WELLS INTERNATIONAL COLLEGE

T. +61 2 9283 4388 | **F.** +61 2 9283 0748 | **E.** info@wic.nsw.edu.au
Lower Ground, 101 Sussex St., Sydney NSW 2000 Australia | www.wic.nsw.edu.au

ABN: 19 080 559 600 | **CRICOS CODE:** 01856K | **RTO:** 90501

Assessment 2 – Case Study

Instructions:

This is a group of 2 student assessment.

You need to analyse a case scenarios and complete tasks mentioned after scenario.

You need to demonstrate your develop ICT solution ability to identify the solution, determine client support and manage the team in development an awareness of cyber security in workplace.

Duration:

Trainer will set the duration of the assessment.

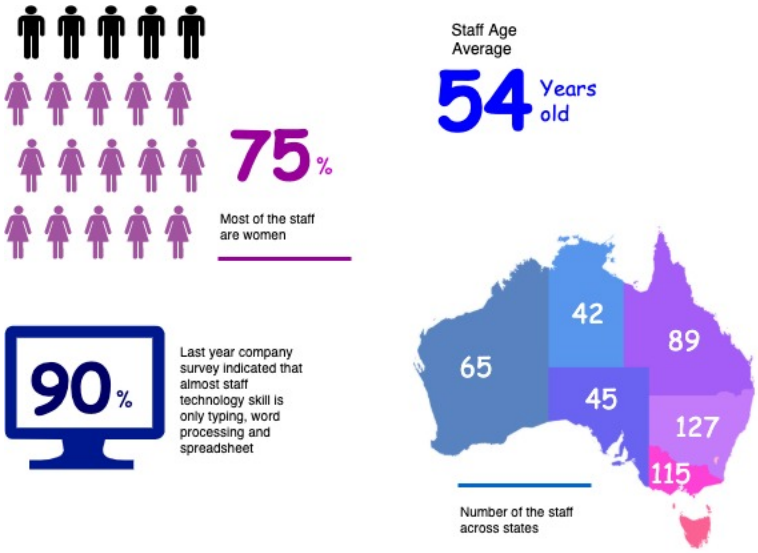
Evidence required:

Tasks	*Evidence*	*Submission*
Supporting Plan Report	A complete report on team supporting and monitoring team performance, and client support for the case study.	In printing

Case scenario

Established in 1999 with offices located throughout the western Sydney, Heaven Systems is a world-class, full-service provider of residential, commercial, and logistics-based transportation solutions for businesses and individuals. Many of the world's largest, most respected corporations rely on the company's unwavering commitment to innovation, quality, and customer service to move their employees, offices, and industrial facilities—domestically and internationally—anywhere in the world. Heaven Systems was experiencing an increase of phishing emails that were reaching employee inboxes and introducing the risk of a data breach. As phishing attacks increased, productivity slowed down while end users waited for IT to investigate the suspicious emails. "Phishing emails were getting more specific and sophisticated, and we worried that an employee might open one and cause serious damage," said David Potter, IT Director at Heaven Systems. While there are multiple layers of security to filter email as it enters Heaven Systems' network, it's still possible for some targeted phishing emails to slip through and get into employee in-boxes. For this reason, IT must rely on end users to determine whether an email is safe to open. But it's not always easy to tell. "For instance," said Potter, "one area of the company was getting phishing emails that looked legitimate. They appeared to come from a customer, but the attachment was malicious."

Refer to employee background statistic show below:



To help employees identify phishing emails, IT holds annual training to show them what red flags to look for. Then, IT sends mock phishing attacks to test them. If a user clicks on a couple simulated phishing emails, they're required to take the security training again. Human nature being what it is, some users were ignoring legitimate email because they didn't want to make a mistake that would require them to take the training again. Others decided to play it safe and send every questionable email they received to IT to see if it was OK. While IT recognized the obvious threats, even they had to question some of the attachments. "You can imagine the amount of time we spent investigating emails," said Potter. "It took about an hour per email to copy the attachment to a USB drive and then spin up a machine to test the file off network," he explained. "That's valuable time that IT could spend doing other things."

