

Apple

Crisis Communication Plan

Bobby Schutts, Taylor Argabright, Natalie DeLeon,
Makenna Buckskin, Abigail Cowan

TABLE OF CONTENTS

Introduction	3
Statement from Management to Employees	4
Definitions	6
Crisis Inventory	8
Warning Signs of a Possible Crisis	9
Audiences During a Crisis	11
Methods of Communication During a Crisis	13
Communications Procedure for Handling a Minor Crisis	15
Communications Procedure for Handling a Major Crisis	16
Emergency Operations Center (EOC)	18
Crisis Team & Communication Chain	20
Crisis Directory & Contact List	22
Crisis Management Plan: Spyware Attack	25
Crisis Management Plan: Faulty Products	28
Crisis Management Plan: Employee Unrest	30
Identification of a Spokesperson	32
Guidelines for Spokespeople	33
Format for Briefing Someone Identified as a Spokesperson	36
Example of Initial Statement for Release	37
Sample News Release	40
Background Statement	42
Fact Sheet	43



Sample Letters to Stockholders	45
Website	49
Social Media	50
Messages for the News Media During an Employee Unrest Crisis	51
Messages for the News Media During a Spyware Attack Crisis	52
Messages for the News Media During a Faulty Product Crisis	53
Possible Questions and Suggested Responses	54
Pre-Gathered Information	57
URLs for Resources	58
Evaluation of Plan Effectiveness After a Crisis	59

INTRODUCTION

Apple is dedicated to remaining at the forefront of technology, innovation, and above all else: satisfying the customers. We want to always be breaking the boundaries of what is possible and we are always finding ways to improve not only our products but the world. In order for Apple to consistently break barriers, we must be prepared for any crisis that tries to knock us off our path of being the greatest technology company in the world. We strive to be prepared for any crisis. Whether it be external or internal, whether we are the victims or we are at fault, we strive to rectify situations and come out of a situation better than we were before.

This plan will explicitly state how to handle crises that have happened to us before, and crises that if they were to ever happen, we are now prepared for. Every employee of Apple should be familiar with this plan to ensure the effectiveness of plans that could determine the future of this company. Being prepared for crises is something that has been proven to be crucial to the success that Apple has seen, and the strict following of this plan will have tangible, dramatic improvements in success and reputation.

If a crisis were to happen and this plan was disregarded, it would be detrimental to the company, its employees and all the progress we have made in decades of groundbreaking business. Each and every employee has the power to utilize this crisis plan and solidify a future of success and excellent crisis management.



STATEMENT FROM MANAGEMENT TO EMPLOYEES

Tech is a field defined by constant change and innovation. As the go-to retailer for technology, business, education and entertainment, there are many issues we must be prepared for. Consumers depend on us to provide them with an efficient and simple process to connect them to the rest of the world. Apple's mission statement is to bring the best user experience to customers through innovative hardware, software and services. Especially in technology, there is a heightened risk of data breaches and spyware, supply chain issues, faulty products and inappropriate employee behavior. Because of these dangers, it is crucial that Apple employees and executives are prepared to deal with the media and the public quickly and efficiently in the event of a crisis. We bring the best user experience to our customers through innovative hardware, software and services and must be prepared for relevant crises to occur.

We have worked diligently and consistently to build a pristine reputation with the public for providing innovative, simple and clean technology products that allow our consumers to connect with the world around them. Because the most damaging scare in technology is spyware and data breaches, it is crucial that Apple be prepared for any possible circumstances involving a user of our product being affected by spyware on their devices. With the rise in spyware like the Pegasus software, we need to be continually aware of how these spyware programs affect our consumers. In order to prevent harm to our consumers, and damage to our company as a result, we must remain actively aware of how these programs affect other companies, and how they communicate with the media and the public.

If this crisis communications plan is not followed in the event of a crisis, irreparable damage to the reputation of Apple is possible. The loss of trust among our customers could also lead to a large drop in sales. In handling this crisis plan, we must not forget that trust and reliability are incredibly important to customers when choosing where to purchase their technology, and Apple must protect its reputation as a reliable technology provider. We trust that all employees will keep up their exceptional work in order to protect our company from such a crisis.

Purposes

In the event of a victim or preventable crisis situation, we must take immediate action to inform our publics of the situation and the measures they need to take. Our open and honest transfer of information to the media and product owners will

eliminate confusion among our publics. By being straightforward and sincere, the crisis situation can be more smoothly resolved and action can be taken to eliminate any further problems. We are bringing the best user experience through innovative software, hardware and services, so spyware outbreaks would be harmful to this reputation.

Objectives

We will make every effort to:

1. Initiate the crisis communications plan within 2 hours of the crisis outbreak in the event of a suspected spyware outbreak or data breach in the products that we have released.
2. Inform all consumers with affected devices, including those at risk.
3. Inform all owners and managers within 3 hours of the outbreak.
4. Inform the media and store managers within 4 hours of the outbreak.
5. Keep the media and all public regularly informed of updated information through regular news conferences and updates to the company's social media platforms.
6. Maintain honesty with the media about all known information.
7. Find the source of the outbreak as soon as possible.
8. Distribute our findings to the media and all publics.
9. Develop ways to safeguard against future problems.
10. Implement necessary changes as soon as possible and resume business as usual



DEFINITIONS

Crises

The plural form of crisis. Events that disrupt regular business functions, cause stakeholder unrest and have the potential to damage the company's reputation.

Stakeholder

Primary stakeholders are people who have a direct interest in an organization, like employees or investors. Secondary stakeholders are people who have indirect interests, like the local community or the media (Gregory, 2015)

Crisis Communication Plan

A plan created by communications professionals in adherence to company ambitions, values and practices that are approved by board members and executed throughout the company in the event of a crisis. A crisis communication plan is meant to reduce harm to the company and its stakeholders.

Crises Categories

As a global tech company, Apple's key crisis categories are the economic, social, political and technological types.

Data Breach

Exposure of sensitive information or protected data by cyber attackers.

Spyware

Systems or software that retrieve user information covertly, or without consent, endangering the user or third parties.

Supply Chain Issues

Local or global shortages that disrupt regular product development pace and cause severe delays or halt production entirely.

Faulty Product

A product that malfunctions, does not meet standards clearly advertised by Apple, is damaged prior to the product sale, contains software or hardware errors, or is dangerous to its user.

Inappropriate Employee Behavior

Offensive, repeated and unreasonable behaviors such as, but not limited to discrimination, harassment, humiliation, bullying, displaying excessive need for control, threats, violence and impairment due to substance use.

Sexual Harassment

Apple does not condone sexual harassment, which includes but is not limited to: unwanted touching, repeated rejected advances, circulating explicit material, actual or attempted assault, suggestive comments, as well as pressure for sexual acts in exchange for or threatening of workplace advancement or lack thereof.

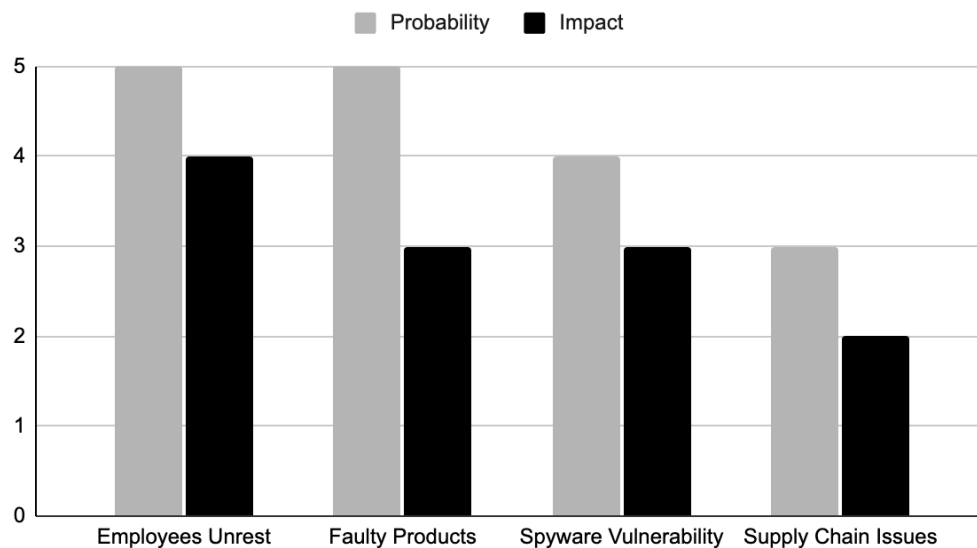


CRISIS INVENTORY

The following chart indicates four potential crises Apple could encounter. Based on previous crises that both Apple and their competitors have faced, malfunctioning products and features leading to faulty products (Watson, 2022), several hundred employees publicly spoke out about the work environment leading to employee unrest (Nicas & Browning, 2021), Covid-related disruptions and shortages leading to supply chain issues (McGee, 2022) and a software exploit leading to spyware vulnerability (Lyngaas, 2021) have been determined to be potential crises.

