1. What was the issue?

* The issue was data breach which happened in the university TKU. PII is very sensitive data from the students or the employees who have been handed over to the university for several purposes.
* PII was not held securely because of unawareness of the security activities which must be handled by the people who were responsible for sensitive data. The main loophole was employees were handling over the sensitive information to other people who might be on contract or temporary and do not have any authorization to deal with it.
* Even the server information which is not to be shared with the people who do not have authorization on it, but due to leakage of the server information the hacking into the system and having Admin rights made it easy.
* Passwords were not made any secure and were not been changed ever and it could be derived from the information which is available on the free source of the university which held it more insecure and easier to get into if they know the server information
* The system was not secure and the polices were not good enough to have a well-secured system from the employees.

1. Who was involved (i.e. what people were causing the issue and resolving?)?

Involvement in the issue:

People who caused the issue and identified the issue happened and resolved the issue are as stated below:

IDENTIFYING: They decided that data is breached as there is an incident where data is exported in a large amount at 2am in the morning which is unusual which was found by gray who is the administrator of TMS.

CAUSING: Lot of people might be included in the bracket of who was included in causing the breach

* Mainly the system was not secure enough to deal with the external breaches
* The Admins gave a lot of people authorization by leaking their password which made the system more insecure.
* The employees have never been educated on the security perspective to handle the system.
* The problem can be categorized to software engineering attempt where the person is tricked rather than the machine gets into the system.

RESOLVING: The Culprit was eventually found though many people were involved in resolving the issue.

* The first issue has been discussed with the Chief financial officer.
* After discussion with the management, the responsibility was given to Financial team mainly Dan was held responsible for identifying the cause
* The External Auditor has also played an important role in resolving the issue.
* All the System Admins and the Admin Group people were enquired to resolve the issue.

1. What approaches were taken to resolve the issue?

The main approach followed is by identifying the users of the PII.

* They started interviewing people in 3 different wings
  + Administrative wing
    - They found the password was passed to temporary workers in order to go on with the flow of the system
  + IT division(computing systems department)
    - There was no clear written policy, business rules have been set and there were 3 admins who had full access to the system in this department.
    - The Password was not standardized and had never been changed from the decades.
  + Financial department
    - The financial department had limited access but still, the password has been shared with people in phone email etc.
* They found where were the possibilities the data could have been breached.
* There were lot many loopholes and stated that the system isn’t secure.
* They arrived at the conclusion when the system admin was asked by some contract employee the details of the server and password was asked to share where though he denied to share it as he felt unusual, he asked an employee to come in person. The Person never showed up.
* As the system password pattern was known she was able to get into the system and took admin rights and steeled the information in minutes as server information where PII was kept was known.

1. What were the outcomes of the issue?

* The process of finding the victim led them to realize the loopholes in the organization.
* Lack of coordination of security policies.
* They were able to find out and distinguish the victims of the data breach
* They found who made it and why they steeled the data of PII from the
* Top management supported to have dedicated resources for creating policies and establish the culture and norms
* Password policies need to be implemented. Access permissions are defined based on the task and not on the designation.
* Training on policies and awareness among the people were conducted to remind that employees are an integral part of security.

From PPT and websites:

1. Are policies different from standards or procedures?  In what ways?

* Policies: It answers what and why and it relates to issues of the key issues of the organizations
* Standard states How much Security implications should be applied to it.
* The procedure says how it has to be implemented and when the policy has to be implemented and who has to follow that policy and do the work.

1. What is the purpose of an EISP, ISSP, and SysSP?  What are the differences?

EISP: Enterprise Information Security Policy

* EISP defines how the corporate system should behave in terms of philosophy on security.
* The responsibility of all the members of the organization has been defined specifically.
* Security has been defined uniquely for each role within the organization.

ISSP: Issue-Specific Security Policy

* Issue-Specific Security Policy specifies the details on the guidance which have been stated
* Rectifying Inefficiency and ambiguity of the organization policy.
* It appropriately specifies the liabilities of the employees and defines the when the system usage is treated as illegal.
* Updating the policies which according to the time

SysSP: System specific Policies:

* The system-specific policies are updated on a regular basis
* The system authorization roles should be changed regularly
* System-related issues like hardware or the software or OS needs to be updated on time to avoid the vulnerable activities.
* Managerial policies, Access control policies etc are involved in technical specification on SysSP.

1. List and describe at least 2 approaches to policy development.

* Implementation of policy
  + Writing the policy
    - Writing the policy which does not obligate the system is a tougher task.
    - Writing Appropriate security policy makes the system more reliable
  + Policy distribution
    - The written policy must be distributed and must be known to everyone inside the system who are included
    - The policies have to be strictly enforced so that everyone needs to remember about it.
* Maintenance of Phase of the policy
  + Maintain and modify the policy as needed
    - The policy must be modified according to the circumstances and it must be well maintained by enforcing it strictly.
  + Built-in the reporting mechanism
    - Policies must be maintained and retained as per required.
    - The incidents occurred outside the policy should be reported immediately.
    - Monthly or weekly scrutiny of the systems on the campus and the system which are accessing the network remotely must be done
  + Periodic review
    - The review of the Policy needs certain attention as policies change according to the change in the system.