Risk assessment report based on NIST Cybersecurity Framework

Telecome Company

Summary:

company is a Telecome company operating in different reginal locations. To secure the infrastructure and the services provided by this company a risk assessment based on the NIST Cybersecurity Framework is required to be carried out. SeaCell has a Headquarter in Rome Italy and many branches spread out through Europe.

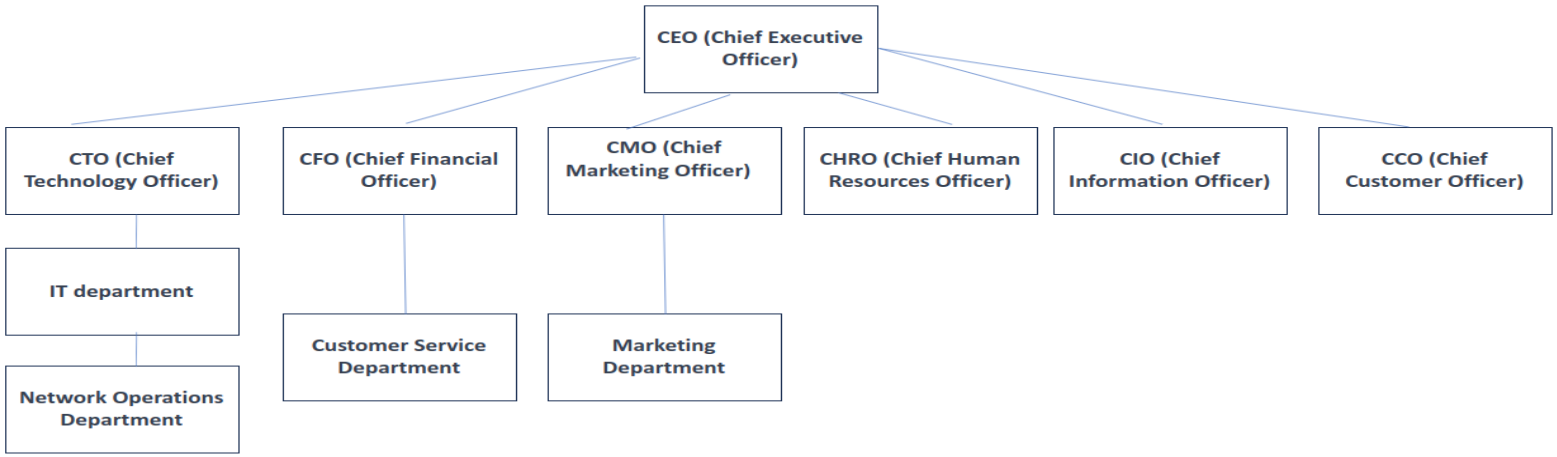

Figure-1 – SeaCell organizational chart

As shown in the organizational chart in Figure-1 SeaCell has a large organizational structure with departments clearly defined.

In this report the major valuable entities of the organization have been assessed based on the NIST framework as shown in Figure-2.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Figure-2 – Functions and categories

In this report in addition to using the NIST Cybersecurity Framework, I have tried to take into consideration the top 20 Critical Security Controls published by the Center for Internet Security and prioritize the controls based on that. (https://www.cisecurity.org/controls/cis-controls-list)

Identify (ID)	**ID.AM-1: Physical devices and systems within the organization are inventoried**	The SeaCell Network is a sprawling network spanning multiple regions, and due to its extensive branch network/remote sites, maintaining an accurate inventory of connected devices has been challenging. As a result, there are a significant number of devices on the network that can access corporate data on the network without being properly inventoried. This lack of visibility increases the risk of unauthorized devices and malicious access to sensitive data. To mitigate these risks, it is imperative for the SeaCell Network to establish a comprehensive inventory of physical equipment, devices, and systems within the organization. By maintaining an accurate and up-to-date inventory, the network can effectively identify and monitor all authorized devices, ensuring that any unidentified or rogue devices are promptly detected and mitigated.