We have ranked the probability and potential impact of each crisis. The issue of employee unrest is highly probable with considerable damage. Faulty products are also highly probable with considerable damage. Spyware vulnerability is somewhat probable with considerable damage. Lastly, supply chain issues are possible but would likely only have some damage.

Apple Crisis Probability and Impact Chart



WARNINGS SIGNS OF POSSIBLE CRISIS

Employee Unrest

- Apple will host all-staff meetings to listen to and hear out the concerns of employees. Apple will create an open-door, confidentiality agreement with human resource employees. For staff to voice their concerns or potential threats to an HR director so that they can provide the employees with adequate resources and connect them to any next steps that need to be followed. This will prevent an uproar or upset in the company and social media while also providing specialized care to each employee's concern.
 - In 2021, Apple employees began a movement called #AppleToo to voice concerns about discrimination, harassment, abuse and many other issues within the company. In response, Apple's chief executive, Tim Cook, held an all-staff meeting to answer questions and listen to the concerns held by employees of the company. His response was seen by staff as a "notable acknowledgment that the workplace and social issues that have been roiling Silicon Valley for several years have taken root at Apple," (Browning & Nicas, 2001).

Faulty Products/ Technology Malfunctions

- Warning signs for technical malfunctions can be recognized early on by monitoring Apple's help/issue forum, and by creating a log of common problems brought into the Apple store. When a complaint about a system or a malfunction is commonly appeared Apple will adapt this problem in new IOS updates and inform customers that they are aware of the issue and are actively trying to create a solution.
 - In 2022, Apple's new emergency phone call feature raised many shocking applause as well as concerns with the watch's faulty system that accidentally calls the police at times with no potential danger. Apple released a new advertisement using real-life 911 calls to showcase the necessity and life-saving ability of this technology to promote its use (Watson, 2022).

Spyware Vulnerability

- Apple will regularly test its software to detect security vulnerabilities. If a vulnerability is detected. Apple will release a software update to prevent any



areas that are susceptible, and urge customers to download the newest update.

- In 2022, Apple detected issues within their software that could allow potential attackers to take over devices by retrieving arbitrary code and rendering websites to create “maliciously crafted web content.” In response, Apple urged their customers to update every device’s IOS software and Safari to the latest version of each Apple device (Manfredi, 2022).

Supply Chain Issues

- To help prevent supply chain issues, Apple will once again provide quarterly revenue guidance. Apple will monitor its supply chain to account for its more popular items in times of shortage.
 - Apple took a significant hit in its supply chain after Covid-19 created shortages, resulting in \$4 billion to \$8 billion in revenue loss. During the shortages, Apple attempted to adapt its systems and “prioritized the chips for iPhones rather than iPads.” Apple also made “aggressive moves to please Wall Street with buybacks and dividends” (McGee 2022).

AUDIENCES DURING A CRISIS

Internal Publics

Employees: Internal and Enabling Public

- Employees need to be updated honestly and swiftly during a crisis situation. A crisis can lead to layoffs, pay decreases, decrease in stock prices, etc..., so employees need to always be notified about company news. Updates on crisis situations can be sent out via email, phone, or by news releases from management.

Upper-Level Management: Internal and Enabling Public

- Upper-level management must have full knowledge of the situation at hand so they can tell the employees the relevant information and foster communication. Management will be sent all necessary resources if a situation is to arise and they will open channels for questions and concerns.

Shareholders: Internal and Enabling Public

- Shareholders need to be updated with absolute transparency with a clear focus on what will be done to assure a crisis will never be repeated. Trust is a core aspect for shareholders and accountability must be taken with shareholders, without shareholder trust a company can fold rapidly. When communicating with shareholders, there will be an emphasis on the ability to answer any question necessary to maintain trust.

External Publics

Customers: Functional and External Public

- Customers want to be able to trust a company, especially one like Apple that is ingrained in a customer's daily life. There must be a constant flow of communication with this public and whether it be listening to complaints or notifying each customer about relevant issues.

Suppliers: Functional and External Public

- We need to not only keep our suppliers updated about crises and the happenings of the company but also monitor them for potential crises. Suppliers can be the root of a huge crisis for a company and our suppliers must always be in accordance with our company values and policies.

News Media: Diffused and External Public



- We want to maintain a truthful and open relationship with the media so that in times of crisis we do not have to earn that reputation. The media must be dealt with in a way that it does not look like we are hiding something, or covering something up. Messages to the media need to be concise, factual, poignant and show Apple in a good light.

Competitors: Normative and External Public

- Communication with competitors needs to be very professional and concise, yet informative. During a crisis, we want to know what competitors are doing right and wrong and do it better. If there is a crisis that affects the entire industry our messages must convey to the publics we are ahead of the competition and crisis.

METHODS OF COMMUNICATION/NOTIFYING KEY PUBLICS

Different publics need to be contacted in different ways in times of crisis. All of the publics that Apple deals with have different relationships/motivations with Apple. All publics should be notified as honestly as quickly as possible. The list below shows the different publics and different strategies for notifying them of a crisis event.

Employees:

- Direct knowledge of the event
- Notified by other employees/meeting
- Notification on company software/app
- Manager
- Email
- News Report

Upper-Level Management

- Direct knowledge of the event
- Company security, Communication/PR team
- Personal call from an employee
- Responsible for the event
- Social Media/News Report

Shareholders

- Direct knowledge of the event
- Notified by company security, the management or PR/Comm team
- Whistleblower
- Responsible for the event
- Email
- Social Media/News Report

Customers

- Direct knowledge of the event
- Mass Email to all customers
- Company social media post/press release
- News Media Coverage
- Word of mouth

Minority Publics

- Spanish-speaking communities
- Mandarin-speaking communities



- The blind and disabled
- Important minorities in the affected area during a localized crisis
- Notified in their respective languages through channels relevant to their stakeholder type (customer, employee, supplier, etc.)

Suppliers

- Direct knowledge of the event
- Mass Email to all suppliers
- Company social media post/press release
- News Media Coverage
- Industry-wide issue

News Media

- Public Relations/Communication representative
- Whistleblower
- Other news media
- Police/Fire Scanner
- Bystanders or first-hand witness

Competitors

- Knowledge of the event
- News Media Coverage
- Whistleblower
- Company social media post/press release
- Industry-wide issue

COMMUNICATIONS PROCEDURE FOR HANDLING A MINOR CRISIS

1. The first Crisis Committee member aware of the crisis briefs the other members, the PR Lead and the CEO with a list of key facts and concerns.
2. The PR Lead gathers further information and briefs other communications managers, including Social Media, Internal Communications and any team most relevant to the crisis at hand.
3. The PR Lead determines if a communicator should be dispatched to gain firsthand information and report back.
4. The PR Lead and PR Manager collaborate to prepare and present statements and a plan to the Committee and CEO for approval. The approved plan is put into action and addressed through appropriate media if applicable.
5. The PR Lead responds to any inquiries and drafts replies which are then distributed to customer service and employee relations.
6. The Crisis Committee monitors effectiveness to assure adequate measures were taken.



COMMUNICATIONS PROCEDURE FOR HANDLING A MAJOR CRISIS

The following plan should be executed in the event of a crisis, practiced semi-annually, and introduced to onboarded communications employees for the safety of all stakeholders.

1. The first Crisis Committee member aware of the crisis briefs the other members, the PR Lead and the CEO. The Crisis Committee collectively creates a list of known information, questions and an event timeline.

- The Crisis Committee is to confirm the appropriate PR Lead for a major crisis, who should likely be the Director of Communications and will serve as media contact.
- Committee members are to diligently research and consider stakeholder concerns for the duration of the crisis event and prioritize the major crisis over other organizational duties.

