**Administrative/Managerial Controls:**

1. **Least Privilege:**
   * **Control Type:** Preventative
   * **Control Purpose:** Reduce the risk and overall impact of malicious insider or compromised accounts.
   * **Comments:** This control is crucial for limiting access and potential damage caused by insider threats. Ensure proper implementation and periodic reviews.
2. **Disaster Recovery Plans:**
   * **Control Type:** Corrective
   * **Control Purpose:** Provide business continuity.
   * **Comments:** A critical control to ensure the organization can recover from incidents. Regularly test and update the plans to ensure effectiveness.
3. **Password Policies:**
   * **Control Type:** Preventative
   * **Control Purpose:** Reduce the likelihood of account compromise through brute force or dictionary attack techniques.
   * **Comments:** Enforce strong password policies in line with industry standards to enhance the security of user accounts.
4. **Access Control Policies:**
   * **Control Type:** Preventative
   * **Control Purpose:** Bolster confidentiality and integrity by defining which groups can access or modify data.
   * **Comments:** Clearly defined access control policies are essential for maintaining data confidentiality and integrity. Regularly review and update.
5. **Account Management Policies:**
   * **Control Type:** Preventative
   * **Control Purpose:** Managing account lifecycle, reducing attack surface, and limiting overall impact from disgruntled former employees and default account usage.
   * **Comments:** Proper account management is crucial for minimizing security risks. Ensure comprehensive policies and procedures are in place.
6. **Separation of Duties:**
   * **Control Type:** Preventative
   * **Control Purpose:** Reduce the risk and overall impact of malicious insider or compromised accounts.
   * **Comments:** Implementing separation of duties is essential for preventing conflicts of interest and minimizing the potential for unauthorized activities.

**Technical Controls:**

1. **Firewall:**
   * **Control Type:** Preventative
   * **Control Purpose:** To filter unwanted or malicious traffic from entering the network.
   * **Comments:** Ensure proper configuration and regular updates to effectively filter and block unauthorized access.
2. **IDS/IPS:**
   * **Control Type:** Detective
   * **Control Purpose:** To detect and prevent anomalous traffic that matches a signature or rule.
   * **Comments:** Regularly update signatures and rules to detect emerging threats. Implement response mechanisms for identified incidents.
3. **Encryption:**
   * **Control Type:** Deterrent
   * **Control Purpose:** Provide confidentiality to sensitive information.
   * **Comments:** Implement encryption for sensitive data, especially customer credit card information, to ensure confidentiality.
4. **Backups:**
   * **Control Type:** Corrective
   * **Control Purpose:** Restore/recover from an event.
   * **Comments:** Regularly test backup restoration processes. Ensure backups cover all critical data.
5. **Password Management:**
   * **Control Type:** Preventative
   * **Control Purpose:** Reduce password fatigue.
   * **Comments:** Implement effective password management tools and practices. Consider multi-factor authentication for enhanced security.
6. **Antivirus (AV) Software:**
   * **Control Type:** Corrective
   * **Control Purpose:** Detect and quarantine known threats.
   * **Comments:** Regularly update antivirus definitions and ensure real-time monitoring. Implement additional endpoint protection measures.
7. **Manual Monitoring, Maintenance, and Intervention:**
   * **Control Type:** Preventative
   * **Control Purpose:** Necessary to identify and manage threats, risks, or vulnerabilities to out-of-date systems.
   * **Comments:** Regularly monitor and maintain systems to identify and address vulnerabilities promptly.

**Physical/Operational Controls:**

1. **Time-Controlled Safe:**
   * **Control Type:** Deterrent
   * **Control Purpose:** Reduce the attack surface and overall impact from physical threats.
   * **Comments:** Implement time-controlled safes where applicable to deter unauthorized access during specific times.
2. **Adequate Lighting:**
   * **Control Type:** Deterrent
   * **Control Purpose:** Deter threats by limiting "hiding" places.
   * **Comments:** Ensure well-lit areas to deter potential intruders and improve overall physical security.
3. **Closed-Circuit Television (CCTV):**
   * **Control Type:** Preventative/Detective
   * **Control Purpose:** Both preventative and detective. Presence reduces the risk of certain events, and it can be used after an event to inform on event conditions.
   * **Comments:** Regularly check and maintain CCTV systems. Use footage for post-event analysis and investigations.
4. **Locking Cabinets (for Network Gear):**
   * **Control Type:** Preventative
   * **Control Purpose:** Bolster integrity by preventing unauthorized personnel and other individuals from physically accessing or modifying network infrastructure gear.
   * **Comments:** Ensure network gear is securely stored in locked cabinets to prevent tampering or unauthorized access.
5. **Signage Indicating Alarm Service Provider:**
   * **Control Type:** Deterrent
   * **Control Purpose:** Deter certain types of threats by making the likelihood of a successful attack seem low.
   * **Comments:** Clearly visible signage can deter potential intruders. Ensure signs are prominent and up to date.
6. **Locks:**
   * **Control Type:** Deterrent/Preventative
   * **Control Purpose:** Bolster integrity by deterring and preventing unauthorized personnel, individuals from physically accessing assets.
   * **Comments:** Regularly inspect and maintain locks to ensure they function properly. Consider upgrading to more secure locking systems.
7. **Fire Detection and Prevention (Fire Alarm, Sprinkler System, etc.):**
   * **Control Type:** Detective/Preventative
   * **Control Purpose:** Detect fire in the physical location and prevent damage to physical assets.
   * **Comments:** Regularly test and maintain fire detection and prevention systems. Ensure they comply with safety standards.

**Overall Recommendations:**

* Periodically review and update policies, procedures, and controls to adapt to evolving threats and business needs.
* Conduct regular training sessions to ensure employees are aware of security protocols.
* Collaborate with IT and business units to integrate controls seamlessly into day-to-day operations.
* Establish a regular schedule for monitoring and maintenance of both technical and physical controls.
* Continuously assess the effectiveness of controls and adjust as needed based on emerging threats and vulnerabilities.