**Overview**

This phase of the project completes the design phase and develops a business continuity and disaster recovery plan for the final solution. This phase of the project must include the secured design diagrams that minimize risk and appropriately address the threats identified in **Project 1: Problem Identification Assignment**. **Threats from “distributed denial of service attacks” -**include semantic attacks and brute force attacks. And also Man in the middle attack from include semantic attacks and brute force attacks.

Any single points of failure must be addressed with appropriate fault-tolerant designs. Solutions must parallel the analyzed solutions. For example, if vulnerability was determined between 2 network gateways, a solution could include a virtual private network (VPN) with appropriate public key infrastructure (PKI) and certificates. If a man-in-the-middle network attack is a threat, Dynamic ARP Inspection and DHCP Snooping features on networking equipment can be indicated in the network design diagram to prevent these attacks.

**Instructions**

Each design must be justified by the textbook and peer-reviewed research. You will be evaluated based upon the appropriate security solutions to the identified problem. The final design must seek to construct the appropriate controls for the target given various, regularly used vulnerabilities. For example, if the target is availability and the vulnerability is connection flooding (e.g. SYN flood), appropriately designed solutions would likely include the minimum controls of an intrusion detection system (IDS), firewall, access control list (ACL) on the border gateway/router, and a honeypot to counteract unauthorized attempts. A design diagram must properly illustrate this secured solution, and the author must subsequently explain each dimension of the security strategy.

Current and proper APA formatting is required and must include a title page, proper margins, citations, organization, proper grammar and spelling, and an ending resources page.

At the minimum, this phase of the project must include:

I. Executive summary and introduction

II. Systems Design

**a.** Detail the final systems design, supporting the results given the original review of the literature and the analysis performed in **Project 2: Methodology Development Analysis Assignment**

b. Design the final solution

i. Target of the attack

ii. Vulnerability

iii. Control

c. Create the appropriate design diagrams for the secured solution

d. NOTE: Required minimum length **(8 peer-reviewed sources** and at least 10 double-spaced, current APA-formatted pages) in the grading rubric **excludes all** systems analysis and design (SAD) diagrams and any other tables and/or graphical elements

III. Business continuity and disaster recovery plan (must be supported by relevant and current research from scholarly, peer-reviewed journals)

a. Basic BCP Policy

b. Basic business impact analysis (BIA)

c. Preventative measures

d. Recovery and restoration

IV. Project conclusion

a. Summary of the solution

b. Future recommendations and implications for business

c. Final project conclusion

V. **Diagram examples** in this phase could include but are not limited to:

a. Secured and hardened advanced system and/or network architecture diagrams

b. Secured package, design class, system security, and system control diagrams

c. Secured CPU/Memory/OS buffer, segmenting, address, and/or data bus mappings

d. NOTE: **A minimum of 5 diagrams** exist that accurately analyze a secure system, network, and/or application solution. Within EACH of the 5 diagrams, a minimum of 10 elements exist that accurately detail analysis of the environment that needs securing (Note, if 10 elements are not necessary in a diagram, add diagrams as needed to sufficiently meet this requirement). Each diagram is thoroughly developed based upon existing architecture and/or applications. Each diagram meets the associated technical requirements, programming language, notations, formatting, and modeling rules of the language (e.g. UML), industry standards for the diagram, and/or literature review. Analysis and design diagrams must have an associated industry standard that is widely accepted to be recognized (e.g. UML).

Note: Your assignment will be checked for originality via the Turnitin plagiarism tool.