2. The PR Lead gathers further information and briefs other communications managers, including Social Media, Internal Communications and any team relevant to the crisis at hand.

3. The PR Lead determines if a communicator should be dispatched to gain firsthand information and report back.

- The Dispatched Communicator collaborates with local officials, the PR Lead and the Crisis Manager to ensure the safety of self and others if applicable.

4. The Crisis Committee compiles a list of and consults with experts on the crisis at hand.

5. The PR Lead and PR Manager collaborate to prepare and present statements and a plan to the Committee and CEO for approval. The approved plan aligns with expert consideration, and crisis management and should underscore appropriate communication method details. The plan is distributed and put into action.

- See “Crisis Management Plans” in the Crisis Plan Book as the first line of defense.

6. Web pages about the crisis and its management should be created and/or activated; relevant social media should be published as approved by the PR Manager. The general public is directed to assets.
7. The PR Lead and PR Manager draft a press release and plan a press conference. These methods will be used only if the Crisis Committee approves the drafts and deems them necessary.
8. The PR Lead and CEO choose or confirm a Designated Spokesperson who then addresses and collaborates with the media. The Designated Spokesperson may also be the PR Lead depending on the crisis.
9. A report and a survey are distributed to communications managers. Ongoing needs and concerns, related incidents, lessons learned and proposed organizational optimization methods are logged and considered by the Crisis Committee.



EMERGENCY OPERATIONS CENTER (EOC)

The EOC will be run by Crisis Team Manager (Kristin Huguet Quayle) and Assistant Crisis Manager (Adrian Petrica) and they will take over the role of communications managers in the facility. The Crisis Team Manager will be required to monitor communications internally and externally. Assistant Crisis Manager will be designated to record all information and add it to the crisis file, along with creating any statements for release internally and externally. In case of electronic means of communication being out, communicators will use a runner system.

The EOC will have multiple possible locations surrounding Apple Headquarters in Cupertino, CA. Along with this, there will also be multiple locations spread across the United States. Two members of our crisis team will be appointed to manage each location as needed.

Possible EOC locations:

- De Anza College
 - Located in Cupertino, California, this location is an 8-minute drive from Apple Headquarters and would have the capacity to hold both technology and communicators.
- Saratoga High School
 - Located in Cupertino, California, this location is a 12-minute drive away from Apple Headquarters and located further out of the city. The high school would be capable of holding communicators but is limited in space.
- KIPP Austin Public Schools
 - Located in Austin, Texas, a 5-minute drive away from Apple's corporate office.

Emergency Equipment:

Each EOC location will be equipped with maps, stationery supplies, telephones, and whiteboards. Lead communicators will be responsible for storing items on location or nearby:

- Office supplies such as pens, paper, printers, tape
- Laptop computers
- A main telephone for communication internally and externally
- Chairs and desks
- First aid kits, along with various medical supplies

- Transportation
- Multiple TVs and radios
- Crisis communication plan
- List of Apple emergency contacts list and directory.

The procedure for the EOC will remain consistent with the procedure of handling any major crisis. The severity of the crisis will determine which supplies/equipment will be needed. The Emergency Response Team will be responsible for determining which supplies will be needed at the Emergency Operations Center.



CRISIS TEAM AND COMMUNICATION CHAIN

Tim Cook- Chief Executive Officer

- Approve all major decisions
- Signs off on all communication directives

Crisis Team Manager: Kristin Huguet Quayle- Director of Communications

- Communicates with top management and leadership of Apple
- Briefs spokesperson
- Directs staff members
- Prepares or approves initial statements

Assistant Crisis Manager: Adrian Perica- Crisis Team Coordinator

- Organizes crisis team meetings
- Evaluating each department's performance
- Fills in for Michele Morehouse when she is unavailable

Katherine Adams- Senior Vice President and General Counsel

- Provide legal counsel to the chairman of the board, board of directors, chief executive officer and other senior management
- Managing legal affairs of the company

Aaron Stevens - Environmental Scanner

- Monitors internal and external factors
- Coordinates with the social media team for how stakeholders are communicating with the company via social media
- Constantly scans for possible crises

PR Personnel

Public Relations Lead

- Prepare initial statements to be released
- Brief spokesperson
- If necessary, collaborates with Emergency Operations Center
- Provides updates to top management
- Appoints members where they're needed

PR Back-up

- Appointed by PR lead
 - Directs media inquiries

- If necessary, conducts media interviews
- Update Apple's corporate personnel (if applicable)

Communication Chain

In the event of a crisis, team members are contacted as follows:

1. Contact Team manager Kristin Huguet Quayle.
2. Team manager contacts CEO.
3. Team manager contacts assistant crisis manager.
4. Team manager contacts the vice president of legal and global security.
5. Team manager contacts PR personnel.
6. PR personnel contacts remaining board members.
7. PR contacts state and local officials (if necessary).
8. Team manager contacts environmental scanner.
9. Team manager contacts spokesperson.
10. Spokesperson contacts media outlets.
11. Letters sent to employees and all those affected by the crisis.
12. All media inquiries are directed to PR lead and personnel.
13. Spokesperson contacts team manager with incoming updates.



CRISIS DIRECTORY AND CONTACT LIST

Tim Cook- CEO

Phone: (408)-996-1010

Email: tcook@apple.com

Craig Federighi- Senior Vice President of Software Engineering

Phone: (408)-791-4939

Email: C.Federighi@apple.com

John Ternus- Senior Vice President of Hardware Engineering

Phone: (408)- 747-0021

Email: john.ternus@apple.com

Adrian Perica- Crisis Team Coordinator

Phone: (408)-123-4567

Email: adrian.perica@apple.com

Deirdre O'Brien- Senior Vice President of Retail and People

Phone: (415)- 908-3660

Email: D.obrien@apple.com

Katherine Adams- Vice President of Legal and Global Security

Phone: (415)- 728-9908

Email: kadams@apple.com

Kristin Huguet Quayle- Vice President of Worldwide Communications

Phone: (408)- 450-3260

Email: K.quayle@apple.com

Arthur D. Levinson- Chairman of the Board

Phone: (408)- 385-6262

Email: arthur.levinson@apple.com

Aaron Stevens - Environmental Scanner

Phone: (415)-996-1119

Email: astevens@apple.com

Josh Ladner - Social Media Regulator

Phone: (408)-321-7654

E-mail: Josh.Ladner@apple.com

Gina Tabascio - Crisis Team Secretary

Phone: (408)- 765-4321

Email: Gina.Tabascio@apple.com

Emergency Personal and Local Officials

Santa Clara County Fire Department

Phone: (408)-615-4900

Email: info@cnt.sccgov.org

Santa Clara Sheriff's Office

Phone: (408)-808-4400

Email: sheriff@cupertino.org

County of Santa Clara Medical Emergency Services

Phone: (408)-645-7311

Email: emsagency@ems.sccgov.org

Mayor of Cupertino- Hung Wei

Phone: (408)-777-3193

Email: Hwei@cupertino.org

Governor- Gavin Newsom

Phone: (408)- 786-2884

Email: governor@governor.ca.gov

Key Media Contacts

CNN

Phone: (404)-827-1500

Email: teamcnn@cnn.com

FOX News

Contact: Ken LaCorte



Phone: (310)-571-2000
Email: klacorte@foxnews.com

NBC News

Contact: Erika Masonhall
Phone: (212)-664-3230
Email: Erika.masonhall@nbcuni.com

Los Angeles Times

Contact: Davan Maharaj
Phone: (213)-237-5000
Email: Davan.Maharaj@latimes.com

ABC News

Contact: Jeffrey Schneider
Phone: (212)-456-7277
Email: Jeffrey.schneider@abc.com

