

Everyone's Smart University

Project (Spring 2021)

Student Name	Mohammed Naser Akram Alsati	اسم الطالب
Students I.D	2021200588	الرقم الجامعي

Section	Date	Course Code
Master of Project Management	Thursday 11 / 05 / 2021	(PMG506)

Advanced Project Management

Instructions:

- اخر موعد للتسليم هو يوم الخميس 2021-05-20 في تمام الساعة ٩ مساءً.
- الإجابة متاحة باللغة الإنجليزية أو اللغة العربية مع مراعاة أن تكون المصطلحات العلمية باللغة الانجليزية.
- يتم تسليم المشروع في صيغة ملف . pdf مع الالتزام نموذج الجامعة ولن تقبل أي مستندات أخرى.
- يجب مراعاة أقسام البحث الرئيسية (مقدمة Introduction، دراسات علمية سابقة Literature Review، طريقة البحث Methodology، النتائج والمناقشة Results and Discussion، وأخيراً المراجع References . وان كان هناك ملحقات Appendices يتم إضافتها)
- يجب الالتزام بـ Theme موحد كما يلي:
- حجم الخط 12.
- نوع الخط Arial.
- لون الخط أسود.
- المسافة بين الأسطر 1.5 line spacing
- عدد صفحات البحث (لا يقل عن ثلاث صفحات ولا يزيد عن ست صفحات).

Instructor's Name: ~~Eng. Amaal Aburumman~~ **Eng. Dr. Akram M. S. Ali**

Project:

You are required to document your role in administering a project. The project may be set in a business, social, sporting, or family environment but must be of a significant size and scale. If you do not have an actual project to write about you may complete the project hypothetically.

This report will be between three to six pages in length. This is a significant research project.

Your report must address ~~each~~ **ONE** of the following issues:

1. Identify and describe the purpose, scope, and objectives of the project. **Display this information using an appropriate tool.**
2. Describe how the team is given an outline of the project.
3. Describe the strategies that are going to be set up to maintain communication with the team members.
4. Describe the tools that are going to be used to monitor the goals, time frames or milestones.
5. Identify project milestones and activities. **Display this information using an appropriate tool.**
6. Create a budget and link the costs to the key milestones for a project.
7. Describe how you are going to divide tasks and resources amongst a project team. **Display this information using an appropriate tool.**
8. Briefly describe how the progress will be monitored.
9. How are current project records maintained? Who has responsibility for this? provide some recommendations on how this process could be improved.
10. Describe the current procedure for finalizing projects. Create your own procedure and identify how you will evaluate the success of the project.
11. Legislation that may affect the project including health and safety, and anti-discrimination legislation.

Best of luck...

The Answer:

Introduction:

The purpose of the following assignment is to focus on installation of cyber security systems in the workplace. A range of questions are answered in the assignment, like 'Why do companies conduct cyber security risk assessments? What do they find out from these assessments? Why should companies increase cyber security awareness among their employees? How can they do this? However, the most pressing issue is how the project records maintained? Who has responsibility for this, and how this process could be improved in future.

The Value of Cyber Security Risk Assessments:

Companies do conduct cyber security risk assessments to collect data on the cyber security framework of network. Also, companies gather information regarding security controls and weaknesses of it. Such the information could be affected from a cyber-attack. A cyber-security risk assessment scans the vulnerable area of information that may affect from cyber-attack. The key focus of the evaluation is the security plan of a company. Overall, a cyber-security risk assessment is a complex process of identification, analysis, and evaluation of critical data of a company. Indeed, the landscape of the threat is continuously changing, hence company executives need to consider further legal and moral aspects.

Need to Conduct Cyber Security Risk Assessments:

An organization gains maturity in integrated thinking regarding the information that creates value (Oyewo, Obigbemi and Uwuigbe, 2015, p. 65). However, the transformation to cyber security systems does not make overnight in the organization. Instead, the process does require an integrated information system to support

processes and activities. Nevertheless, technological change comes along with risks, like data privacy and security risks. Hence, security data protocols must be implemented to bring transparency in the project process and make the change successful at the corporate level. Rest on, the rapidly changing technological sector also creates a range of threats to the systems and processes like cyber hacking and so on.

From conducting cyber security risk assessment, companies find out those weak areas that would need to protect and may cost to the business, in the future. However, it is important to consider all aspects of security and not overlook any one to ensure changing nature of threat, legal and ethical implications. Thus, from cyber security risk assessment, companies cannot only recognize existing threats to information, but potential threats too. Indeed, the process of evaluation requires right combination of in-house people that are trusted to the topmost level. Rest on; cyber-attack could affect software, hardware, or entire system of a company.

[The Importance of Cyber Security Awareness:](#)

Companies should increase cyber security awareness among their employees because of the two main reasons, i.e. boost up confidence of employees, and reduce the increasing level of stress due to uncertain cyber security (Thakur, Hayajneh & Tseng, 2019, p. 45). A major reason is that around 69 percent employees consider feel stress due to data breach and leakage of personal and confidential information. Hence, the latest intelligence threat and cyber-attack tactics caused create stressful situation for employees, during their work.

It is widely accepted that social engineering is an art to deploy others to provide personal information. In an article by Aldawood & Skinner (2019), the authors stated that social engineers use psychological tactics to gain personal information of other people (p. 73). Any confidential or sensitive information must not share to any other person, particularly over the internet to maintain records (Thakur, Hayajneh & Tseng, 2019, p. 45). In the event that it would turn into a survivor of the cybercrime, one can

just fault to oneself since it didn't contact to security service software organization that can guarantee protection and security of personal data. Additionally, over those online discussions where workers used to talk, they should be mindful of those impersonators working among them. The entirety of that individual data ought to be discarded, securely, so it could never be recouped again by another person. The information each worker utilized over the web must be well encrypted. Everyone should keep their passwords private and not share with anybody.

Cyber Security Awareness Program:

Email security and representative training are the top difficulties looked by information technology (IT) security experts. In spite of firewalls and other security programming, workers are as yet the most widely recognized passage focuses for phishers (Aldawood & Skinner, 2019, p. 73). For an organization with more workers, similarly, the section focuses on increment and in like manner, it suggests an expansion in 'phish' in the ocean. Online cyber security training is to assist representatives with protecting themselves and the organization against digital assaults and dangers. It is widely believed that the cyber world is daily attracting a range of individuals to do legal or illegal acts. However, it depends on people not to share confidential data with anyone (Aldawood & Skinner, 2019). At least, the organizational workers should be highly careful not to share corporate details with any person, calling from any unofficial number.

Conclusion:

In conclusion, a cyber-security risk assessment scans the vulnerable area of information that may be affected from a cyber-attack. From conducting a cyber security risk assessment, the company identifies those weak areas that would need to be protected and may cost the business in the future. The company should increase cyber security awareness among their employees because of the two main reasons, i.e. boost up confidence of employees, and reduce the increasing level of stress due to uncertain cyber security. It

is important to check records daily and appropriately to avoid from uncertain circumstances.

References:

- Aldawood, H., & Skinner, G. (2019). Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. *Future Internet*, 11(3) 73.
- Thakur, K., Hayajneh, T., & Tseng, J. (2019). Cyber security in social media: challenges and the way forward. *IT Professional*, 21(2) 41-49.
- Oyewo, B., Obigbemi, I. & Uwuigbe, U. (2015). Should Integrated Reporting be incorporated in the Management Accounting Curriculum? *International Journal of Education and Research*, 3 (1) 63-76.