easily accessible to all stakeholders in the smartphone industry ecosystem (Lim et al., 2018). Governments would need to mandate the participation of all stakeholders in the CB (especially MNOs) because the IMEI authentication of devices and subsequent blocking of unauthorised and/or blacklisted IMEIs would be carried out at the LTE-MME nodes that local MNOs maintain (RCR Wireless News, 2014). The LTE-MME nodes are structures that authenticate mobile devices before allowing them to connect to the network to make calls, send SMS, and access the internet (ibid.). Unlike former efforts, this approach is open to different stakeholders and is de-monopolised and transparent, thereby creating more stimulus and incentives to implement a globally accepted solution.

- (If taught in MBA, MSc. class) How well has Apple managed the crisis caused by cargo thefts so far? How would the envisioned solutions allow reaching CM success? What would still potentially result in CM failure?

The potential answer is provided in Table 15.1.

Table 15.1 Analysis of Apple's CM and success of the potential solution (framework adapted from Pearson and Clair, 1998)

Crisis Concern	Evaluation
Signal Detection	The signals of potential crises caused by cargo thefts have been present for some time; however, Apple has expressed little reaction. The latter indicates CM failure. In this case, however, David can sense increased intensity, notice relevant reports, and understand potential emergencies coming. At this stage, providing good working conditions for the employees and training them to take security measures may cause early detection of signals, as employees would report if suspicious actions would come to their attention.
Incident Containment	Incidents were contained very little so far, indicating CM failure. However, solution (a) "security measures" – reduces thefts and ensures there are no injuries and/or deaths of truck drivers (partial success)**;**

	solutions (b) “GSMA membership” and (c) “blockchain database” – prevent the crises (complete CM success).
Business Resumption	Even on the occasions of theft, Apple’s business was operating with minor disturbances and delays. Thus, crises were at least partially managed from this perspective. However, implementing the proposed solutions would ensure business continuity without losses (complete success in CM).
Effects on Learning	According to the case, Apple made little effort to analyse previous crises. However, there has been some pondering on the ecosystem conditions in which re-occurring crises happen (minimal CM). For achieving complete CM success, organisational learning should involve a deep analysis of the crises’ *Cause* and *Consequence*, including the interplay between cargo thefts and COVID-19. This learning would improve the *Caution* aspect. Finally, implementation of proposed solutions would lead to *Coping* with crises and consequently towards the restoration of the company’s resilience.
Effects on Reputation	Cargo thefts lead to short-lived adverse effects on Apple’s reputation. Consumption of Apple’s products was not affected by this negativity. On the contrary, the perception of the desirability of Apple phones might have increased (partial CM success). By taking leadership and establishing successful solutions as proposed in (b) and (c), Apple would shift from being a “victim” to being a “hero”, reassuring its leadership in the market and technological innovations (complete CM success).
Resource Availability	Apple is one of the most resource-rich companies in the world (Szmigiera, 2021). Thus, the availability of tangible resources is neither an issue for Apple nor for the other well-established stakeholders in the industry who would need to implement the solutions proposed. However, trust and collaboration, the intangible resources crucial for enacting solutions, are missing (partial CM success). Blockchain features allow for overcoming a lack of trust, and therefore blockchain adoption would result in complete CM success.
Decision-making	Unlike other industry leaders, e.g., Samsung or LG, Apple has not taken any decisions to manage cargo theft-related crises. There are external

constraints for some solutions, but decisions that a company could make on its own (e.g., solution (a)) have also been avoided (CM failure). If Apple would finally take some steps to act, CM would be significantly better.

References

Ali, R. (2020, July 24). *Mobile phone prices soar over 20 years.* Uswitch. https://www.uswitch.com/mobiles/news/2020/07/mobile-phone-prices-soar-over-20-years/

Aljafari, A. (2016). Apple Inc. industry analysis – Business policy and strategy. *International Journal of Scientific and Engineering Research*, 7(3), 406–441. https://www.ijser.org/researchpaper/Apple-Inc-Industry-Analysis-Business-Policy-and-Strategy.pdf

BBC. (2020, November 17). *Apple products worth £5m stolen from lorry on M1*. https://www.bbc.com/news/uk-england-northamptonshire-54972784

BIFA. (2021). *TAPA warns of a significant spike in cargo thefts as criminals get back to 'business as usual*. British International Freight Association. https://www.bifa.org/news/articles/2020/jun/tapa-warns-of-a-significant-spike-in-cargo-thefts-as-criminals-get-back-to-business-as-usual

BSI and TT Club. (2021, February 22). *Cargo theft report 2021*. https://www.ttclub.com/-/media/files/tt-club/bsi-tt-club-cargo-theft-report/2021-02-23---bsi-and-tt-club-cargo-theft-report-2021.pdf

BusinessWire. (2020, April 22). *Trustonic security to be implemented in LG Mobile Smartphones*. https://www.businesswire.com/news/home/20200422005064/en/Trustonic-Security-to-be-Implemented-in-LG-Mobile-Smartphones

Coombs, W. T., and Laufer, D. (2018). Global crisis management – current research and future directions. *Journal of International Management*, 24(3), 199–203. https://doi.org/10.1016/j.intman.2017.12.003

