Southern New Hampshire University

IT 380 Module Two Case Study Analysis Guidelines and Rubric

Overview: This case study will help you analyze a cybersecurity scenario and identify which tenets were violated. Each skill in this paper is an essential part of the final project and the accompanying milestones in this course.

Prompt: Use the information provided in the scenario to analyze the cybersecurity occurrence and determine which tenet(s) were violated.

The required resources for this module detail a scenario at RSA that is similar to the one you will analyze for this assignment. Review each module resource and analyze the security breach that occurred with RSA. Note similarities between this example and the provided scenario for this assignment.

Scenario: In late May of 2011, Lockheed-Martin was targeted by a cyberattack. Lockheed-Martin claimed that they discovered the attack early and reacted quickly, with the result that no real harm was done.

The basis for this breach was with two-factor authentication, where a "factor" in authentication can be something you know, something your are, or something you have. A two-factor authentication system requires you to present instances of two of these three to authenticate with a system. Lockheed-Martin employed a two-factor authentication system that combined a password (something you know) with SecurID, a system produced by RSA labs that provides the "something you have" factor.

A SecurID is a small key fob that displays a number, which changes every 60 seconds. Each key fob has a unique number called its seed, which determines what number is shown in the fob at any given point in time. The server stores your username, password hash, and the seed value for your key fob, and this allows it to determine what number is showing on your key fob (as the fob is synched with your account). When you authenticate, you enter your username and regular password, then you look at the key fob and enter in the number shown there. The authentication server knows what number should be shown at that time on the key fob, and so can verify that the key fob is indeed a thing you have. This is called a one-time password (OTP) system.

In March of 2011, someone attacked RSA with a relatively unsophisticated phishing attack with an attached Excel file with embedded code that exploited a zero-day vulnerability in Adobe Flash.

This enabled attackers to set up a "backdoor"—a way for them to get into the computer—where the attackers were able to steal from RSA the seed values of SecurID key fobs.

In late May of 2011, the attack moved to Lockheed-Martin, where attackers managed to get a keylogger onto a company system. The keylogger recorded the username, password, and SecurID OTPs used by the victim when he or she authenticated, along with the date and time of the log in.

Two-factor authentication is designed for just this kind of scenario. The attacker cannot authenticate because knowing the username, password, and an old OTP is not enough; the current OTP is required. However, these attackers stole seed values. For a given seed value and date/time, they could calculate the number the key fob with that seed value would display at that date and time. All the attackers had to do was to write a program that would compute, for every stolen seed value, the number that would have been showing at the date and time the keylogger recorded the victim's login. Once they found a match with the OTP the keylogger recorded, they would have matched a seed value with a username. This appeared as if the attackers actually had the key fobs themselves.

Southern New Hampshire University

Critical Elements
Your paper should include these critical elements:

- Identification of cybersecurity tenets that were violated and rationale of cause
- Analysis of cybersecurity occurrence and data defense
- Recommendation of best practices to prevent further recurrence

Rubric

Guidelines for Submission: Your paper should be submitted as a 2- to 3-page Microsoft Word document with double spacing, 12-point Times New Roman font, and one-inch margins. All sources must be cited in APA format if used.

Instructor Feedback: This activity uses an integrated rubric in Blackboard. Students can view instructor feedback in the Grade Center. For more information, review these instructions.

Critical Elements	Exemplary (100%)	Proficient (90%)	Needs Improvement (70%)	Not Evident (0%)	Value
Identification of Violated Cybersecurity Tenets	Meets "Proficient" criteria and correctly identifies which tenets were violated with empirical supporting examples	Correctly identifies which tenets were violated with supporting examples	Identifies which tenets were violated but supporting examples have gaps	Does not identify a single tenet	30
Analysis of Data Defense	Meets "Proficient" criteria and analysis demonstrates keen insight of data defense and prevention methods	Analysis demonstrates accurate knowledge of data defense and prevention methods	Analysis demonstrates knowledge of data defense methods but needs additional information to support prevention ideas	Does not analyze the data defense and prevention methods	30
Best Practices Recommendation	Meets "Proficient" criteria and recommendation demonstrates understanding of industry best practices that would remedy the situation appropriately	Recommends industry best practices to ensure proper resolution of scenario	Recommends a single best practice to remedy situation but recommendation has gaps in strategic implementation	Does not recommend any industry best practices	30
Proper Use of Writing, Mechanics, and Grammar	Paper is free of errors in organization and grammar with applicable sources cited	Paper is mostly free of errors of organization and grammar; errors are marginal and rarely interrupt the flow; applicable sources cited	Paper contains errors of organization and grammar but errors are limited enough so that entries can be understood; applicable sources cited	Paper contains errors of organization and grammar making the content difficult to understand	10
				Total	**100%**