Unit 6 Assignment

Scenario

You are a Cyber Security Threat Analyst for a consulting company that does work for both the pubic and private sectors. You have been assigned a new project and it is to help to develop a process or framework for a mid-sized (200 employees) software company. The software company develops a commercially available web-based system with an accompanying mobile application (Android and iOS) for the financial sector. The company's yearly revenue is approximately $15 million. The Director of Research and Development is concerned about their application development and the development operations (DevOps) activities in regards to insider threats. The software company frequently uses contractors (on-site and remote) and some of the contractors are from foreign countries. The contractors help develop and test their software product and are also used for in-house software development and maintenance. There is only one Research and Development (R&D) facility for the company. Your project is use to create and action plan/framework to help mitigate cyber risks due to development operations, application development, and insider threats. Realizing insider threats are a concern, it is also your job to ease the Director of Research and Development's mind in regards to continuing to use contractors and those of which are from foreign countries. He is a fact driven decision maker and would benefit from facts regarding how multiculturalism and diversity could benefit his company and not harm it.

Consider the following in your action plan:

- How you will convince the director you can effectively address any potential issues related to multiculturalism and diversity
- How you will utilize problem-solving skills and conflict resolution to bridge cultural differences
- How you will address change that occurs due to the presence of multiculturalism and diversity in a business environment

Background about the NIST Cybersecurity Framework:

President Obama issued Executive Order 13636, Improving Critical Infrastructure Cybersecurity, in February 2013. The order directed NIST to work with various stakeholders to develop a voluntary framework based on existing standards, best practices and guidelines with the intent of reducing cyber risks to critical infrastructures. NIST released the first version on February 12, 2014. The NIST Cybersecurity framework is available in three formats one of which is a database driven tool that is compatible with later versions of Microsoft Windows and MAC's OS 10. More information about the Cybersecurity Framework can be found on the NIST web site (www.nist.gov).

In addition to creating and maintaining a web-based financial system and mobile application to accompany it, the company uses several enterprise-based systems for day-to-day operations. They have an email system, customer relationship management system, source code control system, a bug tracking system, and technical support tracking system. The technical support tracking system is an in-house developed system and considered a legacy system. The company is researching various technical support systems to replace the legacy system. The other enterprise systems were purchased/leased from various vendors. The customer

relationship management system is cloud based and an Oracle product. The other systems reside on-premise and are in a harden data center located 10 miles from the R&D facility and it has successfully gone through a SSAE 16 audit.

The company has a business continuity plan however the disaster recovery plan needs to be improved as the company does not have a hot backup site. They do backup all critical systems several times per day. The backup data is automatically streamed to another harden data center (also SSAE 16 certified) that is located 25 miles away. All of the systems at the data center are considered critical systems. In addition, the system test and software quality assurance departments have all the necessary software and hardware (mobile/tablets included) to sufficiently maintain high quality assurance. This test infrastructure is located at the R&D facility and not in the data center.

Instructions:

In this assignment you will analyze the NIST Cybersecurity framework. You will determine if it can be used as a guide to produce an action plan/framework for the company to use in an effort to reduce the likelihood of insecure application development and insider threats. If it cannot be used/mapped to the software company then what framework or method is better suited for the software company? Will you use various frameworks/guides and result in a hybrid approach? You have to produce an action plan/framework so it is important for you to do as much research as possible on other types of solutions.

It is very important for you to consider that the cybersecurity landscape includes cyber criminals that use the latest technological tools and technologies to cause harm. The action plan/framework that you create should be agile enough so it can adapt to changing risk environments over time. Finally, as you formulate your plan, costs will have to be justified in time so consider the revenue of the company and an industry standard percentage spent on cyber security budgets.

Your action plan should be at least 5–6 pages of content (exclusive of cover sheet etc.), using Times New Roman font style, 12pt, double-spaced, using correct APA formatting, and include a cover sheet, table of contents, abstract, and reference page(s). If applicable, be sure to document your content with proper APA in text citations that match your reference list. You can have more than one table and more than one figure however they must be fully explained.

You must support your research and assertions with at least 5 credible sources. You may use peer-reviewed articles, trade magazine articles or IT research company (Gartner, Forrester, etc.) reports to support your research; you can use the Kaplan University library to search for supporting articles and for peer-reviewed articles. Wikipedia and sources like it are unacceptable.

In accordance with the Kaplan University Academic Integrity policy, your assignment will be automatically submitted to TurnItIn (see: http://turnitin.com/en_us/features/originalitycheck). KU policy states that papers submitted for credit in any Kaplan course should contain less than 25% “non-original” material, so avoid large sections of direct quotes and be sure that you use APA formatting to properly cite and reference all non-original material.

Assignment Requirements:

- At least 5–6 pages of content (exclusive of cover sheet etc.), using Times New Roman font style, 12pt, double-spaced, using correct APA formatting, and include a cover sheet, table of contents, abstract, and reference page(s).
- No spelling errors.
- No grammar errors.
- No APA errors.

For more information and example of APA formatting, see the resources in Doc sharing or visit the KU Writing Center from the KU Homepage.

Also review the KU Policy on Plagiarism. If you have any questions, please contact your professor.

Assignment Grading Rubric = 115 points

Assignment Requirements	Points Possible	Points Earned
1. Described in sufficient detail any assumptions made prior to developing the action plan/framework for the software company.	**0-10**	
2. Described how the NIST Cybersecurity framework or another framework (or a hybrid) can be used in relationship to secure application development.	**0–25**	
3. Described how the NIST Cybersecurity or another framework (or a hybrid) can be used in relationship to development operations.	**0–25**	
4. Described how the NIST Cybersecurity framework or another framework (or a hybrid) can be used to manage employees and contract workers to help reduce insider threats. All three bulleted multiculturalism and diversity considerations were addressed.	**0–25**	
5. Justified an estimated budget amount put towards implementing the framework you propose.	**0-10**	
6. Grammar and spelling are error-free, and	**0–10**	

correct APA formatting is used throughout the paper. Paper has TurnItIn score of 25% or less for non-original material, and uses no more than 1 figure and/or table.		
7. At least 5–6 pages of content (exclusive of cover sheet etc.), using Times New Roman font style, 12pt, double-spaced, and includes a cover sheet, table of contents, abstract, and reference page(s).	**0–10**	
Column Total	**0–115**	
Points deducted for spelling, grammar, and/or APA errors.		
Adjusted total points