Assignment 2: Identifying Potential Risk, Response, and Recovery

Due Week 8 and worth 75 points

In Assignment 1, a videogame development company recently hired you as an Information Security Engineer. After viewing a growing number of reports detailing malicious activity, the CIO requested that you draft a report in which you identify potential malicious attacks and threats specific to your organization. She asked you to include a brief explanation of each item and the potential impact it could have on the organization.

After reviewing your report, the CIO requests that you develop a follow-up plan detailing a strategy for addressing all risks (i.e., risk mitigation, risk assignment, risk acceptance, or risk avoidance) identified in Assignment 1. Further, your plan should identify controls (i.e., administrative, preventative, detective, and corrective) that the company will use to mitigate each risk previously identified.

Write a four to five (4-5) page paper in which you:

1. For each of the three (3) or more malicious attacks and / or threats that you identified in Assignment 1, choose a strategy for addressing the associated risk (i.e., risk mitigation, risk assignment, risk acceptance, or risk avoidance). Explain your rationale.
2. For each of the three (3) or more malicious attacks and / or threats identified in Assignment 1, develop potential controls (i.e., administrative, preventative, detective, and corrective) that the company could use to mitigate each associated risk.
3. Explain in detail why you believe the risk management, control identification, and selection processes are so important, specifically in this organization.
4. Draft a one (1) page Executive Summary that details your strategies and recommendations to the CIO (Note: The Executive Summary is included in the assignment’s length requirements).
5. Use at least three (3) quality resources in this assignment (no more than 2-3 years old) from material outside the textbook. Note: Wikipedia and similar Websites do not qualify as quality resources.

Your assignment must follow these formatting requirements:

* Be typed, double spaced, using Times New Roman font (size 12), with one-inch margins on all sides; references must follow APA or school-specific format. Check with your professor for any additional instructions.
* Include a cover page containing the title of the assignment, the student’s name, the professor’s name, the course title, and the date. The cover page and the reference page are not included in the required page length.

The specific course learning outcomes associated with this assignment are:

* Explain the concepts of information systems security as applied to an IT infrastructure.
* Describe the principles of risk management, common response techniques, and issues related to recovery of IT systems.
* Describe how malicious attacks, threats, and vulnerabilities impact an IT infrastructure.
* Explain the means attackers use to compromise systems and networks, and defenses used by organizations.
* Use technology and information resources to research issues in information systems security.
* Write clearly and concisely about network security topics using proper writing mechanics and technical style conventions.

Grading for this assignment will be based on answer quality, logic / organization of the paper, and language and writing skills. Click here to access the rubric for this assignmen