	ID.AM-2: Software platforms and applications within the organization are inventoried	While an inventory of connected devices has been established at the headquarters of the SeaCell Network, the remote branches currently lack a comprehensive inventory. This creates a significant challenge as many users in these branches/remote locations, as well as through the cloud, are utilizing/using software programs that are unknown and not officially authorized. Also, numerous developers are directly testing their web app/software on the production environment using AWS, which poses a significant security risk. These unauthorized software installations can be easily manipulated by malicious users, exposing the network to potential security breaches. Additionally, the practice of leaving running applications unattended without following proper exit or removal strategies further increases the risk of unauthorized access by potential intruders. For example, web applications tested by remote users and developers without authorization have

		left several accessible subdomains exposed to external parties. The absence of a centralized repository for authorized software further increases the security risks. Users should be required to access the repository first and install applications from there, regardless of their location (HQ, remote devices, or cloud). To address these issues, it is crucial for the SeaCell Network to establish a centralized and comprehensive inventory software system across all branches. Additionally, strict policies should be implemented to ensure that only authorized software is used and that proper exit strategies are followed for running applications. By centralizing the repository for authorized software, the network can significantly reduce the risk of security breaches and ensure a more controlled and secure environment for all users, regardless of their location.
	ID.AM-3: Organizational communication and data flows are mapped	The absence of a comprehensive and up-to-date architectural diagram, as well as

		the lack of detailed data flows for the system, present significant challenges for the SeaCell Network. The current information regarding the network diagram and data flow is presented in plain text and lacks careful visualization. For instance, most of the connections between services in SeaCell are running on port 80 and utilizing HTTP. Similarly, the backend connections run on the default SQL port 1433, which was not clearly indicated in the data flow diagram, and to understand such information from text-based documentation needs a great amount of time. Furthermore, the data flow does not accurately depict the intended path it should follow. This lack of detailed diagrams and accurate data flows can create difficulties in locating and securing assets within the SeaCell Network. Without a clear visual representation of the network architecture and data flow, it becomes challenging to identify and protect critical components of the system.

		To address these issues, it is essential for the SeaCell Network to invest in creating a complete and updated architectural diagram. This diagram should accurately represent the network infrastructure, including the connections between servers, services and the flow of data. Additionally, the diagram should clearly indicate the specific ports and protocols used in the network. By having a visual representation of the system's architecture and data flows, the SeaCell Network will be better equipped to identify potential vulnerabilities, locate assets, and implement appropriate security measures to safeguard the network effectively.
	ID.AM-4: External information systems are catalogued	The broad catalogue of file sharing services, including platforms such as Dropbox, OneDrive, and various private websites, presents challenges in monitoring user activities. These services are being used by SeaCell Network users

		to host files, despite the lack of a valid business use case for the company. The utilization of unauthorized file sharing services introduces several risks to the network's security and data integrity. It becomes difficult for the company to enforce proper access controls, track data transfers, and ensure compliance with regulatory requirements. Additionally, the lack of visibility into these external platforms poses a significant challenge in identifying and mitigating potential security threats. To address this issue, it is crucial for the SeaCell Network to establish clear policies and guidelines regarding file sharing and data storage. These policies should clearly define approved platforms that align with the company's business needs and security requirements. User awareness programs (**PR.AT-1)** can also be implemented to educate employees about the risks associated with using unauthorized file sharing services and

		emphasize the importance of adhering to company policies. Furthermore, the SeaCell Network should invest in suitable technologies and solutions that enable effective monitoring and control of file transfers. This may involve deploying data loss prevention (DLP) tools, network monitoring systems, and user activity tracking mechanisms. By implementing these measures, the company can enforce proper data governance and minimize the risks associated with unauthorized file sharing services, ensuring the protection of sensitive information and maintaining regulatory compliance.
	ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	The current list of assets in the NIST assessment report fails to prioritize based on business drivers, which poses a significant risk. A specific example is the database hosted in the on-premises data center, containing sensitive end user/customer data. Surprisingly, this database is not categorized as a high priority for the organization, despite the

		potential for both financial and legal repercussions (financial loss and damaged reputation) in the event of a breach. To address this issue, it is crucial for the organization to establish a comprehensive understanding of asset criticality. While the current list of assets provides enough information at server, application, and process levels, it lacks a macro view that considers what truly generates value within the organization's systems. By determining the criticality of assets, the organization can effectively allocate resources and prioritize security controls. This holistic perspective will guide decisions on where to implement protective measures, allocate detection resources, and enhance incident response efforts. It is vital to recognize that asset criticality extends beyond financial implications and includes the potential legal consequences resulting from the compromise of sensitive data.

