CASE STUDY

Given the present organizational structure of the existing case study, the structure is the same.

The RACI (Responsible, Accountable, Consulted, and Informed) matrix would inform us about the employees or other people who are accountable for their actions.

These are widely implemented in many organizations and would be helpful in understanding the scenarios.

FRAMEWORK	CISO	SECURITY MANAGER	ADMINISTRATION	IT	FINANCE	SECURITY OPS
DETECT	C	C	I	R	I	A
RESPOND	I	R	I	A	I	R
REPORT	I	R	I	C	C	R
RECOVER	C	A	I	R	I	A
REMEDIATE	A	R	I	R	C	R
REVIEW	R	R	I	A	I	R

The RACI matrix provides us with a detailed report on the organizational structure.

Given the specifications of the organization and the RACI matrix, the fundamentals can be described as:

CISO :

The framework for detection is discussed with the CISO; even though he is not involved in the project, he needs to be informed and involved. He needs to be aware of the stages of responding and reporting, per the RACI matrix. Although he does not actively perform the role, the CISO nevertheless has to be kept informed about the team's progress or decisions and needs updates. The chief information security officer (CISO) is also consulted throughout the recovery phases; his expertise in this area can be beneficial. He is directly responsible for the remediation stage in his capacity as chief lead for security operations. He is also directly accountable for the remediation phase. He needs to be put to work to generate solutions. The CISO is also responsible for reviewing the situation. The CISO is needed to complete the task and make the decision.

SECURITY MANAGER :

The administration, IT, financial, and security operations departments are all under the control of the security manager. The frameworks of detection are discussed with the security manager, and while the manager responds to specific scenarios by taking action, he also elevates situations to other teams in order to address the scenarios. He is also in charge of the procedures for reacting to and summarizing the events. The assigned duty needs to be finished by the security manager. He is also responsible for getting better and needs to act. Additionally, he is the proprietor of the work and has the authority to provide the appropriate teams with his signature.

The steps of remediation and situation review fall under the purview of the security manager. He is at the top of the food chain and can control everything, despite the fact that many others may share responsibility for the situation.

ADMINISTRATION :

Other teams that are components of the company make up the administrative team, including the legal and contracting teams. These teams focus on the system's fundamental features. Even though these teams are not involved in security activities, they must be informed, along with the following teams. They must be informed of developments and kept up-to-date on the issue. They do not directly contribute to the mission and do not require official consultation.

IT :

Data officers and technicians make up the IT teams. The staff, which is in charge of overseeing IT operations, is seen at work. In addition to being liable for detection, the team is also accountable for action. The team's technicians are in charge of making sure duties are carried out and delegating tasks to dependable workers.

The IT staff is also in charge of the phases of remediating and recovering. To make sure the issue has been fixed, they must be taken into account and frequently worked on.

They are directly responsible for the reviewing stage; to ensure the defense is properly built, they must physically undertake operations on the systems and networks.

FINANCE :

The finance team is made up of groups like the collection officers and accountants. These teams work on economics and resource availability while also assisting the retail shoe group in raising the necessary funds. Here, the foundations for detecting and responding are explained to these teams. Here, they are placed in a predicament and informed of the updates and suggestions. On the reporting phase, the team is consulted. They are included in the process and present to offer suggestions. They are apprised of the specific recovery and review frameworks. They must remain under consideration.

SECURITY OPERATION :

The incident responder and security engineer teams are only two examples of the various teams that make up the security operations team. These teams are in charge of making the discovery and entrusting the subsequent process to reputable people or workers. They are also in charge of reacting to and reporting the circumstances. These are the individuals in charge of carrying out the assignment and achieving the goals. These teams, which are established inside the company for the security process, are also in charge of recovery. Physically and externally via networks, the network is responsible for the security of the network; these teams are also in charge of situation detection and recovery.

They are also in charge of assessing and resolving the problem. The IT staff responds to the requests made by the teams and focuses on them individually. In this case, each of these events is reported to the security manager, who then informs the CISO.

- **Where your initial assumptions were right on or needed to be adjusted**

Although the initial assumptions are valid, there are some little adjustments that need to be made. The organization’s structure given is a part of the complete organization. Some of the assumptions that are to be adjusted are the security manager's operations and working of the CISO. Some of the more teams that are to be developed are correlated between IT and the security operations team. For an organization's and its employees' safety and security, security teams are in charge. They work to keep the organization safe from potential threats and to guarantee the security of the organization's assets and facilities. Teams in charge of security may also be in charge of conducting investigations into incidents and educating staff members about security.

- **Any remaining gaps or concerns you still have**

The security operations teams must be addressed separately; teams such as incident responder and security engineer are divided into different teams. An organization can adopt a wide range of security procedures to safeguard its personnel, assets, and data. Physical security, which includes locks and security guards; cyber security, which includes safeguards against online threats; and information security, which includes protocols and technologies to secure sensitive data, are some examples of standard security measures. Organizations can contribute to ensuring the security of their personnel, clients, and assets by creating and putting into place an efficient security plan.

References :

https://www.thebalancesmb.com/what-is-security-operations-2534294