Solution Guide: Security Culture Framework - Part 1

In this exercise, you played the role of a security consultant contracted to help a local bank develop a plan to address a physical security issue that recently resulted in the breach of its financial data servers.

Answers to the questions will vary, but below are some examples of correct answers.

- 1. Explain the security risks that this behavior introduces.
 - This behavior is insecure because it enables non-employees to get into the building without providing identification.

- 2. Describe a method for finding out how many people encourage tailgating, and keeping track of those who do.
 - One method involves simply counting how many employees engage in this behavior.
 - The organization should have the security team audit surveillance feeds to determine what percentage of employees entering secure buildings hold the door for people behind them.
 - They can also keep track of which employees let others in. This number is the average tailgating rate, which can be calculated for each secure building the company manages.
- 3. Set a goal for how many employees *should* engage in this behavior.
 - Ideally, no employees entering secure buildings will allow unauthorized people in. The target should be 0% of employees engaging in tailgating.
 - 1. Identify three potential high-level solutions to this problem, such as training or hiring guards. Note one advantage and disadvantage for each.
 - Develop and deliver a training. The advantage is that this training might have a
 lasting effect on the company's security. The disadvantage is that it takes a long
 time to develop and execute.

- Hire guards for all hours. The advantage is that this provides a direct solution to the problem. The disadvantage is that it raises costs, and doesn't change how employees think about the problem.
- Require keycards for access. This is the most secure option, because it
 restricts access to only those who have been explicitly allowed to enter. The
 disadvantage is that it takes a lot of work to implement.
- 4. Set an estimated timeline for each potential solution.
 - The company has over 500 employees. Training all of them will probably take a full year.
 - Hiring and assigning guards would be faster. This only takes as long as getting the budget approved and hiring the security personnel. At most, this should take one quarter (three months).
 - Developing and implementing key card access would require at least a year, as it requires physical changes to the organization's properties and distributing ID cards.

Bonus

We'll cover these topics in more depth later. For now, consider these sample responses a starting point:

- What C-level officer titles do you know? Which do you think this company has?
 - Most companies relevant to this course have a Chief Executive Officer (CEO), Chief Operating Officer (COO), Chief Finance Officer (CFO), and Chief Information Security Officer (CISO).
 - What security functions/responsibilities does a Security department have?
 - The Security department is responsible for protecting the CIA of the organization's data.
 - Which teams within the department would fulfill these responsibilities?
 - Most security teams have at least Incident Response and Networking teams.
 Companies that build their own applications usually have an Application Security team as well.

© 2020 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.