**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.

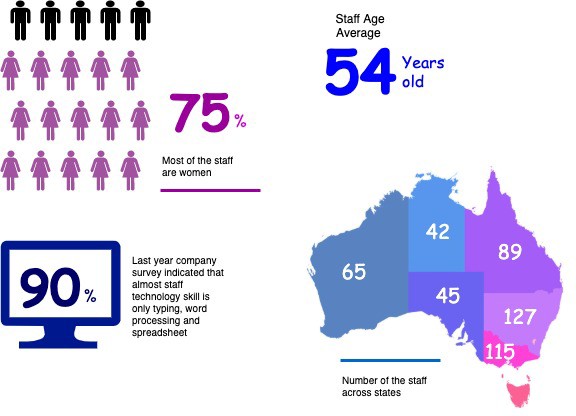
***Evidence required:***

|  |  |  |
| --- | --- | --- |
| *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.

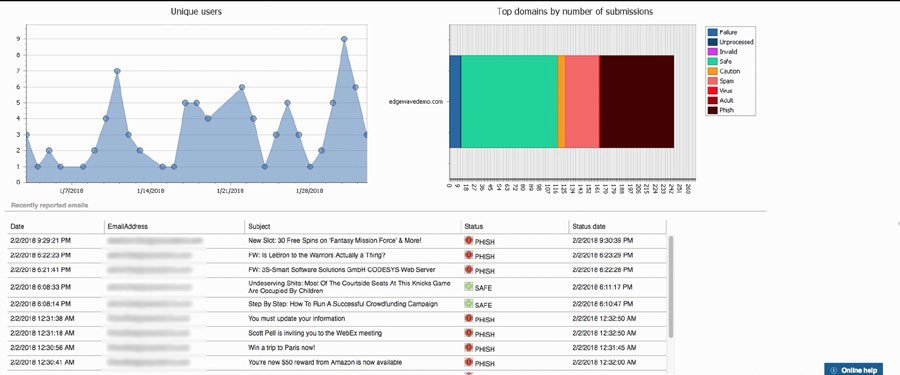


Figure: MailMon Monitoring Sample

# 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

Goal: Gain more awareness on cyber security incidences and prevent them.

Outcome: Maintain a high level of security for our system, employees and customers.

1. Develop communication plan for the project team

It will be part of our team's routine:

- The continued search and study of new security systems and methods;

- The discovery of tools used by criminals;

- Prevention of possible attacks by new invasion methods;

- Internal communication between the team;

- Seminars and training for employees across the company to reduce errors and increase knowledge on the topic.

1. Develop team KPI and action plan to address team training needs
   * Tools and Method for the training

Seminars, meetings, activities and random simulations;

* + Cost and budgeting

There will be not an extra cost since it will be a task with responsibility of our current team.

* + Schedule

It is estimated that these meetings will be held once a month, but depending on the urgency and the more recurrent appearance of new technologies, they may be held more or less often. The simulations will be carried out randomly, without prior notice about dates or type of test.

* + Feedback collection plan

Feedback on understanding the topic will be given immediately after each meeting, this will be a questionnaire which will last just 5 minutes, where participants will be able to leave their comments and recommendations anonymously.

* + Evaluation process after the training

Metrics don't lie. Our results will be measured by them, the more our employees go through the simulations and our system remains intact, this means we will be doing a good job.

# Task 2: Review client support

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

Our company often fails to deliver services within the times established in the SLA. Problem that is caused by lack of standardization, lack of employee knowledge, lack of familiarity with certain tools and systems, organizational difficulties.

Our organizational support today lacks an organization system with the "To Do List" style, creating a more organized routine.

In addition to the routine, we also miss established processes within some activities. The creation of these processes will bring us a result of standardization in carrying out our tasks, making it easier to analyze and improve our methods.

1. Develop a client support plan and evaluation plan against company SLAs
   * Area of the support

Costumer service;

* + Resources needs
* Creation of processes to carry out activities;
* Tools and systems focused on organizing an employee's routine activities;
* Training and monitoring employees on new processes and tools;
  + Cost and budgeting
* Pipefy $40/month;
* Hiring of a new Process Operator for $50,000/year;
* Hiring of a new HR for $65,000/year;
  + Schedule
* Pipefy: Immediately;
* Process Operator hiring: Due in 1 month;
* HR hiring: Due in 1 month;

1. Develop a review process on the selected solution
   * Tools and Method

* Pipefy is a low-code business process automation software that helps HR, Procurement, CS & teams manage and automate workflows.
* Operation, effectiveness and analysis of results from the implementation of the new Pipefy tool;
* Training will be provided for new and old employees;
* Analyzing employee performance and conducting improvement methods will be done more frequently.
  + Schedule
* Studies of new Process Operator and HR about Pipefy: 1 month.
* Pipefy processes and organization method created: 2 months.
* Training being provided: 2 months.
* Pipefy implemented: 2.5 months.
* Start to analyze performance of tool and employee: 3 months.
  + Responsibility
* Pipefy will be used for the optimization of the organization and performance supervision in the employee activities.
* The new Process Operator will be responsible for the operation, effectiveness and analysis of results from the implementation of the new Pipefy tool;
* The new HR will be responsible for organizing recurring training for new and old employees, in addition to the duty of analyzing employee performance and conducting improvement methods.

# Task 3: Submit both report to your trainer for approval

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