ENPM685 Group Project - Tabletop Exercise

Prepared by: Group 11

Team Members and Roles

Role	Performed By	UID
Exercise Facilitator	Raghava Gatadi	121941190
CIO	Riti Dobariya	120475986
Director of IT Operations	Heet Gala	122030916
Director of IT Security	Sheldon Douglas	117865974

Day 1 Round Questions to Answer

1. What is the scope of the ransomware attack?

Only the Scranton office has been infected with ransomware.

2. What of Dunder Mifflin's IT Operations are still operational?

Only the Scranton office is offline.

3. Does Dunder Mifflin have backups that they can restore from?

We still need to assess the scope and determine if restoring from backups is viable, we are doubtful they will work. Check back in Round 2.

4. Does Dunder Mifflin have IT Operations playbooks in place to reset everyone's passwords and safely rebuild their Active Directory infrastructure?

We do not have playbooks for any of our IT operations.

5. Does Dunder Mifflin have an incident response plan and processes in place?

We do not have a written incident response plan or any documented playbooks.

6. What is the ransom amount?

$25 million dollars

7. Does Dunder Mifflin have any indication that personally identifiable information has been stolen?

From our initial review we are unsure if PII has been stolen.

8. Does Dunder Mifflin have Cyber Insurance?

We do not have a cyberinsurance policy.

Day 2 Round Questions to Answer

1. How much revenue is Dunder Mifflin losing every day that they are not operational?

$10,000 per day.

2. Are there functioning backups for Dunder Mifflin to restore from?

We believe we can restore about 50% of our data. The data we will not be able to recover is an even split - half is critical to business operations and the other half is nonessential. It will take 20 days to recover the data and rebuild our systems.

3. Have we reset everyone's password?

Since we did not have a playbook for this, we are doing this on the fly and expect it to be complete in 2-3 days.

4. Based on what the security researcher has shared with us do we think customer or employee data has been stolen?

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.

5. If Dunder Mifflin has cyber insurance, is the cyberinsurer being brought in to assist with negotiations to pay the ransom and recover your data?

We do not have a cyberinsurance policy.

Day 3 Round Questions to Answer

1. How much revenue do you estimate will be lost from this incident?

23 days (3 days from exercise + 20 days to restore) × $10,000 (daily estimated revenue) = **$230,000**

2. Is the lost estimate greater than or less than what the cyberinsurance policy is?

N/A - We do not have any cyberinsurance policy in place.

3. Should we engage the cyber insurance company?

No, we do not have cyberinsurance to engage.

Lessons Learned

The Scranton office was infected by a ransomware attack and estimated recovery time is 23 days (with exercise timeline of 3 days and restoration of 20 days). The breach led to the estimated revenue losses of $230,000, 50% of critical business data, and a proven breach of employee PII of several thousand records.

1. What Went Well

1. It was soon realized that the extent of the issue was limited to the Scranton office, and it did not extend to the rest of the branch locations. Consequently, it could not be spread immediately to the other offices, and they were still able to conduct their business activities.

2. The team hired a security researcher, who assisted in evaluating data exfiltration and verified that employee PII had been breached, a required measure in compliance with regulations and for notifying the victims.

3. The team was able to compute the estimated total downtime (23 days) and the resulting lost revenue ($230,000) by Day 3, which is crucial to decision-making by the executives and prioritization of recovery.

2. Areas Needing Significant Improvement

1. Lack of Preparedness

No Incident Response plans and playbooks have been written. The most important recovery operations (such as password reset/AD rebuild) were required to be completed during the extremely slow recovery process (2-3 days of password resets alone).

2. Recovery Strategy

The backup was insufficient and unreliable. The percentage of recoverable data was only 50%, and half of the lost data was vital to business operations. The estimated time for rebuilding systems and data recovery of 20 days is too long, indicating no tested Disaster Recovery plan.

3. Financial Risk Mitigation

No Cyberinsurance Policy. The firm needs to cover the entire cost of the attack ($25M ransom demand, $230K in lost revenue, $50K for credit monitoring, plus legal and recovery fees), with no financial bail or professional third-party help that is usually offered through insurance.

4. Business Resilience

Low network segmentation allowed the ransomware to affect an entire office location. Although Scranton was the only affected area, it was entirely shut down as well, meaning it is prone to single points of failure.

5. Data Protection Assessment

The first PII test was nonproductive (Day 1). Although this was later established, the lag in the awareness of the breach of employee data may have been a reason why the regulatory reporting processes were delayed.

3. Top 3 Items for Incident Response Improvement

Priority 1: Build, write, and test a Full Incident Response Plan and Ransomware Playbooks. This plan should outline specific roles, communication pathways and stepwise technical playbooks for any organizational critical activities.
Action: Tabletop exercises should be conducted annually to verify the effectiveness of the plan and ensure all team members are familiar with their roles and responsibilities.

Priority 2: Enact and Test a Contemporary Air-Gap Backup and Disaster Recovery Strategy. Use the 3-2-1 backup policy (three data copies, two types of media, one copy located offsite/offline/immutable). The current case of backup, where only half of the data can be recovered, is unacceptable in terms of business continuity.
Action: Conduct quarterly test restores to check the recovery time objective (RTO) and accessibility of all essential business data in an uncorrupted form. This will reduce the existing 20-day recovery window by a substantial margin to a more reasonable length.

Priority 3: Acquire Cyberinsurance Policy and Legal/Forensic Retainers. A cyberinsurance policy will cover significant ransom payments, revenue loss, attorney fees, and incident response expenses. The loss of $ 230,000 and credit monitoring expenses of $ 50,000, in addition to the ransom demand of $ 25 million, reveal that the financial risk must be transferred.
Action: Cyber insurers often require minimum security measures (such as MFA, tested backups, and IR plans) in order to get coverage. Such controls will ensure that Dunder Mifflin is eligible to receive insurance, while also enhancing the security posture in general. The insurance policy also links the company to seasoned legal advice and forensic experts, instantly, which would have expedited the initial containment and decision-making process.