NIST Report For a Telecom Company Pegasus

PREPARED BY

Name:

Student ID:

NOTE: **In the report, different colours have been used to represent each function (Identify, Protect, Detect, Respond and Recover) and their respective subcategories.**

1. Asset Management (ID.AM):

The Telecom company "Pegasus" does not understand the critical resources and sensitive data that must be protected, Furthermore, the IT assets used by people who are involved in processing telecom services or providing consultancy while giving a customer's account information (like payment details, bank account information, addresses, social security numbers, etc..). Failing to identify these important assets will lead to issues in the future, such as a risk of data breaches and compromises.

The IT department should start Identifying and categorising all the crucial devices that are used to access information to help apply security measures and ensure that the sensitive information is protected. The Information Technology function is therefore asked to survey the IT assets in the light of the classification rules provided by the internal Compliance & Information Security function, to comply with the following controls:

- **ID.AM-1: The identification and inventory of physical devices and systems used for financial management (such as billing servers) which allows the organisation to monitor and ensure protection against unauthorised access of these critical assets. By doing this the telecom company mitigates the risk of the data being compromised.**
    -
- **ID.AM-2: Pegasus should identify and document the important hardware and software that are important to the companies telecommunication services. Doing this the company can prioritise the protection of these essential components.**
    -
- **ID.AM-6: The implementation of a risk-based data classification ensures the sensitive data is correctly identified, labelled, categorised and protected based on its sensitivity (importance).**

2. Governance (ID.GV):

Pegasus company is using unlicensed software (pirated applications) on some of the devices. This could pose a threat to the company financially since pirated applications may contain viruses and make the company face legal and financial consequences. The Information Technology function is therefore asked to survey the IT assets in the light of the classification rules provided by the internal Compliance & Information Security function, to comply with the following controls:

- **ID.GV-3: The company needs to implement new laws and policies that prevent employees from downloading or using pirated applications. The company should understand the legal consequences and the need to comply with the law.**

1. Access Control (PR.AC):

Pegasus Company does not have a clear policy to define the access rights and privileges granted to its employees and third parties. The lack of control on access privileges can lead to unauthorised access, data breaches and abuses. A former employee still had access and the company didn't properly provoke it. Another employee accessed a customer's data without any authority to do so. The Compliance & Information Security function is asked to provide a more detailed policy on user activation flows and stronger rules on password policies in line with the following controls:

- **PR.AC-2: Assigning users the appropriate access rights based on their role and responsibilities reduces the risk of unauthorised access or internal abuse. This ensures that only authorised persons have access to sensitive assets (especially financial ones) and limits the possibility of data manipulation or theft.**

- **PR.AC-3: Implementing strong authentication mechanisms like multi factor authentication can increase the security of user accounts. This control minimises the risk of unauthorised access.**

- **PR.AC-5: Periodically changing authenticators, such as passwords, reduces the risk of unauthorised access due to compromised or stolen passwords. Frequently updating authenticators limits the effectiveness of attacks based on previously obtained passwords.**

- **PR.AC-6: Regularly reviewing user privileges and revoking wrong privileges will help Pegasus minimise the risk of abuse. By implementing the principles of least privilege the company can minimise the risk of unauthorised access.**

2. Awareness and Training (PR.AT):

Pegasus lacks the security awareness and training programs for its employees, because of that the company will have vulnerabilities because of human errors and social engineering attacks. Therefore the Human resources and the Cyber security functions should provide the needed training for the company, the training should have these requirements:

- **PR.AT-1: Providing a security training program to all employees educates staff about security risks and good cybersecurity practice, helping to raise awareness about protecting financial information and common fraud methods. This reduces human errors, such as opening suspicious attachments or clicking on malicious links, which could lead to security breaches, i.e. it reduces the possibility of employees falling victim to fraudulent activity.**

- **PR.AT-3: Communicating security information to external stakeholders, such as customers, enables them to take appropriate security measures.**

This awareness reduces the risk of social engineering attacks, where external users can be tricked into acting insecurely or disclosing sensitive information.

