Risks

1. Database tampering/deletion
   * Risk Exposure – High Risk
     + Probability: 10%
     + Loss: 2 hours
     + Prevention: Make sure we have RAID setup for back ups.
2. Emails getting hacked
   * Risk Exposure – Moderate Risk
     + Probability: 25%
     + Loss: 2 weeks
     + Prevention: We need to make sure our email threat prevention is updated when potential threats arise
3. Damage to hardware
   * Risk Exposure – Minor Risk
     + Probability: 50%
     + Loss: $100
     + Prevention: Have cases on devices that can have them to help protect the hardware
4. Customers gain access to unauthorized websites
   * Risk Exposure – Minor Risk
     + Probability: 10%
     + Loss: 2 days
     + Prevention: The best way to prevent is to make sure the firewall is configured and if needed make sure we update the sites that we don’t want visited.
5. WiFi goes down
   * Risk Exposure – Moderate Risk
     + Probability: 15%
     + Loss: 2.5 hours
     + Prevention: Have a plan of action if the wifi does go down. Set boundaries on the wifi for prevention of DDOS.

Risk Responses

1. Database tampering/deletion
   1. Have a backup ready to go at all times. (Mitigation)
   2. Create prepared statements ready to catch any potential SQL injection attempts. (Mitigation/Avoidance)
   3. **Contingency Plan:** Load the back up, to get the database backup and running.
2. Emails getting hacked
   1. Buy another firewall for better protection. (Transfer)
   2. Instruct employees to not open any links from a non-company email and click on any links found in emails. (Mitigate/Transfer)
   3. **Contingency Plan:** Lock down the account immediately, reset the users password.