Simplified Risk Assessment of the AT&T Lab

Assignment Due Date: 1/27/16

While risk assessment may not be the most exciting area of cyber security in the eyes of many, it is without a doubt one of the most critical steps in ensuring that an organization's assets are properly safeguarded from the threats they face. Complete the tasks below and answer the questions that follow. Record your responses using your preferred document editing software. When you're finished, convert the document into a PDF file and submit it via Blackboard for grading in the "Assignments" section.

STEP 1: CONTEXT

For what type of organization are we performing this risk assessment? (See slide 18 from the lecture slides if you're not sure)

What are some possible legal regulations that need to be adhered to? (Consider the shared use of computing equipment)

How much risk do you think the MU IT Program is willing to accept in this lab? Justify your answer.

STEP 2: ASSET IDENTIFICATION

Take a look around the room; what assets are we most concerned about protecting?

Can you think of any other, less obvious assets that may be at risk? If so, why do you think these should be considered assets in need of protection?

STEP 3: THREAT IDENTIFICATION

What are some threats that face these assets? You don't need to come up with an exhaustive list, but you should be able to come up with at least two potential threats for each identified asset. Be sure to include the source of the threats you list.

STEP 4: VULNERABILITY IDENTIFICATION

What are some of the vulnerabilities that our assets exhibit? Could the asset in question perform its intended function if the source of the vulnerability were removed?

STEP 5: RISK ANALYSIS

For each identified threat that can be used to exploit an identified vulnerability, determine the likelihood that such an attack will occur. (Note: use your best judgement here, and justify your answers)

STEP 6: ANALYZE EXISTING CONTROLS

What are some of the existing security controls used in the AT&T lab? Do you think they are effective at reducing the amount of risk posed by the threat(s) they intended to defend against? Why or why not?

STEP 7: RECOMMEND ADDITIONAL SECURITY CONTROLS

Are there any additional security controls that you think should be deployed in the lab? Why or why not? (Note: use common sense here… sure, hiring someone to physically guard the lab after regular business hours would theoretically increase the lab's level of security, but the cost would greatly outweigh the benefit.)