A close up of a logo

Description automatically generated  
  
  
**MIDTERM PROJECT IN IAS: CASE 5 AND 6**

**GROUP MEMBERS:**CUEVAS C. REYNALDO JR.

DEVENECIA, ROGIN JOHN

DE LEON, AJIRAY DEIGO

GUINOO, ASEL JOHN

HOCSON, BENEDICT ANGELO  
  
HUMOL, RAY IVERSON

MARQUESES, ALEXIS RAFAEL

**INSTRUCTION:**  
1.    Read and analyze each given case.  
  
2.    Answer the questions on the DISCUSS part.   
Justify your answers by citing some information relevant to the case/topic.  
  
3.    Specify the LESSONS LEARNED in the case study.   
(minimum of 2 paragraphs with 5 sentences each paragraph)  
  
4.    Use arial, 12, single spacing, long paper.

**CASE 5:**

DISCUSS:  
  
LESSON LEARNED:

**CASE 6:**   
  
  
  
 For Question 1, saying that which one Chatter’s cyber risks do I think should focus first? Well, according to the about the social media platform named “Chatter”, there are several potential cyber risks that would need immediate attention and consideration. However, among these risks there is one that should be given focus first, this concern is the fact that the email has not been read by all the staff members of the social platform. Not to mention, they have not undertaken any mandatory training. Because of this, future emails or alerts regarding potential cyber security risks could go unnoticed by untrained and uninformed staff employees, which could cause further damage to the social platform. This fact should be attended to, so that employees could do better in detecting and maybe even outright stopping potential cyber threats and risks to the platform.  
  
 For Question 2, Which team you think Chatter needs to help them improve their Cyber Security and why. - We think the team that chatter needs is both the Cyber Threat Team and the Access and Management Team. The Cyber Threat Team is important because it helps to identify the potential threats, knowing that chatter is a social media platform, there are a lot of cyber threats from different sources, based on Charles Griffiths, cyber security attacks globally increased by 125% through 2021, and increasing volumes of cyber-attacks continued to threaten businesses and individuals in 2022. That’s why the Cyber Threat Team is crucial in Chatter. Also, this team’s expertise in analyzing viruses and malware used for information will help chatter in identifying potential vulnerabilities, so this team will surely strengthen chatter’s security. Then the second one is the Access and Management Team, knowing that chatter employs 30 people, surely there are different roles given to each and every employee. So, it is very important for chatter to ensure that each staff member has access only to the systems necessary for their role. This helps in minimizing the risk of unauthorized access.

**LESSON LEARNED:**

I have learned enough info that in to comprehensively address the recent cybersecurity threat at Chatter, a multifaceted strategy is recommended. Besides the previously said risks, enhancing access controls through Identity and Access Management (IAM), applying the principle of least privilege, is essential to restrict unauthorized access and limit lateral movement during a breach. Developing and testing a crisis response plan with Chatter's Crisis Team is imperative to ensure a swift and effective response to various cyber threat scenarios. The Cyber Threat Team should contribute by providing threat intelligence, actively monitoring the threat landscape, and implementing proactive measures to address emerging risks. Lastly, PwC should recommend a continuous monitoring and improvement framework, involving regular assessments, policy updates, and keeping staff informed about evolving cybersecurity practices.

This case taught me that for a social media platform like Chatter, cybersecurity requires a proactive approach. Focusing on Identity and Access Management helps control who can access what, preventing unauthorized entry. Employee training is crucial, making staff a key defense against cyber risks. Planning for crises with Chatter's Crisis Team and using threat intelligence from the Cyber Threat Team are vital. Regular checks and policy updates, guided by PwC, are essential for a strong and adaptable cybersecurity system. The case highlighted the need for a dynamic strategy to tackle both internal and external cyber threats in a fast-changing digital world.