Robert Fink
rwfwcb
Simplified Risk Assessment

Step 1: CONTEXT

1. Education

2. On account of users are coming in and out often for class, there is some risk of a user forgetting to logout. If this were to happen and a different user got on the account, they could possibly log into some other accounts that are still logged in, in order to steal information from that user. FERPA could be at risk here as well if the user is still logged into myZou, because the attacker could easily access the user's grades.

3. I would the MU IT Program is willing to accept low risk in this lab. My reason for this is because of the security measures already put in place. Security measure here would refer to: 1. students must log in with a pawprint. 2. There a multiple security cameras facing different directions to capture the entire room on video. 3. There is a sturdy door to lock up the lab. 4. There are metal storage cabinets with audio recording equipment, etc. that are locked with a padlock.

Step 2: ASSET IDENTIFICATION

1. Looking around the room, the assets we are most concerned about protecting are the many lab computers. The nice new TV at the front of the room is also of concern.

2. Less obvious would be the computer monitors, mice, security cameras, and sound equipment like mics and headsets. These assets need protection from users who might spill liquid on them, or possibly do something more malicious.

Step 3: THREAT IDENTIFICATION

1. The lab computers could face threats from users hijacking someones account after they forget to logout, or a user could potentially install a malicious program to a number of potentially different and dangerous things. The nice TV at the front of the room faces risk from potential theft, or vandalism. The monitors, mice, mics, and headsets all face the risk of being stolen or destroyed. The security cameras are at risk of being destroyed or vandalized.

Step 4: VULNERABILITY IDENTIFICATION

1. Potential vulnerabilities that could affect the lab computers could be a malicious user. The machines are also connected to the internet, which might be a vulnerability (I know there is a

firewall but I'm not sure how it works and how bulletproof it is). The machines need internet so this can't be removed, but a filter could be set up to possible black list some websites.

Step 5. RISK ANALYSIS

1. The likelihood of such an attack occurring is probably very low. My reason for this is because it is my belief that most Mizzou students are generally good people, who are here to better themselves. It is my belief that those who might think of doing something malicious would be deterred by the security cameras and the necessary pawprint login.

Step 6. ANALYZE EXISTING CONTROLS

1. Existing security controls are: 1) users must log in with their pawprint. This should deter a student from doing malicious things on the machine because it could be traced back to them. 2) the security cameras can be used to hold someone accountable for potential vandalism or destruction, or even catch someone using the machines in a malicious way.

Step 7: RECOMMEND ADDITIONAL SECURITY CONTROLS

1. Security controls that should be implemented (if they aren't already) are locking the lab room at night, and locking the building outside. Only certain people should have access to keys. An additional security measure could be making it so the lab must be swiped into using a Mizzou student or staff/faculty ID. The machines should also be shut down at night, with the security cameras left on obviously. More inexpensive security could potentially be motion sensor lighting in the lab and outside the building.