New York Times

Phone: (212) - 878-3945
Email: publisher@nytimes.com

USA Today

Contact: David Callaway
Phone: (224)-586-7021
Email: dcallaway@usatoday.com

Spokespersons

Eddy Cue- Senior Vice President Services

Phone: (408)-352-0764
Email: Eddy.cue@apple.com

Katherine Adams

Phone: (415)- 728-9908
Email: kadams@apple.com

CRISIS MANAGEMENT PLAN: SPYWARE

PROGRAM OBJECTIVES IN THE EVENT OF A SPYWARE ATTACK

1. Retrieve any stolen data
2. Clean devices affected

STEPS TO BE TAKEN IN THE EVENT OF A SPYWARE ATTACK

1. Any staff member that becomes aware of a possible spyware attack whether through social media or other means is to report it immediately to the Chief Executive Officer, General Counsel, the Vice President of Worldwide Communications and the Senior Vice President of Software Engineering.
2. The Chief Executive Officer, General Counsel, the Vice President of Worldwide Communications and the Senior Vice President of Software Engineering will assemble a team of public relations practitioners and information technology experts to assess the attack and stop it.
3. The Chief Executive Officer and General Counsel will report the incident to the Chairperson of the Board, or to a director in the chairperson's absence.
4. The Chief Executive Officer, General Counsel and the Vice President of Worldwide Communications will contact the public relations department and organize a press conference and news release to alert all affected parties of the spyware attack. They will express urgency without inducing panic.
5. The Vice President of Worldwide Communications, or General Counsel in the Vice President's absence, will be the only authorized spokesperson for personnel and media relations.
6. In the case of massive data loss, the Chief Executive Officer, General Counsel, the Vice President of Worldwide Communications and the Senior Vice President of Software Engineering will work with software engineering and cybersecurity experts to identify where the attack began and retrieve the lost data.
7. The Chief Executive Officer and Chairperson of the Board will contact the corporation's insurance agent within a reasonable period of time and will follow up in writing within 24 hours. The Chief Executive Officer, or Chairperson of the Board in the Chief Executive Officer's absence, will file the necessary forms.



8. Apple will cooperate fully with all government and oversight committees and provide all necessary information for those agencies to reach their conclusion.
9. In the event anyone in the company is contacted by the media, all questions are to be referred to the approved company spokesperson.
10. The Chief Executive Officer and the Vice President of Worldwide Communications will release the dark website allowing consumers to report their affected devices and directing them to the nearest service center to clean their devices.
11. Staff should be given the proper information about the incident and informed of what to say if they are approached by the media.
12. Staff should be prepared to speak to consumers who may have been affected by the spyware attack. All consumers who were confirmed to be affected should be referred to Apple customer services to clean their devices and retrieve their data.
13. The Chief Executive Officer, General Counsel, the Vice President of Worldwide Communications, the Senior Vice President of Software Engineering and all Apple representatives involved will thoroughly document all of their actions related to the incident for case files. The files will include but not be limited to:
 - a. Records of the original spyware attack
 - b. Metadata of the attacker's path into each device
 - c. The model, year, location and software version that each device was on
 - d. Where each affected device was bought
 - e. If the consumer downloaded suspicious files, or apps, or clicked any suspicious links
 - f. Contact with government representatives
 - g. Contact with Apple staff
 - h. Contact with the media
 - i. Contact with the victims and their families
 - j. News releases about the incident, all social media posts and website updates
14. The Chief Executive Officer, General Counsel, the Vice President of Worldwide Communications and the Senior Vice President of Software Engineering will organize a press conference when the spyware threat has been identified and contained announcing this success and detailing future

cybersecurity efforts moving forward. This press conference will remind consumers of the importance of not downloading suspicious apps or files or clicking suspicious links.

15. The Chief Executive Officer, General Counsel, the Vice President of Worldwide Communications and the Senior Vice President of Software Engineering will follow up with all staff and victims and ensure their devices are working properly and all questions have been answered.



CRISIS MANAGEMENT PLAN: FAULTY PRODUCTS

PROGRAM OBJECTIVES IN THE EVENT OF A FAULTY PRODUCT

1. Recall and identify the faulty hardware or software
2. Repair and rerelease products

STEPS TO BE TAKEN IN THE EVENT OF A FAULTY PRODUCT

1. Any staff member that becomes aware of a possible faulty product whether through social media or other means is to report it immediately to the Chief Executive Officer, General Counsel, the Vice President of Worldwide Communications and the Senior Vice President of Software Engineering.
2. The Chief Executive Officer, General Counsel, the Vice President of Worldwide Communications, the Senior Vice President of Software Engineering and the Senior Vice President of Hardware Engineering will assemble a team of public relations practitioners, software engineering and hardware engineering experts to assess the faulty products and identify any issues.
3. The Chief Executive Officer and General Counsel will report the incident to the Chairperson of the Board, or to a director in the chairperson's absence.
4. The Chief Executive Officer, General Counsel and the Vice President of Worldwide Communications will contact the public relations department and organize a press conference and news release to alert all affected parties of the faulty product. They will provide directions to restore the device to working order.
5. The Vice President of Worldwide Communications, or General Counsel in the Vice President's absence, will be the only authorized spokesperson for personnel and media relations.
6. In the event anyone in the company is contacted by the media, all questions are to be referred to the approved company spokesperson.
7. The Chief Executive Officer and the Vice President of Worldwide Communications will release the dark website allowing consumers to report their faulty devices and directing them to the nearest service center to restore their devices.
8. Staff should be given the proper information about the incident and informed of what to say if they are approached by the media.
9. Staff should be prepared to speak to consumers who may have been affected by faulty products. All consumers who were confirmed to own

faulty products should be referred to Apple customer services to restore their devices to proper working order.

10. The Chief Executive Officer, General Counsel, the Vice President of Worldwide Communications, the Senior Vice President of Software Engineering and the Senior Vice President of Hardware Engineering and all Apple representatives involved will thoroughly document all of their actions related to the incident for case files. The files will include but not be limited to:
 - a. Records of the original report of the faulty product
 - b. The make, model, year and software version of each faulty device
 - c. The location where each device was purchased
 - d. Where each faulty device was purchased
 - e. Any user-reported harm to the device (water damage, cracks, drops, etc.)
 - f. Contact with Apple staff
 - g. Contact with the media
 - h. Contact with the device owners
 - i. News releases about the incident, all social media posts and website updates
11. The Chief Executive Officer, General Counsel, the Vice President of Worldwide Communications, the Senior Vice President of Software Engineering and the Senior Vice President of Hardware Engineering will organize a press conference when the product issue has been identified announcing this success and detailing future efforts moving forward. This press conference will reassure consumers that Apple is still the premier technology corporation.
12. The Chief Executive Officer, General Counsel, the Vice President of Worldwide Communications, the Senior Vice President of Software Engineering and the Senior Vice President of Hardware Engineering will ensure that proper updates are released or manufacturing changes are made and release these details to the public.



CRISIS MANAGEMENT PLAN: EMPLOYEE UNREST

PROGRAM OBJECTIVES IN THE EVENT OF AN EMPLOYEE UNREST

1. Minimize damage to corporate reputation
2. Work with employees to reach a sufficient agreement

STEPS TO BE TAKEN IN THE EVENT OF AN EMPLOYEE UNREST

1. Any staff member that becomes aware of possible employee unrest whether through social media or other means is to report it immediately to the Chief Executive Officer, General Counsel, the Vice President of Worldwide Communications and the Senior Vice President of Retail + People.
2. The Chief Executive Officer, General Counsel, the Vice President of Worldwide Communications and the Senior Vice President of Retail + People will assemble a team of public relations practitioners and legal experts to assess the unrest.
3. The Chief Executive Officer and General Counsel will report the incident to the Chairperson of the Board, or to a director in the chairperson's absence.
4. The Chief Executive Officer, General Counsel and the Vice President of Worldwide Communications will contact the public relations department and organize a press conference and statement to release to the news media about the unrest.
5. The Vice President of Worldwide Communications, or General Counsel in the Vice President's absence, will be the only authorized spokesperson for personnel and media relations.
6. In the event anyone in the company is contacted by the media, all questions are to be referred to the approved company spokesperson.
7. The Chief Executive Officer and the Vice President of Worldwide Communications will release the dark website with the prepared statement addressing employee unrest.
8. Staff should be given the proper information about the incident and informed of what to say if they are approached by the media.
9. The Chief Executive Officer, General Counsel, the Vice President of Worldwide Communications and the Senior Vice President of Retail + People should meet with unresting thought leaders to assess the situation and determine the next steps.
10. The Chief Executive Officer, General Counsel, the Vice President of Worldwide Communications and the Senior Vice President of Retail + People

and all Apple representatives involved will thoroughly document all of their actions related to the incident for case files. The files will include but not be limited to:

- a. Records of the original report of the unrest
 - b. Any statements made by the employees taking part in the unrest
 - c. The location where the unrest began
 - d. Social media sentiment and news reports
 - e. Contact with Apple staff
 - f. Contact with the media
 - g. Contact with the thought leaders
 - h. News releases about the incident, all social media posts and website updates
11. The Chief Executive Officer, General Counsel, the Vice President of Worldwide Communications and the Senior Vice President of Retail + People will organize a press conference when the unrest has been resolved to announce changes moving forward.
12. The Chief Executive Officer, General Counsel, the Vice President of Worldwide Communications and the Senior Vice President of Retail + People will ensure that staffing changes and employee support programs are announced to the public as soon as they are implemented.