		Establishing asset criticality based on business drivers is imperative for the organization's overall security strategy. This approach will facilitate the implementation of appropriate controls, enabling the organization to prioritize its protection efforts, enhance detection capabilities, and ensure efficient incident response. By accurately assessing the criticality of assets, the organization can safeguard its most valuable systems and data, mitigating risks and potential damages to both its financial standing and legal compliance.
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	This control primarily focuses on individuals and their roles within the organization. However, it is observed that roles and responsibilities have not been fully assigned in alignment with established policies. The existing security programs primarily concentrate on corporate security

		(internal IT infrastructure), overlooking the importance of enterprise security and service/product security. Also, third-party stakeholders are excluded from the scope of security considerations. The internal/domestic security team lacks well-defined scopes of responsibility, leading to uncertainties within the organization. This results in a lack of clarity regarding the expectations from the security/IT team, as well as team members' understanding of what is expected from them. To address these issues, it is crucial for the organization to take the following steps: Reassess and realign roles and responsibilities in accordance with established policies: This will ensure that individuals are assigned appropriate responsibilities based on their roles, ensuring accountability and adherence to security policies.

		Expand security programs to encompass enterprise security and service/product security: By including these aspects, the organization can comprehensively address security requirements and consider the involvement of third-party stakeholders. Clearly define the scope of responsibilities for the internal/domestic security team: This will enable the organization to set clear expectations and establish a framework for the security/IT team members. It will also help team members understand their specific roles and responsibilities within the organization. By implementing these measures, the organization can improve its security posture, foster clarity and accountability within the security/IT team and ensure a comprehensive approach to security that encompasses all relevant stakeholders.
Protect (PR)	**PR.AC-3: Remote access is managed**	The current remote access system for branches connecting to the Headquarter

		in Rome, Italy lacks a strong access control policy. Users are only authorized by passwords, and the cryptographic method used is not robust. Furthermore, there is no dedicated device in place to manage remote connections. To address these issues, implementing the following measures is recommended: Implement 2-factor authentication (2FA): Adding an extra layer of authentication, such as a token-based or biometric authentication method, alongside passwords can significantly enhance the security of remote access. This ensures that even if passwords are compromised, unauthorized access is still prevented. It is required to use stronger cryptographic methods: Upgrade the cryptographic algorithms and protocols used for remote access to more secure and robust options. This will enhance the confidentiality and integrity of data transmitted over the network, reducing

		the risk of unauthorized interception or tampering. Deploy specialized devices for remote connection management: Introduce edge multi-layer switches or similar dedicated devices to manage and secure remote connections. These devices can act as gateways, terminating and controlling connections before allowing access to the internal network. They provide additional security features, such as firewall capabilities and intrusion detection systems, to protect against unauthorized access attempts. By implementing these measures, the organization can significantly improve the security of remote access connections. 2FA adds an additional layer of authentication, making it more difficult for unauthorized individuals to gain access even if passwords are compromised. Stronger cryptographic methods ensure secure transmission of data, while dedicated devices for remote

		connection management provide enhanced control and protection against unauthorized access attempts. Overall, these measures will help strengthen the organization's remote access security and safeguard the network from potential threats
	PR.AT-1: Awareness and Training	The organization currently lacks an information security and privacy awareness training policy, which exposes them to increased risks of social engineering and phishing attacks. To address this gap, it is crucial to establish a comprehensive information security and privacy awareness training program. This program should be mandatory for all new employees and stakeholders as part of their initial training. By incorporating basic security and privacy awareness training into the onboarding process, individuals will be equipped with the basic and necessary

		knowledge/skills to identify and mitigate potential risks. The training program should cover essential topics such as recognizing phishing emails, understanding social engineering tactics, safeguarding sensitive information, and following best practices for data protection. It should emphasize the importance of maintaining strong passwords, being cautious with sharing personal or confidential information, and remaining vigilant against suspicious online activities. Additionally, the training program should be periodically updated to address emerging threats and changes in security and privacy regulations. Regular reinforcement sessions and ongoing awareness campaigns can also help reinforce good security practices and foster a culture of security within the organization.

