Multiple Choice Question

The following will be a suggestion for a multiple choice question (MCQ) for the course *Data Security (02239)* at DTU. It will consist of:

- Topic of the question including relevant theory
- Presentation of the question, with possible answers.
- Discussion of answers (both correct answer and distractors)
- Discussion of the cognitive level of the question and course-specific learning objective

Topic

The topic of the proposed MCQ here is data security management, specifically security planning. In the textbook[1] security planning is about making a good security plan. The description of a security plan in the book dictates that it must contain:

- Policy
- Current state
- Requirements
- Recommended controls
- Accountability
- Timetable
- Maintenance

Notice that a security plan is much more extensive than a security policy. The security policy is meant to document the needs and priorities of an enterprise. It is in the policy it is states who should be allowed access to what and how users are supposed to operate within the system. The "current state" is meant to describe the current state of the enforced security. The requirements are a discussion of *what* should be accomplished security-wise, not *how*. Recommended controls are the discussion of *how* to meet the specified security requirements. Accountability defines *who* is accountable, i.e., in charge, for implementations of the *hows* defined in the recommended controls. The timetable is the time plan for *when* to put things into action. Finally, the maintenance should answer when to revise the security plan.

These are all formal requirements for a security plan, however, the textbook fails to address an important issue, at least to some degree. Namely that any security plan hinges on the user-willingness to follow the plan. It can be argued that willingness to follow the plan is somewhat discussed in the security policy, but there is no point on this checklist that addresses collaboration with the users. In the very first lecture given in the course, it was mentioned that currently, the most significant vulnerability to most systems is the users themselves. In the lecture about security management, it was stressed that a security plan the users do not know about and/or understand will most likely not be followed. A security plan that is not followed has zero effect, no matter how good it is on paper.

To underline this fact, we were presented with a statistic in the lecture:

[1] Security in computing, 5th edition

"91% of all cyber attacks begin with a phishing email to an unexpected victim."
According to Deloitte.
Therefore, this simple requirement is the most important in the security plan: The people involved need to understand *why* the security plan is important and what its purpose of it is.

The Question

What makes a good enterprise security plan? Please select the best answer.

A) *A security plan made in collaboration with the relevant users.*

B) *A security plan where it is clear who is responsible for what.*

C) *A security plan that renders malicious usage infeasible.*

D) *A security plan that ensures the worst case scenario is survivable.*

E) *A security plan where the risk of incidents is minimized.*

Discussion of answers

A) A security plan made in collaboration with the relevant users. Correct

Why do I believe this answer is the best one? I do so because of two reasons:
Firstly, the answer says *A security plan made [...]*. According to the definition of a security plan, the plan must contain the points stated in the *Topic* section. That is, all the formal requirements for a security plan should be satisfied. Additionally, and this is the important part, it says *made in collaboration with relevant users.* This means that the users have had an influence on how and the plan was made and/or participated in the thought process. Therefore, it is reasonable to expect these users to understand the *whys* behind the policy, requirements etc. This, in turn, makes it much more likely that the plan will actually be followed, and the system will be more secure.

B) A security plan where it is clear who is responsible for what. Wrong

Why do I believe this answer is plausible?
I believe this is a plausible answer (or at least sounds like it) because it seems very reasonable that a security plan should address who is responsible for what. In fact, according to the requirements of a security plan given in the book, this is one of the things that must be addressed. In other words, this answer is not entirely wrong, i.e., it is a necessary condition but not a sufficient one.

Why do I not believe this is the best answer?
I do not believe it is the best answer, because it fails to address the issue of ensuring that the users actually follow the plan. As previously mentioned, it does not matter how a plan is on paper if no one follows it.

C) A security plan that renders malicious usage infeasible. Wrong

Why do I believe this answer is plausible?
I believe this answer sounds feasible because, in the end, malicious usage is one of the things we generally want to prevent. Before I took this course, the first thing that came to mind when hearing the words "data security" was things like hacking, phishing, and spoofing. In general, things where some bad guy tries to do something malicious. However, after this course, it should be clear that data

security is not just about protecting yourself from some bad guy that wants to hurt you. Additionally, the verbatim *infeasible* reminds somewhat of verbatim used when talking about encryption protocols, and therefore might seem familiar.

Why do I not believe this is the best answer?
I do not believe this is the best answer because of two things. Firstly, the purpose of a security plan is not necessary to render all malicious usage infeasible. This would potentially be almost impossible and require much more effort than the risks justify. Of course, there might be some functionalities, e.g., access to the main database, where malicious usage should be infeasible, but often there is no need for such extreme lengths for everything. Secondly, this answer also fails to address the issue of getting the users to follow the instructions. You can only imagine that with a security plan where ANY malicious usage should be infeasible, using the system will most likely be cumbersome for the users, and the likelihood of them not following the instructions is high.

D) A security plan that ensures the worst-case scenario is survivable. Wrong

Why do I believe this answer is plausible?
I believe this answer is plausible since is resembles some parts of the content of a security plan. A normal security plan must contain some risk analysis that answers how likely some scenarios are and how severe their impact will be. This is used to determine the maximal security efforts. Generally speaking, the worst-case scenario should be survivable for an enterprise. However, it also depends on the risk of this scenario, and the effort required to prevent it.
Why do I not believe this is the best answer?
I do not believe this is the best answer for three reasons. Firstly, it does not address the probability of this worst-case scenario; it may be extremely low. Secondly, it does not address the efforts needed to prevent the worst-case scenario. Image the worst-case scenario is being hacked by the NSA. This is very unlikely but also very hard to prevent. Maybe it is not necessary for most enterprises to consider this. Finally, the users involved are not addressed in this answer; just like the previous two.

E) A security plan where the risk of incidents is minimized. Wrong

Why do I believe this answer is plausible?
Generally speaking, the idea behind data security can be seen as minimizing some risks under some conditions. Naturally, we would like to minimize the risk of any incident. This is true for all data security, therefore this answer does seem somewhat plausible.
Why do I not believe this is the best answer? I do not believe this is the best answer because it fails to address the conditions of this minimization. Obviously, it would be nice to minimize all risks, however, there is some natural restrictions. It is not possible to use an infinite amount of money and effort of making a plan to minimize all risks. Additionally, such a plan might put high requirements on the users, which increases the likelihood of them not following the plan.

Level of question

This multiple choice question presented here requires the examinee to select the *best* answer amongst multiple more or less plausible answers. The correct answer does not contain any specific vertabium of clues that indicates this is the correct answer. Therefore, the examinee is required to compare the answers and justify which is *best.* Bloom's taxonomy of knowledge suggests that the question ranks as a level 5 (evaluating) of knowledge.
One of the learning objectives of the course is: *Identify all major factors that have to be addressed in a security analysis of a particular system.* A natural approach to identifying all major factors to address

is to make a security plan. Therefore the security plan was the first part of lecture 11 (data security management). Therefore, a question that requires the examinee to have an understanding of security plans and their limitation falls within the aforementioned learning objective.