IDENTIFICATION OF A SPOKESPERSON

When selecting a spokesperson(s) for the company, Apple will be careful in their selection and considerate of the crisis. The spokesperson selected must have a position within the company to appear powerful and credible in front of the media and public. They must also be calm, speak with care and be considerate of those directly affected by the crisis. The spokesperson will need to talk with clarity, be able to remain calm on and off camera, as well as be accessible throughout all points of the crisis.

With these guidelines in mind, the primary spokesperson will be the CEO of Apple, Tim Cook, in case of death or a widespread crisis. If the crisis surrounds health, Apple's Director of Health, Divya Nag, will be selected as Spokesperson. In cases regarding security, Apple's Head of Global Security, Tom Moyer will be our selected spokesperson.

Kristin Huguet Quayle, Apple's Vice President of Worldwide Communications as well as Lisa Jackson, Apple's Vice President of Environment, Policy, and Social Initiatives will be selected as backup spokespeople for CEO, Tim Cook.

Apple will use spokespeople outside of the company in certain crisis situations. These spokespeople are:

Sheriff of Santa Clara County Police Dept. (408) 686-3650
California Food and Drug Branch. (800) 495-3232

GUIDELINES FOR SPOKESPEOPLE

All spokespeople should be prepared and aware of the questions journalists may ask. The spokesperson should first review who, what, where, when, why and how questions with the crisis communications team as well as review and know the two to three key message points.

Spokespeople must be prepared for all questions such as:

1. Speculation
 - a. Questions that begin with “if”
 - b. For example, “If this crisis occurred at a different time, how many may have died?”
2. Leading Questions
 - a. Reporters searching for verification on speculation.
3. Loaded Questions
 - a. Questions typically lead with “Isn’t it true”
 - b. Looking to get an emotional response back
4. Naive Questions
 - a. Asking questions that everyone knows.
5. False Questions
 - a. Looking for you to verify the false details.
 - b. Be aware of these and listen to reporters’ questions carefully.
6. Know-it-all questions:
 - a. Pretending to know all the details and asking you to verify their research.
7. Silence
 - a. Looking for you to reveal more information. Do not be afraid to let the silence linger.
8. Accusatory Questions
 - a. Looking for you to place blame on someone.
 - b. “Who is responsible for this crisis?”
9. Multiple-Part Questions
 - a. Trying to confuse you. Answer one question at a time.
10. Jargon Questions
 - a. Questions using specific technical terms to confuse the public.
 - b. Respond with common, everyday language.
11. Chummy Questions



- a. Asking “off-the-record questions”
- 12. Labeling Questions
 - a. Trying to paint Apple in a bad light.
- 13. Good-bye questions
 - a. Questions asked after the interview has ended but still looking to record answers.

Tips for spokesperson when addressing media:

1. There are no “off the record” statements. Answer everything as if it will be revealed to the public in the media.
2. Do not elaborate on hypotheticals. Stick to the facts.
3. Do not use “no comment.” This statement suggests we are trying to hide facts.
4. Speak in common, simple terms.
5. If you do not understand a question, ask for clarification.
6. Focus on the two or three key message points and repeat them to communicate them effectively during the interview.

Tips for how to act while addressing media:

1. Be slow to speak, pause and think about words before answering.
2. Remain calm. Do not let emotions rise.
3. Don’t just act empathetic, really do care about the lives affected by the crisis.
4. Answer the questions by facing the reporter and making eye contact with them as well as the camera crew.

Every spokesperson should avoid:

1. Questions looking to accuse the company of the crisis
 - a. Example: “Were there any warning signs that the crisis might have occurred?”
2. Speculative questions trying to frame Apple in a bad light.
 - a. Example: “With a high-functioning company like Apple, the work atmosphere must be high-paced and stressful, right?”
3. Framing Questions
 - a. Example: “Do you believe the crisis could have been avoided if...”



FORMAT FOR BRIEFING SOMEONE IDENTIFIED AS A SPOKESPERSON FOR INTERVIEWS/NEWS BRIEFING

Executives who are scheduled to talk to the media should be briefed and given more information well before the interview. This policy stands for all executives and all types of interviews, even a short phone call.

The briefing must include these 11 items at a minimum:

- Date, time and location of the interview
- Name of reporter
- Name of the publication, station, outlet, etc.
- Our relationship with the reporter or publication, to help the interviewee understand what type of caution needs to be taken when answering and the risk of words being twisted or set up with trick questions
- Subjects/issues/questions requested to cover by the reporter
- Our position/stance on particular topics and subjects
- Top three to five messages we want to be conveyed through this interview, regardless of what the interviewer asks
- List of other executives that should be interviewed during this visit, including key topics and messages other executives should cover
- Issues/topics that the executive should avoid, and how to properly sidestep a question regarding a sensitive topic
- Background information/statistics/data that would be useful in preparing arguments for the interview
- Length of interview

Background material and briefing for an interview should, if possible, always be conveyed in writing, physical or digital, so it can be read carefully. Only under certain circumstances should an oral briefing be given as the primary briefing for the interviewee.

In critical situations, preparing a thorough set of questions and answers to be rehearsed before the interview can be tremendously helpful.

EXAMPLE OF INITIAL STATEMENT FOR RELEASE

During an emergency situation, it may be determined that a news release should be distributed to the media. The purpose of the news release is to convey written information on the incident and to avoid misinterpretation.

Circumstances That May Require A News Release

- A data breach or spyware infection that results in major data loss or property damage
- A faulty or broken product that results in loss of customer satisfaction or personal injury
- Employee unrest or strike resulting in negative media coverage or misinformation
- Natural disasters resulting in personal injury or property damage
- An accident, fire, or explosion that results in serious injury, death, or considerable property damage
- A health or environmental incident, or discovery of a health or environmental hazard that may affect employees, the surrounding community, or the environment
- Sabotage, abduction or extortion, bomb threats, or acts of terrorism involving company personnel, products, or property
- News of an incident that is likely to be known by employees or circulated in the community and creates misleading impressions
- News of an event that is unusual enough to cause concern to employees, nearby residents, or community officials
- Consistently misleading news reports

Information Appropriate for Release

During an emergency situation, there will be information that is appropriate to release to employees and to the media. Communications personnel should do the following:

- Tell what happened: Give a description of the emergency situation. Include details of affected publics and current threat level.
- Tell who is involved: Report how many employees were evacuated and if any have been taken to the hospital for observation or due to injury. Report



when emergency team members and/or the various city or county fire departments and police arrived on the scene (if applicable).

- Indicate where it occurred: Give the street address of the scene of the emergency. If the emergency is not physical, give a description of the devices or iOS systems involved.
- Identify when it happened: Give the time and date the incident began.

Information That Is Not Appropriate for Release

There will inherently be information that is not appropriate for release until more is known about the nature of the crisis response and the extent of the impact.

- Do not speculate on why the emergency occurred or what type of hazardous materials are involved. Likewise, don't make any statement that blames any individual for the accident. (Although the cause of the incident may appear obvious, it cannot be accurately determined without an extensive investigation, nor can the blame be placed on an individual without a thorough investigation.)
- Do not include "off the record" information because there is no such information.
- Do not overreact to or exaggerate the situation. For instance, during a spyware attack, a reporter may ask for the "worst-case scenario" of what could happen with the spyware involved in the accident. It is impossible to determine this until you have specific data regarding the spyware involved. Bridge back to facts and messages.
- Do not minimize the situation. Never regard an emergency as a minor incident.
- Do not release the names of injured or affected individuals, unless Human Resources authorized it following confirmation that the victim(s)' family(ies) have been notified.
- Do not release dollar estimates concerning the extent of property damage. Normally, there is no way to accurately determine this until extensive studies have been conducted.
- Avoid the "no comment" response because it often leads the reporter to speculate. If you don't know the answer to a reporter's question or if you can't discuss something, explain why in simple terms.

