Group Project II
Table Top Exercise

Honor Pledge: "We pledge on our honor that we have not given or received any unauthorized assistance on this exam/assignment"

Submitted By – Group 2

Group Members and individual Roles Performed-

Role	**Performed By**	**UID**
Exercise facilitator	Aryan Kulshrestha	120342035
CIO	Rachit Arora	120211546
Director of IT Operations	Rohith Chandra Shekaran Nair	120379857
Director of IT Security	Shreya Patil	120405709

INDEX

1. DAY 1

1.1 Director of IT Operations

Objective: The CIO asked the following four questions to the Director of IT Operations on the first day of the tabletop exercise. The facilitator recorded all answers as follows.

I. **What is the scope of the ransomware attack?** (Dice 6)
Only the Scranton office has been infected with ransomware.

II. **What of Dunder Mifflin's IT Operations are still operational?** (Dice 3)
The Akron, Scranton, Stamford, Utica, and Yonkers offices are offline but for other offices it is business as usual.

III. **Does Dunder Mifflin have backups that they can restore from?** (Dice 6)
We still need to assess the scope and determine if restoring from backups is viable. Check back in Round 2.

IV. **Does Dunder Mifflin have IT Operations playbooks in place to reset everyone's passwords and safely rebuild their Active Directory infrastructure?** (Dice 5)
We have detailed instructions which we tested 6 months ago and they proved to be accurate.

1.2 Director of IT Security

Objective: The CIO asked the following four questions to the Director of IT Security on the first day of the tabletop exercise. Further, the facilitator documented all the answers as follows.

I. **Does Dunder Mifflin have an incident response plan and processes in place?** (Dice 4)
We have a highly detailed incident response plan, processes, and we have a dedicated incident response team which can be rapidly "spun up" to perform their duties.

II. **What is the ransom amount?** (Dice 6)
$25 million dollars.

III. **Does Dunder Mifflin have any indication that personally identifiable information has been stolen?** (Dice 3)
From our initial review we are unsure if PII has been stolen.

IV. Does Dunder Mifflin have cyberinsurance? (Dice 5)
We have a cyberinsurance policy that covers up to $5 million in expenses.

1.3 Summary of Day 1

On the first day of the tabletop exercise, the Director of IT Operations reported a ransomware attack on the Akron, Scranton, Stamford, Utica, and Yonkers offices which took them offline. The Director of IT Security also confirmed the presence of an incident response plan with a dedicated team which reported a ransom demand of $25 million with uncertainly when it comes to PII leaks. Dunder Mifflin also has a cyberinsurance policy covering up to $5 million in expenses.

2. DAY 2

2.1 CIO Addresses Ongoing Attack Queries

Objective: Prior to collecting information from IT Operations and IT Security, the facilitator poses several questions to the CIO for insights regarding the ongoing attack.

I. How much revenue is Dunder Mifflin losing every day that they are not operational?
$1 million - (Dice 1)

II. Are there functioning backups for Dunder Mifflin to restore from?
We don't have immediate functioning backup but we do have offline immutable backup which takes 10 days to fully rebuild our entire infrastructure.

III. If Dunder Mifflin has cyber insurance, is the cyber-insurer being brought in to assist with negotiations to pay the ransom and recover your data?
Yes, if Dunder Mifflin has cyber insurance covering up to $5 million in expenses, the cyber-insurer should be brought in to assist with negotiations to pay the ransom and recover data. However, the final decision to engage the cyber-insurer should be made by the CIO and Board of Directors, considering the terms of the insurance policy, financial implications, and overall strategy for ransom negotiation and data recovery.

2.2 Director of IT Operations

Objective: After gathering revenue and backup information, the facilitator prompts the CIO to obtain specific insights from IT Operations through relevant questioning.

I. **With an additional 24 hours, what is the status of our backups? Can we recover from them?** (Dice 6, same value as Day1 question 3)
We believe we can fully recover our critical data thanks to offline immutable backups. It will take 10 days to fully rebuild our entire infrastructure.

II. **Have we reset everyone's password? (**Dice 5, same value as Day1 question 4)
Yes, we have an 50% of users have reset their password on our newly rebuilt and deployed Active Directory infrastructure.

2.3 Director of IT Security

Objective: The facilitator now directs the CIO to gather details from IT Security on questions related to stolen data and PII.

I. **Based on what the security researcher has shared with us do we think customer or employee data has been stolen?** (Dice 3, Day1 question 3)
We believe that only employee PII has been stolen, a few thousand records. It will cost $50,000 to provide credit monitoring for those impacted.

