**Instructions:**

You are presented with a table of risks and threats associated with the seven domains of a typical IT infrastructure. Below the table are solutions or preventative actions to manage the risks and threats. Enter the letter of the correct solution or preventative action in the blank to the right of each risk or threat.

|  |  |
| --- | --- |
| **Risk/Threat** | **Solution/ Preventative Action** |
| 1.  Security policy violation | C |
| 2.   Compromised confidentiality of data transmissions via WLAN | A |
| 3.   Unauthorized network probing and port scanning | H |
| 4.   IP router, firewall, and network appliance operating system software vulnerability | G |
| 5.   Private data or confidential data compromised remotely | K |
| 6.   A mobile worker’s laptop may be stolen | B |
| 7.   Infection of a user’s workstation or laptop computer by viruses, malicious code, or malware | L |
| 8.  Insecure cloud computing virtual environments by default | F |
| 9.  Downtime of IT systems for an extended period after a disaster | J |
| 10. Attacks on the organization or acts of sabotage by disgruntled employees | I |
| 11. Vulnerable to DoS, DDoS, TCP SYN flooding, and IP spoofing attacks | D |
| 12. Employees and users want to use their own smartphone or tablets | E |

**Solutions or Preventative Actions**

A. Implement encryption between workstation and WAP to maintain confidentiality.

B. Encrypt the data on the hard drive if the user has access to private or confidential data. Apply real-time lockout rules when told of a lost or stolen laptop by a user.

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 wide area network (WAN) interfaces.

E. Develop a Bring Your Own Device (BYOD) policy and procedure. BYOD policies and procedures typically permit the organization to data-wipe the user’s smartphone or mobile device if it is lost or the employee is terminated.

F. Implement virtual firewalls and server segmentation on separate virtual LANs (VLANs). A virtual firewall is a software-based firewall used in virtual environments.

G. Define a strict zero-day vulnerability window definition. Update devices with security fixes and software patches right away.

H. Disable ping, probing, and port scanning on all exterior IP devices within the LAN-to-WAN Domain. Ping uses the Internet Control Message Protocol (ICMP) echo-request and echo-reply protocol. Disallow IP port numbers used for probing and scanning and monitor with IDS/IPS.

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 within 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.