Writing a News Release

By following a few basic principles when writing news releases, our company stands a better chance of having reporters use the information with only minor changes. Remember to consult the legal department as needed.

1. Tell the most important information in your lead paragraph. Your “story” competes with other news and information, so the most important point should be stated clearly in the first paragraph.
2. Answer four of the five “Ws”—Who, What, Where and When — and an “H” for How. Explain what the event is. Identify who is involved in the event as well as the material and equipment involved. Tell where and when the event occurred, if it occurred online, describe the affected devices and servers. Explain what action we are taking to mitigate or respond to the emergency. Do not explain why the event occurred unless complete information is available.
3. Attribute information to a qualified source. A news release is useful only if it conveys credible information.
4. Write the remaining information in descending order of importance. If the media cuts off the bottom of your story, they will cut information that is least important to the public.
5. Explain technical points in simple language. A direct quote can add the human element to otherwise technical information and help explain a situation or event in layman’s terms. Tell the real story. Avoid using language that is overly specific or technical.
6. Be concise. A good news release is judged by the quality of information it communicates, not by its length. Stop writing when you’ve said all you need to say.



SAMPLE NEWS RELEASE

FOR IMMEDIATE RELEASE

Jan 1., 20XX (Date of Release)

Firstname Lastname

Title

email@email.com

(123)456-7890

Title

City, ST. — At ___ (time of notification), Apple received news that a data breach had been identified and personal user information had been compromised. At this time the access has been blocked and data is being recovered. The breach has been reported to local authorities.

Our primary concern is the safety and trust of our users. We will continue to investigate the cause of this breach and take precautions to secure all data and personal information. We continually monitor our servers for security breaches and are prepared at all times to locate, retrieve data and update software in the case of a data breach.

Apple conducts periodic audits of its data security protocols to ensure they comply with company security standards during normal and emergency conditions. Apple will continue to work closely with state and federal agencies to meet or exceed security regulations and report results.

We have contacted all affected users and have opened an internal investigation to identify how the breach occurred. Users should take precautions to secure their accounts by updating their Apple ID passwords and enabling two-factor authentication.

About Apple

Apple revolutionized personal technology with the introduction of the Macintosh in

- More -

1984. Today, Apple leads the world in innovation with iPhone, iPad, Mac, Apple Watch, and Apple TV. Apple's five software platforms — iOS, iPadOS, macOS, watchOS, and tvOS — provide seamless experiences across all Apple devices and empower people with breakthrough services including the App Store, Apple Music, Apple Pay, and iCloud. Apple's more than 100,000 employees are dedicated to making the best products on earth, and to leaving the world better than we found it.

###



BACKGROUND STATEMENT

Some background information that would be important for reporters/media to know would be that Apple has been serving the community since April 1976. By informing the media of this, it could provide a sense of trust during a time of crisis.

Knowing that Apple has spent years dedicating itself to its customers may provide some relief to those affected by a crisis. It is also important to include any information about charities, company values, grant programs, volunteer time, etc. This will put emphasis on the admirable features of Apple that could assist in rebuilding trust with the key publics.

The following is a list of facts about Apple:

- For over 10 years, Apple's Employee Giving program has raised around \$725 million for 39,000 organizations globally (2023).
- There are 518 Apple stores across 25 countries, and 251 of them are located in the United States (Wise, 2023).
- With a market cap of over \$2 trillion, Apple has become one of the largest companies to be recognized globally (Wright, 2022).
- Through the Strengthen Local Communities grant program, Apple supports local food banks and other organizations to provide food, shelter and other services to those in need (2023).
- Apple's value statement is "To make the best products on earth and to leave the world better than we found it."

Boilerplate

Apple's boilerplate introduction goes as follows:

Since 1976, Apple has been dedicated to serving communities across the globe.

Being one of the largest companies to be recognized globally, Apple is devoted to leaving the world a better place than we found it through charity and grant programs that benefit communities all over.

FACT SHEET

Based on the previously determined crises (employee unrest, faulty products, spyware vulnerability, supply chain issues), the following is a list of facts the media and public may need to know:

Employee Unrest

Summary/Explanation: Provide as much non-personal information as possible to the public, defining what took place.

Expectations: Explain in detail what employees should expect moving forward. Ensure that all employees are up-to-date on any developments and updates about the situation. Provide a safe and secure place for employees to report any problems or concerns as part of a prevention plan. It's important to remember that all Apple employees are key internal stakeholders that act as spokespersons.

Who/Where It Happened: If appropriate, inform the public of where it took place.

Methods of Communication: Identify all publics involved, and then determine the most effective form of communication. This includes, but isn't limited to, all levels of management, stakeholders, spokesperson(s), employees, customers, media and suppliers.

Faulty Products

Summary/Explanation: Provide details on what happened and any current updates on what, where, why and how it happened.

Expectations: There will likely be an influx of customer complaints. In this case, direct them to customer support and have them offer a return, refund, or exchange that satisfies the customer.

Methods of Communication: Identify all public involved, and then determine the most effective form of communication. This includes, but isn't limited to, all levels of management, stakeholders, spokesperson(s), employees, customers, media and suppliers.



Spyware Vulnerability

Summary/Explanation: Provide as much detail as possible about the situation and what is being done to resolve it. Be sure to include any appropriate information about who, what, when, where, why and how it happened if and when that information is available.

Expectations: In the event that the public has safety concerns, provide them with appropriate information on how to protect themselves.

Methods of Communication: Identify all public involved, and then determine the most effective form of communication. This includes, but isn't limited to, all levels of management, stakeholders, spokesperson(s), employees, customers, media and suppliers.

Where it Happened: If known, provide information about where the source of the problem is coming from and what actions are being taken to resolve/prevent it.

Supply Chain Issues

Summary/Explanation: Provide a detailed summary of the situation. Be sure to include any appropriate information about who, what, when, where, why and how it happened if and when that information is available.

Expectations: It's likely that there will be a lot of questions and concerns from the public. Provide frequent updates and a timeline for when they are expected to return back to normal.

Methods of communication: Identify all public involved, and then determine the most effective form of communication. This includes, but isn't limited to, all levels of management, stakeholders, spokesperson(s), employees, customers, media and suppliers.

SAMPLE LETTER TO STOCKHOLDERS
DATA BREACH/SPYWARE ATTACK (customers)

Dear Valued Apple Customer,

As your privacy is of great importance to us, we would like to address a recent data breach that has impacted Apple customers. Our teams identified the issue and were able to shut it down within 24 hours. Though most sensitive information had been protected by our constantly updating systems, please update your device and reach out to Apple Support at support.apple.com if you feel you may have been a victim of a data breach on an Apple device.

Your trust in Apple is valued deeply, and we know that we must earn that trust every day. We are committed to being transparent and open with you about this incident and any actions we take in response to it. We apologize for any inconvenience brought to the valued Apple community.

Going forward, we are increasing the level of encryption on our servers and implementing additional security measures to prevent unauthorized access. We will also be providing our users with more information about the steps they can take to protect their own personal information.

We are working to gather further information and will keep you updated as we learn more. Apple is committed to creating products and services that enrich people's lives while protecting their privacy and security. This breach is a setback, but it will not deter us from our mission. Thank you for your continued support and trust. We will work tirelessly to regain that trust and to ensure a safe Apple experience in the ever-evolving technological world.

Sincerely,

Apple, INC.



DATA BREACH/SPYWARE ATTACK (employees)

Dear Apple Employees,

I am writing to you today to address the recent data breach that has impacted our company. We are still investigating the matter, but we believe that a group of cybercriminals was able to gain access to our systems through a phishing attack. We are working closely with law enforcement and cybersecurity experts to identify those responsible and bring them to justice.

I am addressing you, our employees, because you are the heart and soul of our company. Your importance cannot be overstated, and I want you to know that we are doing everything in our power to protect you and our customers.

To prevent future breaches, we are conducting a review of our systems and procedures to identify any vulnerabilities and address them promptly. We are also implementing multi-factor authentication and employee training programs to ensure that our systems remain secure.

There are still unknowns regarding the breach, but we will keep you informed as we learn more. We encourage everyone, employees and customers, to use strong passwords, keep personal information private and report suspicious activity.

