

# Exercise Chain Reaction

Norwegian Cyber Range



A hand in a dark suit is moving a black chess piece (a king) on a chessboard. The chessboard is black and white, and several other pieces are visible. The background is dark and out of focus.

# Timeline

---

- 10:00 (Briefing)
- 10:30 (Intro to Crisis Chess Board)
- 11:00 (Intro to Cyber Threat Analyzer)
- 11:30 (Lunch)
- 12:00 (Exercise Starts)
- 14:00 (Debriefing)



# Scenario



# Innovative Solutions INC.

The organization is a mid-sized manufacturing company based in the United States that specializes in producing high-tech equipment for the automotive industry. The company has been in operation for over 20 years and has a strong reputation in the industry for delivering innovative solutions.



# Financial Outlook

The company has experienced steady growth over the past few years and has been profitable. However, the manufacturing industry is highly competitive, and the company is facing pressure to reduce costs and increase efficiency to remain competitive. The company has recently invested in digital transformation initiatives to improve operations and streamline supply chain management.



# Public Relations

The company has a strong commitment to sustainability and has received recognition for its efforts to reduce its carbon footprint. The company also values diversity and inclusion and has implemented policies to promote these values in the workplace. Overall, the company has a positive reputation among its customers and stakeholders.



# Threats Faced

The company is facing an increasing threat from cyberattacks, particularly ransomware attacks. As a manufacturer, the company has a complex supply chain that includes multiple third-party vendors, which can make it vulnerable to attacks that originate outside the company. The company has invested in cybersecurity measures to prevent such attacks, but the evolving nature of cyber threats means that the company must constantly adapt its security measures to stay ahead of attackers. A cyberattack could have a significant impact on the company's operations and reputation, as well as its financial stability.



People in the organization





# People (Operational Level)

- Olivia Chen : Olivia is a Security Analyst in the company's Security Operations Center (SOC) and is responsible for monitoring the company's systems and identifying security incidents.
- David Kim : David is a System Administrator and is responsible for managing the company's Active Directory (AD) system.



# People (Tactical Level)

- Sarah Patel : Sarah is the company's Chief Financial Officer (CFO) and is responsible for assessing the financial impact of the attack and determining the budget required to recover from the incident.
- John Collins : John is the company's Chief Information Officer (CIO) and is responsible for overseeing the company's IT systems and infrastructure.



# People (Strategic Level)

- Rachel Lee : Rachel is the company's Chief Security Officer (CSO) and is responsible for developing a roadmap for improving the company's security posture.
- Mark Johnson : Mark is the company's Chief Executive Officer (CEO) and is responsible for making high-level decisions that impact the company's overall strategy and direction.
- Emily Rodriguez : Emily is the company's Chief Legal Officer (CLO) and is responsible for coordinating with law enforcement agencies to investigate the attack and determine the identity of the attackers.



# Processes in the organization

Crisis Chess Board



# Platform of the Organization



# Purpose



FOR PARTICIPANTS: INFORMATION  
ANALYSIS, TEAMWORK, DECISION  
MAKING



FOR ORGANIZERS: VALIDATION OF  
DIFFERENT RESEARCH ARTIFACTS





# Exercise Controller

Muhammad Mudassar Yamin

A close-up, slightly blurred photograph of a clock face. The clock has a white dial with dark blue numbers and hands. The hour hand is pointing exactly at the 12, and the minute hand is also pointing at the 12. A thin, light-colored second hand is visible, also pointing towards the 12. The clock is set against a dark, out-of-focus background. The time 12:00 is displayed in white text over the center of the clock face.

12:00

# Task 1:

Start analyzing the scenario document for Information



## Scenario



## innovative solutions

The organization is a mid-sized manufacturing company based in the United States that specializes in producing high-tech equipment for the automotive industry. The company has been in operation for over 20 years and has a strong reputation in the industry for delivering innovative solutions.


