In-Class Activity #4’

Name: ABHISHEK YADAV EUID:11816766

**Instructions:** You are presented with a list of some risks and threats associated with the domains of a

typical IT infrastructure. Below the list, the solutions or preventive actions to manage those risks and

threats are listed. Write the letter of the correct solution or preventative action in the blank to the right of

each risk or threat.

**Risks or threats:**

1. Violation of a security policy by a user \_\_\_C \_\_\_

2. Disgruntled employee sabotage \_\_\_ I\_\_\_\_\_

3. Download of non-business videos using the

Internet to an employer-owned computer \_\_\_A\_\_\_\_\_

4. Malware infection of a user’s laptop \_\_\_L\_\_\_\_

5. Unauthorized physical access to the LAN. \_\_\_N\_\_\_\_\_

6. LAN server operating system vulnerabilities \_\_\_F\_\_\_\_\_

7. Download of unknown file types from unknown sources by local users \_\_\_B\_\_\_\_

8. Errors and weaknesses of network router, firewall, and network

appliance configuration file \_\_\_H\_\_\_\_\_

9. WAN eavesdropping \_\_\_M\_\_\_\_

10. WAN denial of service (DoS) or distributed denial of

service (DDoS) attacks \_\_D\_\_\_\_\_

11. Confidential data compromised remotely \_\_\_K\_\_\_\_\_

12. Mobile worker token stolen \_\_\_G\_\_\_\_\_

13. Corrupt or lost data \_\_\_E\_\_\_\_\_

14. Downtime of customer database \_\_\_J\_\_\_\_\_

**Solutions or preventive actions:**

A. Enable content filtering and antivirus scanning at the entry and exit points of the Internet. Enable

workstation auto-scans and auto-quarantine for unknown file types.

B. Apply file transfer monitoring, scanning, and alarming for unknown file types and sources.

C. Place employee on probation, review acceptable use policy (AUP) and employee manual, and

discuss status during performance reviews.

D. Apply filters on exterior Internet Protocol (IP) stateful firewalls and IP router WAN interfaces.

E. Implement daily data backups and off-site data storage for monthly data archiving. Define data

recovery procedures based on defined Recovery Time Objectives (RTOs).

F. Define vulnerability window policies, standards, procedures, and guidelines. Conduct LAN

domain vulnerability assessments.

G. Apply real-time lockout procedures.

H. Define a strict zero-day vulnerability window definition. Update devices with security fixes and

software patches right away.

I. Track and monitor abnormal employee behavior, erratic job performance, and use of IT

infrastructure during off-hours. Begin IT access control lockout procedures based on AUP

monitoring and compliance.

J. Develop a disaster recovery plan (DRP) specific to the recovery of mission-critical applications

and data to maintain operations.

K. Encrypt all confidential data in the database or hard drive.

L. Use workstation antivirus and malicious code policies, standards, procedures, and guidelines.

Enable an automated antivirus protection solution that scans and updates individual workstations

with proper protection.

M. Use encryption and virtual private network (VPN) tunneling for secure IP communications.

N. Make sure wiring closets, data centers, and computer rooms are secure. Provide no access

without proper credentials.