Finally, I want to remind you of our mission statement, which is to empower people through technology. Despite this setback, I remain confident in our ability to continue delivering on this mission. Thank you for all that you do to further this mission, and please know that we are here to support you in any way that we can.

Sincerely,

Tim Cook
CEO, Apple

FAULTY PRODUCT DISCOVERY (customers)

Dear Valued Apple Customer,

We are writing to you today regarding a recent technical issue that has affected some of our (LIST SPECIFIC PRODUCT HERE). We understand that this has caused inconvenience and frustration for you, and we apologize for any harm this may have caused. We take our commitment to safe, quality products seriously and are taking immediate steps to address the issue and ensure that it does not happen again.

To address this product issue, we have partnered with (SPECIFIC RESEARCH GROUP) to develop a solution. If you are experiencing a faulty (LIST SPECIFIC PRODUCT HERE), please schedule an appointment with an Apple Care technician. If your experience in resolving this issue is not satisfactory, Apple will offer a full refund for up to one year of the item's purchase. Any unknowns about the product's safety will be shared as Apple acquires more knowledge on this issue.

We want to assure you that our mission remains the same: to provide you with the best possible products and customer service. We appreciate your patience and understanding as we work to resolve this issue. If you have any questions or concerns, please do not hesitate to reach out to our customer support team, who are available 24/7 to assist you. Thank you for your continued support of Apple through a transformative technological journey from its inception.

Sincerely,

Apple Customer Support



EMPLOYEE UNREST/STRIKE (employees)

Dear Apple Employees,

I am writing to you today to address recent employee concerns within our company. I want to assure you that we value your input and are committed to creating a workplace where all of our employees feel safe, respected and valued.

We have taken steps to address some of the issues that have been brought to our attention. We are also working with outside experts to ensure that our policies and procedures are in line with best practices and that we are doing everything we can to create a safe and respectful workplace.

Your hard work, dedication and innovative spirit are what has made Apple the industry leader that it is today. At this time, there are still some unknowns, which will be addressed through internal investigations and employee surveys about Apple's workplace climate. We are committed to being as transparent as possible with you and to keeping you informed every step of the way.

In the meantime, we want to remind everyone to take all necessary safety precautions while at work. If you ever feel unsafe or uncomfortable, please speak up and let someone know. We have a zero-tolerance policy for any form of harassment or discrimination, and we will take swift action to address any issues that arise.

Finally, I want to remind everyone of our mission statement: to design and build the world's best products and services while making a positive impact on people's lives. We are committed to working together to create a workplace where everyone feels valued and supported to achieve this mission. Thank you for your hard work and dedication, and we will get through this together.

Sincerely,

Tim Cook
CEO, Apple

WEBSITE

Providing continuously updated information through official channels during a crisis is imperative to a healthy relationship between Apple and its customers. Creating dark web pages for each crisis type will allow for swift, organized dissemination of information through apple.com and its respective applications. The web pages should be informative, positive, offer a “Contact Us” option, an FAQ section and inform the public that the website is regularly updated as Apple acquires new information.

The team designated to manage the web pages should prioritize consistency with statements from Apple executives and the communications team. Any information distributed publicly through any channel is to be accessible or conveyed through apple.com. The web pages are to be clearly labeled and easily accessible. Other web pages would not be needed.

Additionally, at least one source of phone and email information should be included so affected parties can be thoroughly assisted by real people in a crisis call center connected to Apple customer support. Overall, the dark web pages will address the crisis, what to do during the crisis as an Apple employee or customer, what Apple is doing about the crisis, contact information, an FAQ section and other approved context.



SOCIAL MEDIA

The Director of Communications is to inform social media departments of the crisis through email and phone call, and provide updates throughout the crisis. Apple will communicate through Twitter, Facebook and Instagram during the crisis as each platform offers a different way for publics to access and share information from Apple about Apple. Using multiple social media channels will communicate key messages to a broader range of publics.

The Social Media Manager is to **cancel** regularly scheduled or evergreen content on all platforms until the crisis is adequately mitigated. The Social Media Team is to **monitor** hashtags and posts relevant to Apple and the crisis throughout the crisis lifetime. The Social Media Team will **draft** posts relevant to the crisis and **present** them to their manager, who will assess the posts under these criterion and present them to a Crisis Management Team Member:

- Is the post necessary?
- Is the post appropriate?
- Is the post congruent with key messages communicated by the Crisis Management Team?
- Is the post helpful to Apple customers?
- Does the post offer long term benefit to Apple and its stakeholders?

Posts should align with Apple's visual brand and be accompanied by photos unless deemed unnecessary. Captions should be brief and direct traffic to the web page. **No posts are to be made without approval from the Crisis Management Team. Any approved items are to be posted by the Social Media Manager only.**

The Social Media Manager is to draft direct message replies with help from their team. The replies should be easily accessible to all social media team members. Any direct messages about the crisis will be addressed with empathy and direct publics to the Apple web page specifically activated for the crisis.

Posts during a crisis are **not to include** jokes, promotions or sarcasm. News regarding individual lives should not be distributed until it is confirmed that families have been made aware of any injuries or lives lost. Regularly scheduled content will resume over an appropriate period of time, which will be deliberated by the Director of Communications, the Crisis Management Team, and Social Media Managers.

MESSAGES FOR THE NEWS MEDIA DURING EMPLOYEE UNREST CRISES

Mentioning the following messages will help Apple communicate its position and provide clear information on employee unrest:

- At Apple, our main concern is providing a safe and comfortable work environment for our employees.
- We offer all of our employees access to our Employee Assistance Program. The program provides confidential support to anyone that is experiencing personal challenges that can impact their work life. This includes counseling, financial guidance, basic legal advice and much more.
- We frequently conduct assessments of our policies and training and make changes based on emerging trends and conflicts.
- We are currently establishing a process for employees to submit their complaints or concerns about the workplace. This will allow us to conduct an investigation to reach a suitable solution with the information gathered.
- All levels of management and employees will be required to participate in additional diversity and inclusion training.
- Apple will continue to pursue improving our company to ensure that all employees' needs are met and that they have a safe and pleasant work experience.



MESSAGES FOR THE NEWS MEDIA DURING A SPYWARE ATTACK CRISIS

Mention of the following points during interviews and public statements may help the company communicate its process throughout the news of breach/spyware attack crises:

- Our Apple Technology Team is working diligently to identify the source of the breach and resume safe and protected operations quickly.
- Apple's primary concern is to resolve the source of the data breach as quickly as possible.
- We understand the concern for the recent data breaches and sincerely apologize to those who have been affected. Our primary concern is to make Apple devices safe and protected for our customers.
- Our security department is working to ensure that any further data breaches are prevented to keep our customer's information safe.
- Apple has been working with federal law to locate and charge those responsible for data breaches.
- Apple will be implementing new safety and privacy policies to ensure that your data will not be leaked or shared.
- Apple is committed to creating and maintaining a trusted environment for data to be kept private so that your information can remain private.
- For regular updates and more information about Apple's Privacy Policy and protection from data breaches, please visit our website:

<https://www.apple.com/legal/>

MESSAGES FOR THE NEWS MEDIA DURING FAULTY PRODUCT CRISES

The mention of the following points during interviews and public statements may help the company communicate its process throughout the discovery of a faulty product:

- Our primary concern is the trust and satisfaction of our customers. We have identified and recalled the faulty products and are working to improve and re-release these products. In the case of faulty software, a recall will not be issued, but rather a software update to address the issue.
- We continually test our software and products to ensure they meet the highest quality standards.
- We work continuously to provide the highest quality technology products and software to connect you to the world.
- Our employees who work directly on production are highly trained to identify and report any issues with software and products throughout the production and testing processes.
- The company conducts extensive testing of its products and software before releasing it to the public.
- The company will work closely with our product and software development teams to identify the cause of the issue, improve it and prevent any similar issues from reoccurring.
- The company has contacted all affected accounts and recalled all faulty devices. If users believe their device is faulty, they should report their account or device on Apple's website.
- Faulty products can be reported in-store or online, and faulty devices can be mailed in to be fixed, updated, or replaced if necessary.