**Financial Outlook:** The company has experienced steady growth over the past few years and has been profitable. However, the manufacturing industry is highly competitive, and the company is facing pressure to reduce costs and increase efficiency to remain competitive. The company has recently invested in digital transformation initiatives to improve operations and streamline supply chain management.

**Public Relations:** The company has a strong commitment to sustainability and has received recognition for its efforts to reduce its carbon footprint. The company also values diversity and inclusion and has implemented policies to promote these values in the workplace. Overall, the company has a positive reputation among its customers and stakeholders.

**Threats Faced:** The company is facing an increasing threat from cyberattacks, particularly ransomware attacks. As a manufacturer, the company has a complex supply chain that includes multiple third-party vendors, which can make it vulnerable to attacks that originate outside the company. The company has invested in cybersecurity measures to prevent such attacks, but the evolving nature of cyber threats means that the company must constantly adapt its security measures to stay ahead of attackers. A cyberattack could have a significant impact on the company's operations and reputation, as well as its financial stability.

*Shaping the present and the future*





12:15

## Task 2:

### Task

- Analyze is the organization is affected by the disaster
- Check how the organization can contribute to the relief effort

### Deliverables

- Create a 2-liner press release on the disaster and present the organization position.
- **Delivery time:12:25**



12:30



## Task 3:

### Task

- Follow the plan in InCaseIT

### Deliverables

- Create a 2-liner press release on the incident and present the organization position.
- **Delivery time:12:55**



13:00



## Task 3:

### Task

- Follow the plan in InCaseIT

### Deliverables

- Create a 2-liner press release on the incident and present the organization position.
- Delivery time:13:25



13:30



## Task 3:

### **Task**

- Follow the plan in crisis plan

### **Deliverables**

- Create a public statement about the crisis
- Delivery time:13:55




14:00

The background of the image is a dark, semi-transparent financial chart. It features a series of white candlesticks representing price movements over time. Several white lines are overlaid on the chart, including a solid line and two dotted lines, likely representing different types of moving averages or trend lines. The overall aesthetic is professional and data-driven.


# Outcomes






**Successful Negotiation and Payment of Ransom:** The company negotiates with the attacker and pays the ransom, receiving the decryption key in return.

However, this could set a precedent for future attacks and may encourage the attacker to target the company again in the future.



