

SUBDOMAIN 427.3 - SECURITY POLICY & STANDARDS

Competency 427.3.2: Controls and Countermeasures - *The graduate evaluates security threats and identifies and applies security controls based on analyses and industry standards and best practices.*

Scenario:

A small LLP consisting of a group of private investigators is headed by one of your friends. The partnership has a small office with one server and six workstations. Additionally, the partnership hosts its own website where it allows clients to log in and enter their case information. You suspect that the site may be lacking fundamental security and information safeguards.

During the past few weeks, staff members have noticed that the workstations are running sluggishly, and they routinely get advertisements on their computers when they are not on the Internet. Investigators routinely download and install programs and plug-ins from the Internet. However, the computers are not kept up-to-date with operating system patches or software patches for other installed software programs and plug-ins.

Lastly, there have been several complaints from clients that the company website has been unavailable or has timed out. Recently, the website was completely deleted and the homepage read, "You've been hacked." Fortunately, the website was able to be restored from a backup.

You have been asked by your friend to assist the group with its various security challenges by analyzing the threats the LLP faces.

Task:

- A. Outline the top **five** threats to *each* of the following in the given scenario:
 1. The server
 2. The workstations
 3. The website
- B. Create a memo (*suggested length of 2 pages*) in which you do the following:
 1. Evaluate the likelihood of the threats discussed in part A.
 2. Recommend security controls and countermeasures that should be instituted to mitigate these threats.
- C. When you use sources, include all in-text citations and references in APA format.

Note: When bulleted points are present in the task prompt, the level of detail or support called for in the rubric refers to those bulleted points.

Note: For definitions of terms commonly used in the rubric, see the Rubric Terms web link included in the Evaluation Procedures section.

Note: When using sources to support ideas and elements in a paper or project, the submission MUST include APA formatted in-text citations with a corresponding reference list for any direct quotes or paraphrasing. It is not necessary to list sources that were consulted if they have not been quoted or

paraphrased in the text of the paper or project.

Note: No more than a combined total of 30% of a submission can be directly quoted or closely paraphrased from sources, even if cited correctly. For tips on using APA style, please refer to the APA Handout web link included in the General Instructions section.