It is important to note the processes in place to prevent faulty product issues:

- We have continuous, intensive testing for our software and products before they are released to consumers to ensure they meet the highest quality standards.
- We strive to provide the highest quality technology products and software to connect you to the rest of the world.
- The company conducts comprehensive testing of all its products before being released to consumers.



POSSIBLE QUESTIONS AND SUGGESTED RESPONSES

As the public rightfully have questions in a time of crisis, it is important to address their concerns with empathy and accuracy. Here are examples of how to respond to difficult questions and guidelines for providing thoughtful answers during a crisis.

Data Breach/Spyware Attack

Q: Our sources said the breach/attack was an Apple employee's fault. Can you confirm?

A: We have a team of cybersecurity experts investigating the cause. Once we gather enough evidence, we will let you know exactly what happened. If you have information that might be helpful to this investigation, please come forward after the press conference.

Q: How much revenue is Apple expecting to lose because of this?

A: Apple is a customer-focused company, and right now we're focusing on customer safety and restoring their trust in Apple.

Q: Does this data breach/spyware attack leave Apple users in danger?

A: Current findings suggest no information obtained would endanger Apple users. Apple is prioritizing transparency and will notify the public without hesitation if there is any danger.

Q: Are there any lawsuits currently open regarding the data breach?

A: I'm sorry, It is Apple's policy not to discuss litigation with the general public.

Q: Did this incident happen because Apple operates on the cloud?

A: Elements of this incident are not cloud-specific and happen in both cloud-based and onsite data environments.

Faulty Product Discovery

Q: Why didn't Apple test for this problem before?

A: Apple rigorously tests its software and hardware and excels beyond mandatory testing standards. Unexpected issues like this help us further develop our testing methods.

Q: How much in damages is Apple expecting to pay to people who purchased (name of faulty Apple product)?

A: We're committed to customer well-being and will address mitigation directly with those affected.

Q: Why did you release a dangerous product?

A: All product releases are intended to help, not harm, customers. We are keeping in contact with those who have been affected and are assisting in every way we can through their recovery.

Q: Why did this not happen to (competitor)'s product?

A: Each brand has its own unique patented information and testing systems, so I can't quite speak on other brands.

Q: Is Apple lowering its standards for good technology?

A: Apple exists to make customers' lives easier. That means giving them the best products and software we can.

Employee Unrest/Strike

Q: Why are most Apple employees unhappy?

A: We're trying to get to the bottom of the issue at hand and aren't sure how many employees feel Apple needs to make changes. We're listening and learning, and value our employees' input.

Q: Are the (sexual/embezzlement/other) allegations true?

A: Apple is still conducting an internal investigation as well as partnering with outside experts to assess the validity of the claims and reach a resolution.

Q: What does the CEO think of the situation?

A: Apple's CEO said (approved quote from CEO) and will address questions during the next press conference.

Q: Why do high-ranking employees make so much more money than other essential employees at Apple?

A: Apple's salaries are competitive and based on regional data and the current job market. We're meeting with employees who feel they're underpaid to better



understand their tasks. We want everyone at Apple to have a positive employee experience.

Q: Should Apple have fired (employee or executive) sooner?

A: Apple management did their best to follow procedure and could not terminate this employee until it was proven right to do so. These things take time, and we placed the employee in question on leave when we suspected something was wrong.

What to Say Instead of “No Comment”

Apple does not approve of the use of “no comment,” as it has apathetic and secretive implications. If questions cannot be answered by Apple’s key messages and updated information, here are a few alternatives.

- The formula: we don’t know yet but will soon
- “We’re still gathering information and will have a statement once we have more details.”
- “We are looking into the situation and will have a reply once our investigation is concluded.”
- “I’ll check on that and will get back to you.”
- “I checked with management and at this time there is no new information to release.”
- “I’m sorry, Apple does not discuss (ongoing investigations, litigation, proprietary information) with the general public for stakeholder safety.”

What to Say When You Don’t Have the Answers

- Explain that we do not have enough information at this time
- Explain how we might go about getting this information if applicable
- Explain that we will get back to them as soon as we know more

PRE-GATHERED INFORMATION

Employee Unrest General Information

- Reasons for employee unrest can include dishonest payroll, uncompensated overtime, managerial corruption or inappropriate behavior, discrimination, unfair labor practices and multiple other reasons
- Strikes may be lawful or unlawful
- The Right to Strike is protected by the National Labor Relations Act (National Labor Relations Board, 2020)

Data Breach/Spyware Attack General Information

- Data is a valuable asset in the modern world
- Data breach is unauthorized acquisition of or access to data for an unauthorized reason or to an unauthorized individual or company, whether physical or electronic
- Data breaches do not exist solely because of the digital world and are part of record keeping
- Apple may be legally responsible to notify customers of this crisis type (Office for Civil Rights, 2009)

Faulty Product General Information

- Failure to provide warning labels can cause a liability issue
- Injured customers are eligible for damages in regards to lost income, medical expenses and pain and suffering
- Faulty product crises can create further complications for customers as false warranties are often used as scam/phishing tactics
- Sale of damaged product may result in federal penalty (FTC, 2022)

REFERENCES

National Labor Relations Board. (2020). The Right to Strike | NLRB | Public Website. Nlrb.gov. <https://www.nlrb.gov/strikes>

Office for Civil Rights. (2009, September 14). Breach Notification Rule. HHS.gov. <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>

Penalty Offenses Concerning Damaged or Defective Merchandise. (2022, April 21). Federal Trade Commission. <https://www.ftc.gov/enforcement/penalty-offenses/damagedmerchandise>



URLS FOR RESOURCES

Apple Store Website

<https://www.apple.com/store>

- Purchase Apple products
- Product specs and prices
- Support information
- Deals on Apple products

Apple Website

<https://www.apple.com/>

- More information about products
- Information about veterans discounts, Apple classes and upcoming updates

Apple Support/Repair Website

<https://support.apple.com/repair>

- Online support available via call, email, text whichever is preferred by user
- Resources to find the closest Apple store
- Information regarding repairs, warranties, trade in's and upgrades
- Educational tabs informing users of counterfeit parts and gift card scams

Apple Security Website

<https://security.apple.com/>

- Blog posts about current updates from the Apple Security Department
- Applications for users to own a Research Device and be a part of Apple's Research Program
- Apple's Security Bounty where users can get paid for finding a security or privacy vulnerability that affects Apple Devices

EVALUATION OF PLAN EFFECTIVENESS AFTER A CRISIS

After a crisis happens, Apple will take a thorough look internally to find anything that can be done in the future to prevent a crisis of any type. Employees are always properly notified and consistently informed throughout a crisis, which is something Apple will continue to do, but there is always room for improvement. Apple is constantly monitoring and listening to industry news and happenings to make sure that Apple is ahead of the curve and on top of possible risks before they turn into a crisis. Apple is very thankful for its thousands of employees who ensure the company stays strong, however, any employee that is negligent or purposefully responsible for a crisis will be terminated and can be subject to legal repercussions. Here, we assess the success of social media, media relations, department readiness and community relations.

EVALUATION FORM

This form is intended only for the departments that are involved with the crisis, appropriate managers, the crisis team and the Communications Department. 1 is strongly disagree, 2 is disagree, 3 neutral, 4 agree, and 5 strongly agree.

Name (optional)

Position/Department

1. Overall, the crisis was handled in a timely manner
1- SD 2-D 2-NA 4-A 5-SA
2. The Crisis Management Team remained calm throughout the crisis
1- SD 2-D 2-NA 4-A 5-SA
3. Apple continued to inform the customers and Public throughout the crisis
1- SD 2-D 2-NA 4-A 5-SA
4. My department was prepared for this type of crisis
1- SD 2-D 2-NA 4-A 5-SA



5. The use of social media was effective in this instance

1- SD 2-D 2-NA 4-A 5-SA

6. The Crisis Management Team addressed the media respectfully

1- SD 2-D 2-NA 4-A 5-SA

7. Minority publics were properly addressed by Apple

1- SD 2-D 2-NA 4-A 5-SA

8. The safety of the customers was ensured

1- SD 2-D 2-NA 4-A 5-SA

9. The customers interests were valued by Apple

1- SD 2-D 2-NA 4-A 5-SA

10. The crisis communications plan was effective in this particular crisis

1- SD 2-D 2-NA 4-A 5-SA

11. If you disagree please elaborate on the areas that were not effective

12. If you disagree, please elaborate on the areas that were not effective