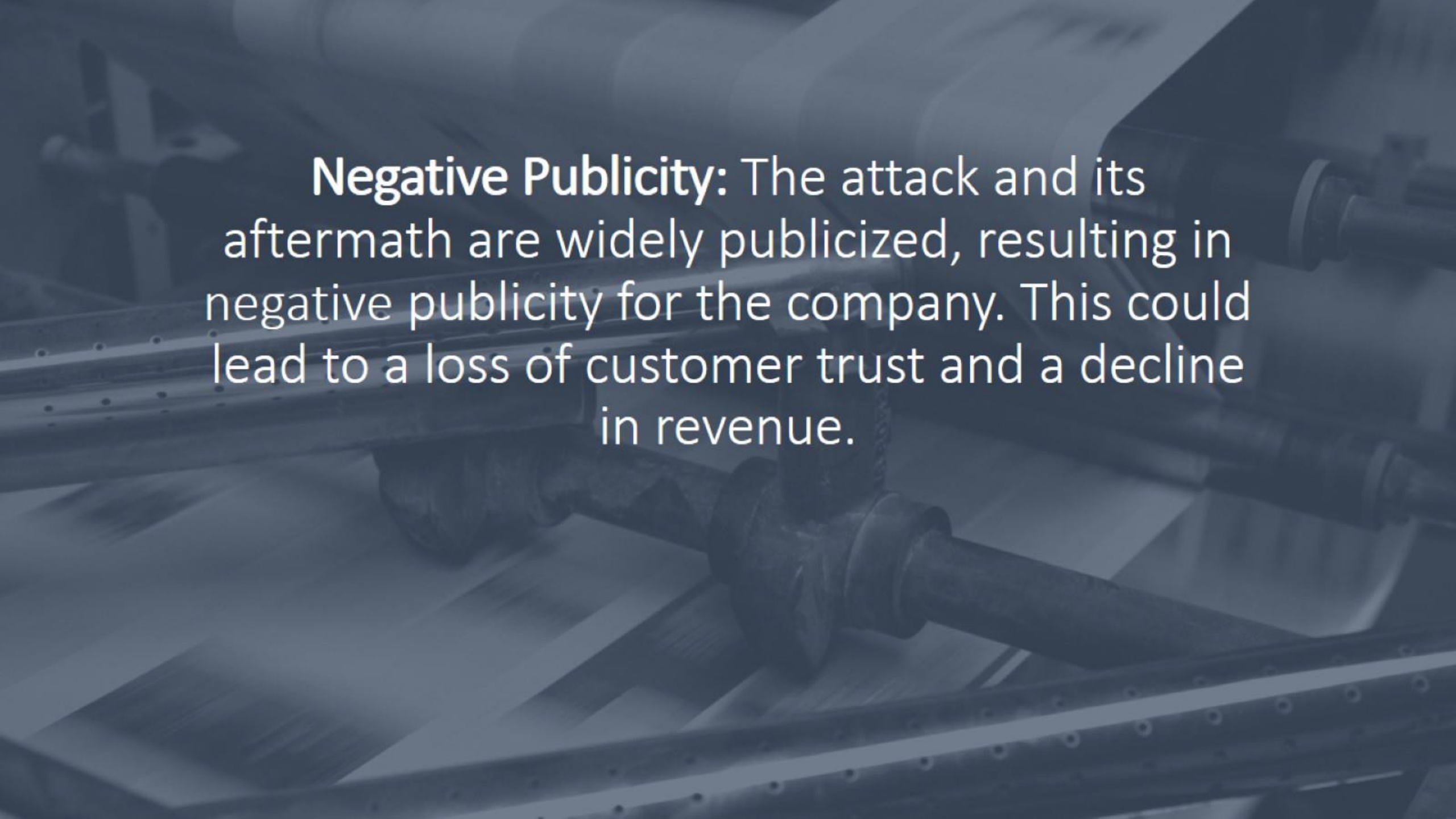
**Partial Recovery:** The company is able to recover some of its data and systems, but not all. This could result in a loss of revenue and reputation damage, as well as possible legal repercussions if sensitive data is compromised.



