GRP1 — GRP1 TASK 2: WLAN AND MOBILE SECURITY PLAN

EMERGING TECHNOLOGIES IN CYBERSECURITY — C844
PRFA — GRP1

TASK OVERVIEW | SUBMISSIONS | EVALUATION REPORT

COMPETENCIES

4042.5.1 : Cellular and Mobile Technologies
The graduate determines how to address vulnerabilities and threats in cellular and mobile network technologies.

4042.5.2 : Wireless Technologies
The graduate determines how to address vulnerabilities and threats in wireless architectures.

INTRODUCTION

As wireless and mobile technologies continue to grow in presence and popularity, the world is becoming more and more connected. Unfortunately, this also means that devices and networks are becoming more and more vulnerable to outside threats. Businesses must identify and mitigate these vulnerabilities and threats in order to protect employees' personal information and ensure the organization is secure from passive leaking of proprietary information.

In this task you will assume the role of an IT professional who is responsible for identifying wireless and mobile vulnerabilities, as outlined in the scenario below. You will then present your findings and recommend solutions to mitigate these risks and prevent future threats.

SCENARIO

You are a network professional on the IT team at Alliah Company, a new but fast-growing social media provider. One year ago, Alliah launched a social media website aimed at young professionals. The company also released a mobile app for accessing the site from cellular devices. Alliah was able to launch its website with money generated by a crowd-funded campaign, but most of the funds were spent on the site and app development, with relatively little money (and time) devoted to the internal office network infrastructure.

Alliah has 35 full-time employees, all of whom have offices or shared work spaces in a three-story building that serves as the company headquarters. The building is an old warehouse that was converted for office use and is approximately 10,000 square feet. Currently, the employees occupy only two floors; the third floor is vacant and available for expansion.

The Alliah WLAN has a gigabit managed switch, a multiservice wireless LAN controller, and seven wireless access points strategically located to provide coverage to office staff. One access point services a large back patio area for employee use. The network is protected by a firewall. The Alliah website servers are located in a data center 100 miles from Alliah headquarters.

Five employees are account representatives who are on the road at least 80 percent of the time, and each rep has a company-issued laptop, tablet, and smartphone. They use a large, shared office in the headquarters building when they are not traveling.

Employees use company-owned computers that connect to the WLAN, and, in an effort to control costs during the launch, Alliah has a bring your own device (BYOD) policy.

The IT staff consists of five employees; three are devoted to website maintenance, one manages the headquarters' computers and network, and another employee assists with the website and the office network. IT staff uses wired Ethernet connections to remotely access the website servers.

The Alliah website is successful, attracting more and more visitors each month. Jennifer, the CEO, anticipates hiring more employees and is considering a strategy that would take the company public within a few years. In preparation, she wants to ensure that Alliah's wireless networking infrastructure is highly secure, especially because it may need to grow quickly in a short period of time, and she wants to understand the security risks the company faces. She also wants to decide if Alliah should continue allowing BYOD or restrict network access to company-owned devices only, or if a compromise solution is available.

REQUIREMENTS

Your submission must be your original work. No more than a combined total of 30% of the submission and no more than a 10% match to any one individual source can be directly quoted or closely paraphrased from sources, even if cited correctly. An originality report is provided when you submit your task that can be used as a guide.

You must use the rubric to direct the creation of your submission because it provides detailed criteria that will be used to evaluate your work. Each requirement below may be evaluated by more than one rubric aspect. The rubric aspect titles may contain hyperlinks to relevant portions of the course.

A. Describe **two** WLAN vulnerabilities that present risks for Alliah, based on the details in the scenario.

B. Describe **two** mobile vulnerabilities that present risks for Alliah, based on the details in the scenario.

C. Summarize the steps for mitigating *each* identified WLAN and mobile vulnerability, including the specific tools or documentation that will be needed for mitigation.

D. Recommend preventive measures to maintain the security posture of WLAN and mobile environments in a small business, such as Alliah. Reference federal, state, or industry regulations that justify these measures.

E. Recommend a solution for the company's BYOD approach, including research to justify your recommendation.

F. Acknowledge sources, using in-text citations and references, for content that is quoted, paraphrased, or summarized.

G. Demonstrate professional communication in the content and presentation of your submission.

File Restrictions

File name may contain only letters, numbers, spaces, and these symbols: ! - _ . * ' ( )
File size limit: 400 MB
File types allowed: doc, docx, rtf, xls, xlsx, ppt, pptx, odt, pdf, txt, qt, mov, mpg, avi, mp3, wav, mp4, wma, flv, asf, mpeg, wmv, m4v, svg, tif, tiff, jpeg, jpg, gif, png, zip, rar, tar, 7z

RUBRIC

A:WLAN VULNERABILITIES

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
The submission does not describe two WLAN vulnerabilities that present risks for Alliah.	The submission describes two WLAN vulnerabilities, but the vulnerabilities are not plausible based on the details of the scenario.	The submission describes two plausible WLAN vulnerabilities that present risks for Alliah, based on the details of the scenario.

B:MOBILE VULNERABILITIES

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
The submission does not describe two mobile vulnerabilities that	The submission describes two mobile vulnerabilities, but the vulnerabilities	The submission describes two plausible mobile vulnerabilities that present risks

present risks for Alliah.	are not plausible based on the details of the scenario.	for Alliah, based on the details of the scenario.

C:STEPS TO MITIGATE VULNERABILITIES

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
The submission does not summarize steps for each identified vulnerability.	The submission summarizes steps for each identified vulnerability, but these steps would not mitigate each identified vulnerability. Or the submission does not include the specific tools and documentation that will be needed for mitigation.	The submission summarizes the steps that should be taken to mitigate each identified vulnerability and includes the specific tools and documentation that will be needed for mitigation.

D:PREVENTIVE MEASURES

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
The submission does not recommend preventive measures to maintain the security posture of WLAN and mobile environments in small businesses.	The submission recommends preventive measures, but these measures would not maintain the security posture of WLAN and mobile environments in small businesses. Or the submission does not reference federal, state, or industry regulations that justify these measures.	The submission recommends preventive measures that will maintain the security posture of WLAN and mobile environments in small businesses, referencing federal, state, or industry regulations that justify these measures.

E:BYOD APPROACH

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
The submission does not recommend a solution for the company's BYOD approach.	The submission recommends a solution for the company's BYOD approach, but the solution is not secure or does not include reliable, academic, or industry-respected research to justify the recommendation.	The submission recommends a secure solution for the company's BYOD approach and includes reliable, academic, or industry-respected research to justify the recommendation.

F: SOURCES

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
The submission does not include both in-text citations and a reference list for sources that are quoted, paraphrased, or summarized.	The submission includes in-text citations for sources that are quoted, paraphrased, or summarized and a reference list; however, the citations or reference list is incomplete or inaccurate.	The submission includes in-text citations for sources that are properly quoted, paraphrased, or summarized and a reference list that accurately identifies the author, date, title, and source location as available.

G: PROFESSIONAL COMMUNICATION

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
Content is unstructured, is disjointed, or contains pervasive errors in mechan-	Content is poorly organized, is difficult to follow, or contains errors in mechan-	Content reflects attention to detail, is organized, and focuses on the main ideas

ics, usage, or grammar. Vocabulary or tone is unprofessional or distracts from the topic.	ics, usage, or grammar that cause confusion. Terminology is misused or ineffective.	as prescribed in the task or chosen by the candidate. Terminology is pertinent, is used correctly, and effectively conveys the intended meaning. Mechanics, usage, and grammar promote accurate interpretation and understanding.