Justin Espiritu
Security
Assignment 1

1.) **Physical control** - If the welding machine didn't have a USB access, such as a USB port lock, this could have been avoided completely.
Technical control - Having an access level that does not allow installation or updates without admin access could have also prevented this from happening
Procedural control - If some type of training was in place to make sure users should not connect any other devices to welding machines this also could have been prevented

2.) **Procedural control** - Some type of training to spot phishing emails and make sure that users don't open such emails
Preventive control - If some type of filter that prevented this type of email from getting to the user this also could have been avoided
Detective control - A piece of software could have been installed that could detect such keylogger when it is downloaded. Then this could have led to some sort of corrective control which could have prevented the information from getting siphoned from the keylogger.

3.) **Procedural control** - Some type of policy that to verify that the person calling was in fact from the IT Service Desk, or even training for people in HR so they don't install such software
Technical control - Someone from HR shouldn't have the access level to be able to install such programs. If such permissions were in place it could have prevented this security disaster
Preventive control - Some sort of firewall that blocks IP addresses from remoting in or even connecting to the computer could have also prevented this from happening

4.) **Procedural control** - Employee should have been trained to not plug in unknown usbs into computers and instead bring them to security or something of the sort
Corrective control - Some sort of plan in place, such as powering off computers that haven't been infected yet, that would prevent the worm from spreading
Preventive control - If the computers in the front had USB locks, this issue could have been avoided. I mean why would the front employees need access to USB other than a keyboard and mouse.

5.) **Technical control** - Employee S shouldn't be able to push and patch code to a test environment. Instead only a manager or lead should have access to be able to push such code to an environment.
Procedural control - Secure code policies could have been put in. Similar to the Technical control above with the permission access, a policy should have been put in that would prevent any developers from pushing code to the test environment and only a hand full of leads should be able to push code to such environment
Detective control - There should be some sort of alert that is sent to lead developers when code is pushed to the test environment. Then this code could have been rolled back and taken out of the test environment.

Justin Espiritu
Security
Assignment 1