Topic: Emergency Meeting on Cyberattack Response

Type: [Decision Making Meeting]

Date: [19th April 2024]

Time: [2:15 PM]

Location: [FAST NUCES Karachi Campus, Library Building, Basement, Conference Room 8]

Attendees:

1. Chair: Talha (CEO)

2. Facilitator: Sufyan

3. Notetaker + Timekeeper: Zubair

4. Chief Financial Officer (CFO): Affan

5. Public Relations Officer (PRO): Fareed

6. IT Head of Department (HOD): Hasnain

7. Chief Human Resources Officer (CHRO): Moazzam

8. Legal Advisor: Aqib

9. External Observer: Mukesh

Absentees:

[NONE]

Meeting Agenda / Agenda Items:

1. Assessment of Damage and its Legal Implications

2. Virus Source Identification

3. Data Recovery

4. Human Resources Concerns

5. Security Enhancement

6. Financial Recovery

Discussion Key Points:

a. Welcome and Introduction

The meeting commenced at [2:15 P.M] with a warm welcome extended to all attendees by [Sufyan] – [Facilitator].

Introduction of new team members, [Mukesh] - [External Observer], who has recently joined the team.

b. Review of Previous Action Items

Action items from the previous meeting were reviewed.

[Affan] reported that the financial analysis regarding cost-cutting measures is underway.

[Moazzam] mentioned that the HR department has completed the review of employee feedback surveys.

[Hasnain] reported that the IT department has implemented security patches for critical vulnerabilities in the system.

c. Meeting Proceedings / Discussion Topics

1. Assessment of Damage and its Legal Implications

The meeting began with Talha, the CEO, setting the stage by acknowledging the severity of the cyberattack and emphasizing the importance of addressing its legal implications.

Hasnain, the IT HOD, presented a comprehensive assessment of the damage to IT systems, outlining the extent of data loss and potential vulnerabilities.

Aqib, the Legal Advisor, provided insights into the legal risks associated with the cyberattack, emphasizing the need for risk mitigation strategies and compliance with data protection laws.

2. Virus Source Identification

Talha directed the discussion towards identifying the source of the virus, prompting Hasnain to share insights from the IT department's forensic analysis.

Hasnain elaborated on the methods used to trace the origins of the cyberattack, including examining system logs and collaborating with external cybersecurity experts.

3. Data Recovery

Talha emphasized the urgency of prioritizing data recovery efforts, prompting Hasnain to outline potential methods and timelines for data restoration.

Hasnain discussed the implementation of robust data backup and recovery solutions, including automated backup systems and cloud storage.

4. Human Resources Concerns

Talha turned the discussion towards addressing employee concerns and supporting them through the crisis, prompting Moazzam, the CHRO, to outline HR strategies.

Moazzam highlighted the importance of employee communication and engagement, as well as the legal obligations related to data protection and employee rights.

5. Security Enhancement

Talha underscored the need for strengthening cybersecurity measures to prevent future attacks, prompting Hasnain to present recommendations for security enhancement.

Hasnain discussed measures such as updating antivirus software, conducting regular security audits, and enhancing encryption protocols.

6. Financial Recovery

Talha requested Affan, the CFO, to provide an assessment of the financial impact of the cyberattack and propose mitigation strategies.

Affan outlined the potential costs incurred, including downtime and regulatory fines, and discussed mitigation strategies such as increasing investment in cybersecurity and exploring insurance claims.

d. New Business

[Moazzam] raised concerns regarding [employee training].

[Moazzam] brought up topic [comprehensive research conduct pertaining security infrastructure including employee training] for discussion, inquiring corroboration from chair [Talha].

[Talha] gave [Moazzam] the greenlight for said requisition and asked [Moazzam] to compile a list of employees detailing their skills and talents.

Subsequently [Talha] requested [Hasnain] to collaborate with [Moazzam] to resolve any IT-relative issues the employees efficiently and effortlessly might face.

e. Next Steps

Talha outlined next steps, including scheduling a follow-up meeting to review performance metrics and sharing insights with all departments to encourage collaboration and learning. Key decisions were summarised. Next meeting scheduled for Friday upcoming week.

f. Meeting Adjournment / Closing Arguments

The meeting concluded at [2:26:33 PM] with Talha expressing appreciation for the team's efforts and highlighting the importance of targeted actions in mitigating the impact of the cyberattack. Sufyan extended appreciation to all attendees for their active participation and contributions. Reminders given to follow up on action items and stay engaged until the next meeting.

g. Action Items (Recap)

The meeting concluded with the identification of action items. Action items were assigned as follows:  
1. [Develop a comprehensive risk mitigation plan addressing legal implications]: [Aqib, Hasnain]  
2. [Conduct a detailed forensic analysis to identify the source of the virus]: [Hasnain]  
3. [Implement robust data backup and recovery solutions]: [Hasnain]  
4. [Revise and update HR policies to ensure compliance with data protection laws]: [Moazzam]  
5. [Enhance cybersecurity measures by updating antivirus software and conducting regular audits]: [Hasnain]  
6. [Assess the financial impact of the cyberattack and propose mitigation strategies]: [Affan]

h. Next meeting

Date: [Friday – 26th April 2024] + Time: [10:00 AM – 11:30 AM]

Location: [FAST – NUCES Karachi Campus, Library Building, Basement, Conference Room 8].

M.O.M Prepared by: [Zubair]

Position: [Notetaker + Timekeeper]

Contact Information: [0320-3060747]

M.O.M reviewed by: [Talha]