You are work as an IT project manager assigned by Potter to handle this problem in the company. The company decide to use the system to detect a Spear-Phishing. To accelerate suspicious email analysis and response, Heaven Systems implemented MailMon, an automated phishing incident reporting and response service that empowers end users to report suspicious emails directly from the inbox. MailMon runs on Microsoft Exchange 2013 or newer and Office365; it is deployed to end users as an Outlook plug-in, including Outlook App for Android and iOS devices.

You and your friend are 10 years' experience staff in the company. After you evaluate the MailMon, it generates a report in the complex form, many of the staff including a current IT department are not familiar

with the system. Potter approved on new project team recruitment, and HR organised 3 **new graduated** IT staffs joining your team. Potter would like your team to gain more awareness on this cyber security incidence.

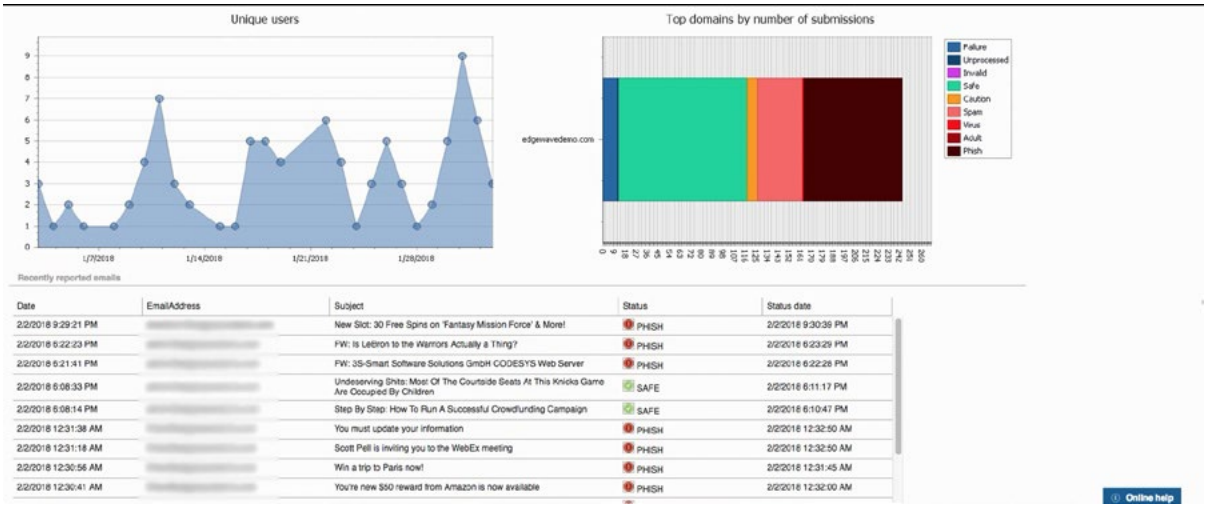


Figure: MailMon Monitoring Sample

Heaven Systems internal IT Service Agreement

Severity Level	Description	Target Response
1 (Outage)	Entire Company Server down	Immediately
2 (Critical)	Entire Department Server down	Within 15 Minutes
3 (Urgent)	Staff computer down	Within 1 hours
4 (Important)	Staff computer not work properly or potential for interrupt their routine work	Within 3 hours
5 (General)	Upgrade software Training request	Within 48 hours

Task 1: Prepare team support and monitor

1. Develop team goal and outcome
2. Develop communication plan for the project team
3. Develop team KPI and action plan to address team training needs
    - Tools and Method for the training
    - Cost and budgeting
    - Schedule
    - Feedback collection plan
    - Evaluation process after the training

Task 2: Review client support

1. Identify and documenting client needs
    - Gap between current organizational support and their needs

2. Develop a client support plan and evaluation plan against company SLAs
    - Area of the support
    - Resources needs
    - Cost and budgeting
    - Schedule
3. Develop a review process on the selected solution
    - Tools and Method
    - Schedule
    - Responsibility

Task 3: Submit both report to your trainer for approval

1. Get feedback from your trainer
2. Amend the document if required