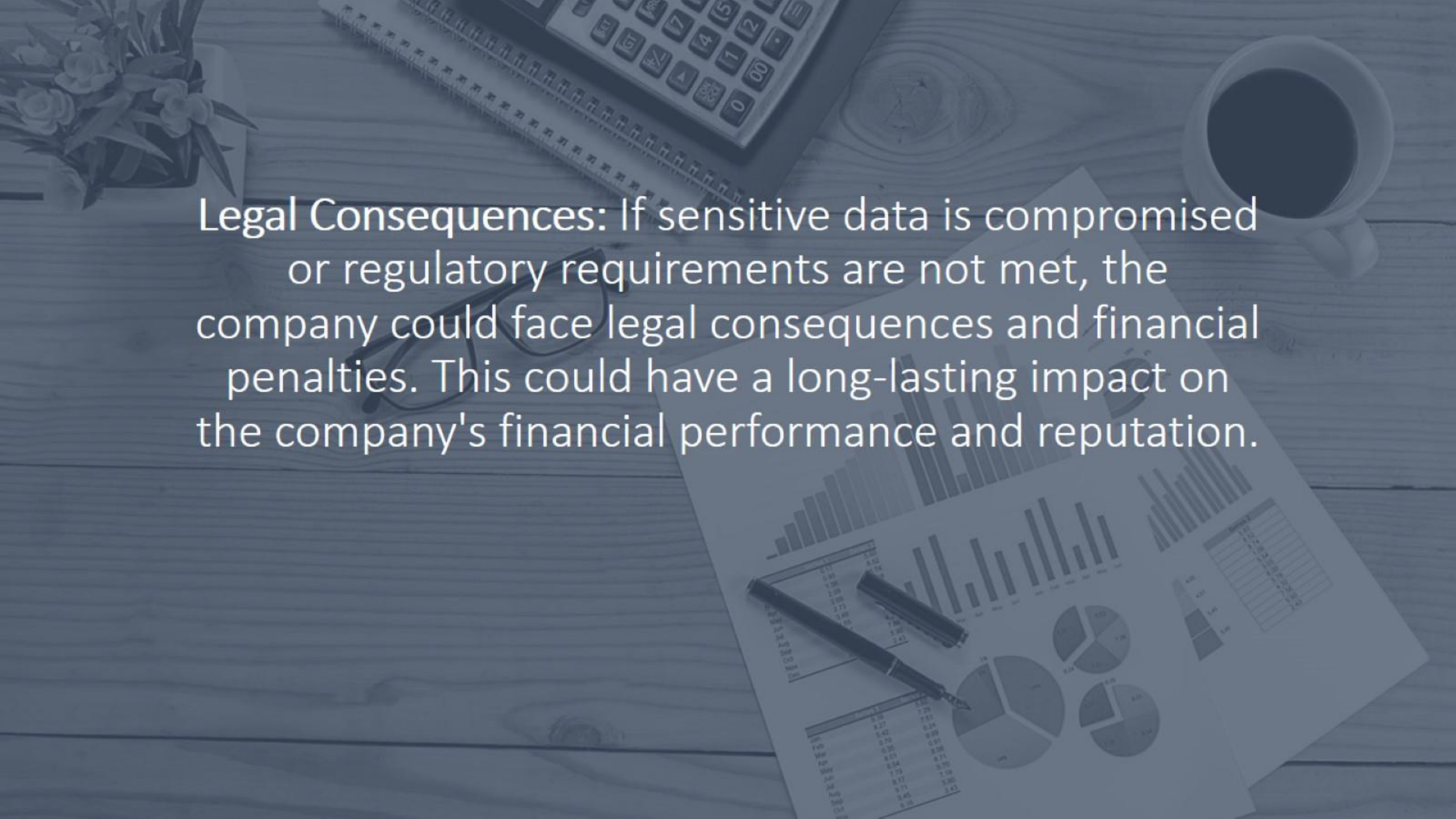
The background of the slide is a dark teal color with a complex, semi-transparent financial chart overlay. The chart includes a line graph with a blue line that trends upwards and then slightly downwards, and a red line that trends upwards. There are also candlestick-style bars in blue and red, and various numerical values and grid lines are visible, though they are faded and serve as a decorative backdrop for the text.

**Failure to Recover:** The company is unable to recover its data and systems, resulting in a significant loss of revenue and customer trust. This could lead to a decline in market share and long-term financial damage.



