CYBR3600
Homework 2: Decision Trees and Strategic Thinking

Problem
Imagine that you work under the chief information security officer (CISO) for First Fictional Bank of Omaha. Your boss tells you about two threats to the authentication system for the bank's online financial management app (app that lets users move money between accounts and track transactions on their statements).

The first threat is that the "forgot password" functionality requires users to enter their username, date of birth, and place of birth. Once entered, the function displays the password for the user's account on the screen.

After speaking with your risk management team, they predict that there is about a 50% chance this will account for major revenue loss (of 100k /year), a 40% chance this will account for small revenue loss (20k/year), and a 10% chance that it will account for negligible revenue loss (0k/year).

The risk team has spoken with development. They state that it can be patched to require additional information and require email confirmation before displaying the password. The patch will cost somewhere between 5k and 20k. Based on previous development they expect there is a 30% chance it will cost 20k, 50%chance it will cost 10k, and 20% chance it will be on budget at 5k.

The second threat is that the authentication system is vulnerable to authenticated CSRF (Cross site request forgery). This means that if a user is authenticated and makes a change to their account, the financial app does not validate that the request came from itself. Hence, malicious sites can potentially exploit session tokens and forge requests to transfer user monies to other accounts.

You speak again with the risk team and they tell you that there is a low chance (5%) this will be exploited each year, but that it could have high impacts of around $1,000,000. If it doesn't occur, there is no cost.

The risk team thinks this particular vulnerability could be patched by development for somewhere between 50 and 100k. The cost is so high because the system is legacy and not well maintained. They place the odds at 50% that it will cost 100k and 50% that it will cost 50k.

Addressing both:
Since there are multiple issues with the system, you discussed a replacement with a third party vendor and they assure you that it can be replaced at a cost of 90k and it will eliminate both threats.

Tasks
Given the scenario make a decision assuming a **neutral risk attitude** (expected least cost) for optimal cost allocation. Do you a) replace the system, b) patch both risks c) patch risk one, but not risk two, d) patch risk two but not risk one, or e) accept both risks. Support your answer by creating and drawing a decision tree that covers the 5 strategic options available to you (i.e. a-e above). **Hint:** All 5 options should stem from a single choice node and the tree should have up to 3 layers. Show all computations for expected value and show the final value of each option.

Would you make the same choice with a pessimistic attitude? Explain using your tree, making different selections based on the differing risk perspective.