II. **If we have cyber-insurance, are we bringing them in to assist with negotiations to pay the ransom and recover our data. (**Dice 5, day1 question 4**)**
We have a cyberinsurance policy that covers up to $5 million in expenses. We need the CIO and Board of Directors to determine if we should engage the cyberinsurance policy.

2.4 Summary of Day 2

On the second day, the CIO revealed that Dunder Mifflin is losing $1 million in revenue daily due to the attack & confimed they can fully rebuild the infrastructure within 10 days with the offline immutable backups. The Director of IT Operations reported that critical data could be fully recovered from the backups and that 50% of users have reset their passwords on the newly rebuilt Active Directory infrastructure. The Director of IT Security indicated that only employee PII was stolen, with an estimated $50,000 needed for credit monitoring, and mentioned the need for a decision from the CIO and Board on engaging the cyberinsurance policy for negotiations.

3. DAY 3

3.1 Cost Estimate by CIO

Objective: The CIO assesses the incident's cost, considering factors such as duration, revenue, insurance, and estimated losses. Further, the CIO briefly responds to three questions.

Count the number of days your organization has been offline and predicts they will be offline

- 3 days from this exercise
- The number of days to restore operations (see IT Operations Day 2 Question 1 for this estimate) = 10 days for restoration of backups
- The total number of days = 3+10 =**13 days**

Take this estimate of days and multiply it by the cost per day of lost revenue (Day 2 Question 1 for the CIO) = **$1million**
Number of days x Daily lost revenue = Total lost estimate. Record number:
13 x 1 million = **$13 million**

I. How much revenue do you estimate will be lost from this incident?
The estimated loss in revenue from this incident is $13 million.

II. Is the lost estimate greater than or less than what the cyberinsurance policy is?
The estimated loss of $13 million exceeds the coverage provided by the cyberinsurance policy, which covers up to $5 million in expenses.

III. Should we engage the cyber insurance company?
Yes, it is advisable to engage the cyber insurance company given that the estimated loss exceeds the coverage provided by the policy. Engaging the cyber insurer can help mitigate financial losses and facilitate the recovery process.

3.2 Summary of Day 3

On day 3, CIO provided a cost estimate for the ransomware incident, predicting a total of 13 days offline (3 days already offline and 10 days needed for restoration). The CIO also confirmed that this estimated loss exceeds the $5 million coverage of the cyberinsurance policy with emphasis on engaging the cyber insurance company to help mitigate the financial losses and assist with the recovery process.

4. LESSONS LEARNED

The scenario presenting the presence of ransomware attack for the tabletop exercise, along with the regional offices with Active Directory domains Scranton (scranton.dm.com), Stamford (stamford.dm.com), Utica (utica.dm.com), and Yonkers (yonkers.dm.com) experienced disruptions but the other Dunder Mifflin offices continued their regular operations without any issues. This helped in mitigating the impact of the attack and maintain some level of business functionality during the attack.

4.1 What went well for Dunder Mifflin

I. **Effective Preparedness:** Dunder Mifflin demonstrated preparedness with detailed instructions for IT operations and a dedicated incident response team, ensuring an organized response to the ransomware attack.
II. **Strategic Risk Management:** The decision to secure cyber insurance coverage was beneficial, offering financial protection against unexpected expenses arising from the incident.
III. **Backup Resilience:** Despite facing initial obstacles with immediate backups, relying on offline immutable backups was crucial in enabling data recovery, even though it took longer to restore the data.

4.2 Areas of Improvements

I. **Enhanced Backup Strategy:** To minimize downtime and maximize data protection, it is necessary to strengthen overall backup redundancy with diverse solutions, along with off-site storage options
II. **Proactive Threat Detection:** Strengthening the monitoring tools with regular security assessments could help in detecting and mitigating cyber-attacks, thus reducing their impact in the future.
III. **Optimized Communication Protocols:** Making communication rules better so that everyone - employees, customers, and insurance companies - gets information quickly and clearly can build trust and stop the company's reputation from getting damaged.

4.3 Top Recommendations for Improvements

I. **Routine Plan Testing:** Regularly test incident response plans, including backup procedures, will ensure their effectiveness and identify areas for refinement.
II. **Employee Training:** Investing in ongoing cybersecurity awareness training allows employees to recognize and respond to threats ensuring overall security.
III. **Threat Monitoring:** Implementing advanced threat monitoring solutions which enables proactive threat identification and response.