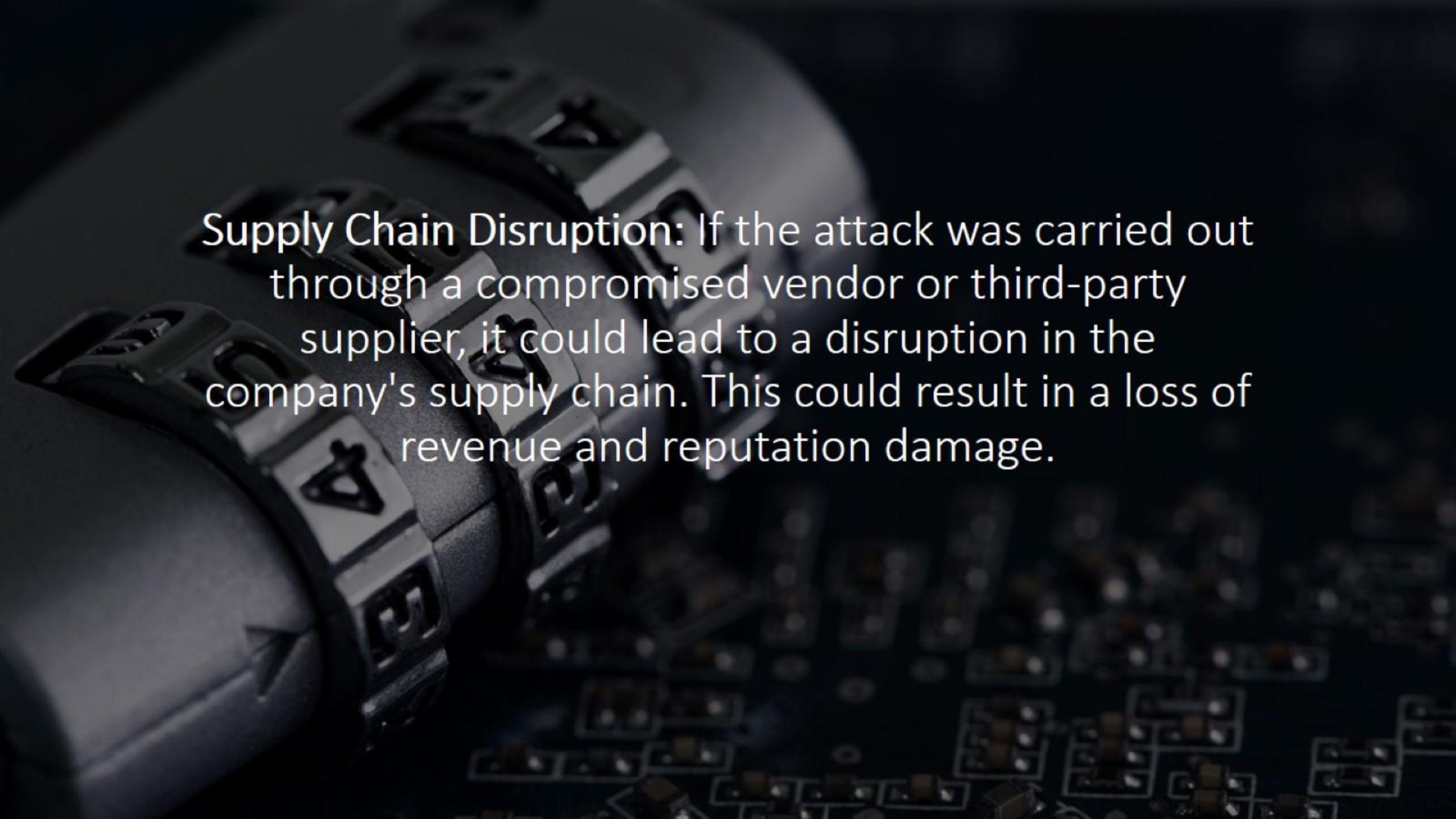


**Negative Publicity:** The attack and its aftermath are widely publicized, resulting in negative publicity for the company. This could lead to a loss of customer trust and a decline in revenue.

A top-down view of a wooden desk. In the top left is a small potted plant with white flowers. Next to it is a silver calculator and a spiral-bound notebook. In the top right is a white mug filled with dark coffee. In the center, a pair of black-rimmed glasses rests on a document. The document features several bar charts, pie charts, and tables of data. A black pen lies diagonally across the bottom half of the document. The entire scene is overlaid with a semi-transparent dark blue filter.


**Legal Consequences:** If sensitive data is compromised or regulatory requirements are not met, the company could face legal consequences and financial penalties. This could have a long-lasting impact on the company's financial performance and reputation.





**Supply Chain Disruption:** If the attack was carried out through a compromised vendor or third-party supplier, it could lead to a disruption in the company's supply chain. This could result in a loss of revenue and reputation damage.



The background of the slide features several interlocking puzzle pieces in a dark blue-grey color. The pieces are arranged in a way that suggests a larger, incomplete picture, with some pieces missing or slightly offset. The lighting creates soft shadows, giving the pieces a three-dimensional appearance.

**Improved Cybersecurity Measures:** The attack prompts the company to invest in stronger cybersecurity measures and policies, leading to improved resilience and protection against future attacks. However, this may come at a significant financial cost.