		By implementing an information security and privacy awareness training policy, the organization can significantly reduce the risks associated with social engineering and phishing attacks. Educating employees and stakeholders about the potential threats they may encounter and providing them with the necessary knowledge and skills will empower them to make informed decisions and take proactive measures to protect sensitive information and maintain a secure work environment.
	PR.DS-1: Data-at-rest is protected	The current encryption method used to protect data at rest on the critical database servers is insufficient. This poses a significant risk as it may potentially compromise the security of customers' personal data, leading to financial loss and reputational damage if not promptly addressed. To mitigate this risk and enhance data protection, it is essential to upgrade the encryption measures employed for data

		at rest on the critical database servers. Strong encryption algorithms, protocols, and key management practices should be implemented to ensure the confidentiality and integrity of the stored data. By employing industry-standard encryption techniques, such as AES-256 (Advanced Encryption Standard with a 256-bit key), the organization can significantly improve the security posture of its critical database servers. This robust encryption algorithm, along with proper key management practices, adds an additional layer of protection to sensitive customer records and reduces the likelihood of unauthorized access. It is crucial to regularly assess and update the encryption mechanisms to stay aligned with the latest security standards and best practices.

		By addressing the inadequacy of the current encryption used for data at rest on critical database servers, the organization can mitigate the risks associated with data exposure. Strengthening encryption measures safeguards customers' personal data, protects the organization's financial well-being, and preserves its reputation.
	PR.DS-2: Data-in-transit is protected	The current replication of data between the headquarter servers and branches lacks the use of a strong encryption method. Instead, a simple and potentially insecure method is employed, which poses a significant risk to the confidentiality and integrity of the data being transmitted. To address this issue and enhance data security during replication, it is crucial to implement a strong encryption method for the channels and tunnels between the headquarter servers and branches. Strong encryption ensures that data is protected

		from unauthorized access and interception during transmission. One recommended approach is to utilize secure protocols such as Transport Layer Security (TLS) or Secure Shell (SSH) for data replication or use IPsec tunnels for remote site-to-site connections. These protocols provide secure communication channels and encryption mechanisms to safeguard data in transit. By implementing strong encryption methods for data replication, the organization can mitigate the risk of data interception and unauthorized access. It ensures that sensitive information remains confidential and maintains the integrity of the replicated data. Also, it is important to regularly assess and update the encryption protocols used for data replication to stay aligned with evolving security standards and best practices. By prioritizing the implementation of strong encryption methods for data in

		transit and in the case of this company, replication, the organization can significantly enhance the security of data transmitted between the headquarter servers and branches, reducing the risk of data breaches and unauthorized access.
Detect (DE)	**DE.AE-2: Detected events are analyzed to understand attack targets and methods**	The current information system audit policy in place does not adequately support all ranges of event types, including user logins, logoffs, failed login attempts, data viewing, data updates, data deletions, changes in data access, user account creations, modifications, and deletions. This gap in event auditing poses a significant risk, particularly in the face of Advanced Persistent Threats (APTs). APTs involve malicious users who aim to infiltrate and persistently operate within the network while remaining undetected. The lack of comprehensive event monitoring increases the likelihood of such threats going unnoticed, potentially leading to severe consequences.

		To mitigate the risks associated with APTs, it is crucial to implement an enhanced audit policy that encompasses the complete range of relevant event types. By monitoring user activities, data access, and account management events, the organization can gain valuable insights into potential security incidents and identify suspicious or unauthorized activities. In addition to an improved audit policy, continuous monitoring of system logs and implementing Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are highly recommended. These systems help in detecting and mitigating potential threats, including APTs, by analyzing network traffic, identifying abnormal behavior, and taking appropriate actions to prevent or minimize the impact of attacks. By implementing a comprehensive audit policy, continuously monitoring system logs, and deploying IDS and IPS systems, the organization can significantly reduce

		the chances of APTs and enhance its ability to detect, respond to, and mitigate potential security threats. It is important to maintain vigilance and stay up-to-date with the latest security practices to effectively combat evolving threats in the digital landscape.