3. Data Security (PR.DS):

Pegasus doesn't have any measures to protect the data in transit; there are no security measures for the data that is being transmitted. Furthermore the company experiences service outages during peak hours because of the lack of capacity to handle high volumes of traffic. That could lead into performance issues which creates opportunities for malicious hackers to exploit the weakness in the system, So the Information Technology function is therefore asked to survey the IT assets to check if everything is needed and to apply measures to protect data in transit with the following:

- **PR.DS-2: to protect data in transit the company should use secure communication protocols such as TLS(Transport layer security) for encrypted data transmission. They should also implement other security practices such as managing firewalls, network segmentation to isolate important data from less important data and use encryption methods.**
- **PR.DS-4: the company should analyse the current and future demands for their telecom services by estimating what requirements are needed to ensure that they have enough capacity to meet customer needs and having extra capacity incase of a disaster.**

1. Security Continuous Monitoring (DE.CM):

Pegasus relies on external service providers for certain things of their operations, using their cloud services, the issue is the company lacks the visibility of the third companies security practices and activities which is a cybersecurity risk. Also since Pegasus is using pirated software there is a huge risk of malicious code and malware infecting the systems. Which could lead to data breaches or service denials. Therefore the company's IT function should comply with the following controls:

- **DE.CM-4: Pegasus should implement advanced antivirus and anti-malware software across their systems regarding the pirated software and implement strict rules on not to use them or downloading them.**

- **DE.CM-6: Pegasus should implement mechanisms to gather information about the security practices, incident response procedures and security monitoring capabilities of the third company services providers. Furthermore Pegasus should implement a monitoring system so they can see any cyber security vulnerabilities related to the use of the cloud services coordinating with the service providers.**

1. Response Planning (RS.RP):

Pegasus lacks a response plan for cybersecurity related incidents, which will result in a slow and bad response. Pegasus should comply with this control to solve this issue

- **RS.RP-1: Company should implement an incident response plan where the plan should include procedures , roles , responsibilities and escalation paths, which will ensure a coordinated and good response.**

2. Communications (RS.CO):

After investigating the Pega further we can see that it doesn't have good coordination within their incident response. Lack of clarity regarding roles and responsibilities can affect the response team's ability to respond to incidents. Furthermore Poor communication protocols will affect the information sharing and coordination during the incidents. The company should comply with these controls to solve these issues:

RS.CO-1: Pegasus should establish clear communication channels and protocols among incident response teams and others. Also implementing secure communication platforms and defining communication procedures.

RS.CO-3: Defining and communicating incident response roles and responsibilities for the company. By making a team leader and conducting regular meetings to synchronise response activities and sharing updates.

3. Analysis (RS.AN):

The company suffers from the lack of forensic analysis which affects the company's ability to understand the cause and impact of cyber incidents. Not only that the cyber security employees have inconsistent documentation for incidents related to the company to fix this Pegasus should implement these controls to solve the issues:

- **RS.AN-1: Establishing robust forensic analysis tools and procedures to collect and analyse digital evidence related to company's services, Also implementing investigations to identify the cause of the incidents.**

- **RS.AN-2: Implementing a standard incident documentation process to capture relevant incident details, action taken and lessons learned from the incident. Also maintaining an incident repository for references.**

1. Recovery Planning (RC.RP):

Pegasus does not have a recovery plan that is well defined or tested. Which is helpful to restore operations after a cyber incident happens. To fix this issue Pegasus should apply these controls:

- **RC.RP-1: Developing an extensive recovery plan that defines the steps , procedures and resources required to recover and restore the operations after a cyber security incident. Also testing the plan to ensure its effectiveness.**

2. Improvements (RC.IM):

The organisation relies on old recovery strategies that do not align with the evolving threats and technologies. These strategies were designed 7 years ago and havent been changed yet. To tackle this issue the company should implement these controls:

- **RS.IM-2: By regularly reviewing and updating the recovery strategies to tackle emerging threats and technological advancements.**

3. Communications (RC.CO):

After inspection Pegasus faced challenges during an incident where the coordination between the response team and recovery team were lacking which led to delays and miscommunication which affected the recovery process. As a result of that the company struggled to minimise the impact of the incident and restore the services in time. To fix this issue the company should apply these controls:

- **RS.CO-3: Defining clear roles, responsibilities for the incident response and recovery teams. By implementing training and meetings to ensure smooth collaboration, information sharing and coordination between them.**