Crick, J. M., and Crick, D. (2020). Coopetition and COVID-19: Collaborative business-to-business marketing strategies in a pandemic crisis. *Industrial Marketing Management*, 88, 206–213. https://doi.org/10.1016/j.indmarman.2020.05.016

Counterpoint Technology. (2022, February 8). *Global Smartphone Market Share: By Quarter.* Counterpoint Research. https://www.counterpointresearch.com/global-smartphone-share/

Deloitte. (2017). *Blockchain and cyber security.* https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/technology-media-telecommunications/Blockchain-and-Cyber.pdf

DHL Trend Research. (2018). *Blockchain in logistics.* https://www.dhl.com/content/dam/dhl/global/core/documents/pdf/glo-core-blockchain-trend-report.pdf

European Commission, Directorate-General for Mobility and Transport. (2019). *EC security guidance for the european commercial road freight transport sector: ROADSEC security toolkit.* Publications Office of the European Union. https://doi.org/10.2832/97074

Farrell, G. (2015). Preventing phone theft and robbery: The need for government action and international coordination. *Crime Science*, 4(1), 1-11. https://doi.org/10.1186/s40163-014-0015-0

GSMA. (n.d.) *Membership – Our Members.* https://www.gsma.com/membership/membership-types/

Hodkinson, T. (2019). *Smartphone crime is growing – how do we turn the tide?* Trustonic. https://www.trustonic.com/opinion/smartphone-crime-turning-the-tide/

IUMI. (2019). *Cargo theft prevention – position paper*. *September.* 1–5. International Union of Marine Insurance. https://iumi.com/document/view/Cargo_Theft_Prevention_17_September_2019__5d721c8003199.pdf

Justus, M., Ceccato, V., Moreira, G. C., and Kahn, T. (2018). Crime Against Trading: The Case of Cargo Theft in São Paulo. In V. Ceccato, and R. Armitage (Eds.), *Retail crime: International evidence and prevention – crime prevention and security management*, (pp. 297–323). Palgrave Macmillan. https://doi.org/10.1007/978-3-319-73065-3_12

Kshetri, N. (2021). *Blockchain and supply chain management.* (1st ed.). Elsevier. https://doi.org/10.1016/C2020-0-02868-9

Lim, S., Fotsing, P., Almasri, A., Musa, O., Kiah, M., Ang, T. and Ismail, R. (2018). Blockchain technology the identity management and authentication service disruptor: A survey. *International Journal on Advanced Science, Engineering*

and Information Technology, 8 (4-2), 1735–1745. https://doi.org/10.18517/ijaseit.8.4-2.6838

McNulty, E. J., and Marcus, L. (2020). Are you leading through the crisis…or managing the response. *Harvard Business Review*. https://hbr.org/2020/03/are-you-leading-through-the-crisis-or-managing-the-response

Moran, J. (2018, July 23). "*Combatting device crime together – best practice to combat mobile device theft*" [Conference session]. International Telecommunication Union Workshop. Geneva, Switzerland. https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180723/Documents/Combatting%20Device%20Crime%20Together.pdf

O'Dea, S. (2021, December 16). *Cell phone sales worldwide 2007–2020*. Statista. https://www.statista.com/statistics/263437/global-smartphone-sales-to-end-users-since-2007/

Pearson, C. M., and Clair, J. A. (1998). Reframing crisis management. *Academy of management review*, 23(1), 59–76. https://doi.org/10.2307/259099

Pearson, C. M., and Mitroff, I. I. (1993). From crisis-prone to crisis prepared: A framework for crisis management. *Academy of Management Perspectives*, 7(1), 48–59. https://doi.org/10.5465/ame.1993.9409142058

Pogačnik, A., and Črnič, A. (2014). iReligion: Religious elements of the Apple phenomenon. *Journal of Religion and Popular Culture,* 26(3), 353–364. http://dx.doi.org/10.3138/jrpc.26.3.353

RCR Wireless News. (2014, May 9). *LTE MME: A core connector for LTE.* https://www.rcrwireless.com/20140509/diameter-signaling-controller-dsc/lte-mme-epc

Romero, H. (2018, July 23). *Global approaches on combating counterfeiting and stolen ICT devices* [Conference session]. International Telecommunication Union Workshop. Geneva, Switzerland. https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180723/Documents/5_Hugo_Romero.pdf

Samsung Knox News. (2020, June 25). *Trustonic forms a global partnership with Samsung to provide class leading device security for mobile operators.* https://www.samsungknox.com/en/blog/trustonic-forms-a-global-partnership-with-samsung-to-provide-class-leading-device-security-for-mobile-operators

Sissman, M. and Sharma, K. (2018). Building supply management with blockchain. *Industrial and Systems Engineering at Work,* 50(7), 43-46.

Szmigiera, M. (2021, September 10). *The 100 largest companies in the world by market capitalisation in 2020.* Statista. https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-capitalization/

Watson, D., Gylling, A. C., Tojo, N., Throne-Holst, H., Bauer, B., and Milios, L. (2017). Circular business models in the mobile phone industry. *Nordic Council of Ministers Secretariat.* https://doi.org/10.6027/TN2017-560

---

[1] The case was designed upon publicly available information.

[2] David Talbot is a fictional name created for this case.