CIS410-50-4238

Case 3 – Care Group James Cook

Summary

Care Group faced a challenging situation due to a critical failure in their network, resulting from the use of an untested program. As they try to fix the problem, Care Group further discovers many more issues that contributed to the failure. While many of its users lack knowledge of IT, Care Group needs to develop a solution to prevent individual users from causing system failures.

Issue

There were many minor issues involved in the Care Group incident. The root cause came from one of the researchers running a program that consumed all the bandwidth, forcing the system to go down. On top of that, outdated systems and unorganized network structure worsened the situation with looping within the network. They did not immediately seek help from the experts, and there was only one key employee who managed the IT. Since the infrastructure was added on top of the existing network, the added complexity made it difficult to diagnose the problem. This originated from it being a decentralized organization with proprietary applications used in individual hospitals - a lack of standardization.

Mission and Strategy

While the mission of Care Group is to provide healthcare across multiple locations, they also focused on medical research to become the leader in the industry. Care Group had connections with academic institutions allowing them to quickly advance. The use of technology in healthcare allowed them to manage the patients with ease while maintaining high quality service.

Five Forces

Based on the context, the market has low threats of substitutes or entry as Care Group was already large in scale. Since medical related organizations require heavy investment and long time to develop, it will be difficult for new parties to enter the market. However, the rivalry is high for the existing competitors as there are even larger groups in the nearby area. The suppliers have somewhat bargaining power, but due to many alternative options, Care Group has the choice to work with a specific vendor for their equipment and services. The buyers, patients in this case, have high bargaining power as HMOs controlled the price in between the patient and the hospital.

Organizational Structure

Care Group was formed with multiple hospitals grouped together creating a network. Each hospital operated primarily on their own, with a bit of management from the Care Group. The transition towards centralized IT structures allowed them to operate more efficiently, but it also revealed weaknesses of system-wide failure just like the outage incident.

Stakeholder Groups

Healthcare providers, such as doctors and nurses, are the core users of the Care Group network. During their day-to-day business, they would utilize the system to access or modify information related to patients. Without a functioning IT system, they would have to work on papers which raises more troubles and difficulties.

Patients are the clients of the Care Group; they visit in need of health care and expect a systematic approach to handling their medical needs. Due to the outage, they experienced delays in the process, negatively affecting patients.

IT department manages the IT within the organization and is responsible for maintaining the system. However, they overly relied upon one person to manage everything which led to problems during one’s absence. Major challenges that the IT department faces are recovering from the outage and improving its redundancy to prevent any future failures.

Cisco is an outside vendor that plays a critical role in this incident. They are the expert groups, highly skilled and efficient in handling tasks. They were able to fix the problem overnight which otherwise would have taken a month. Their priorities are customer care and ensuring the up-to-date industry standard.

Researchers are another group that uses the system but is not directly related to the regular hospital tasks. Their use case has direct and indirect effects on the system, one of them was the cause of this incident. Researchers have access to the system with less knowledge just like healthcare providers, leaving potential points of failure in the system.

 IT service providers, such as vendors that sell hardware and software, are another stakeholder. They would benefit from Care Group purchasing equipment. For Care Group to keep its systems up to date, Care Group needs to work closely with the service providers to gain access to modern technology.

Alternatives

1. Permission control of the system.

Just like the target incident, one researcher was able to take down the whole system due to its ability to access various parts of the network. Since the file sharing program was able to send data to multiple computers within the network, it quickly got out of control. Restricting certain parts of the network by firewalls may allow the system to prevent unauthorized access that triggers high traffic. Furthermore, limiting the software that can be used until they are tested safe can prevent such issues.

1. Implementation of a sandbox environment.

Even though the researchers may need to access the network, it seemed completely unnecessary to gain full access to the entire system during their research process. Whatever they do, it is possible to keep it within the virtualized environment so that all changes are kept within the sandbox and the system is untouched. This allows the system to have an extra layer of protection in case of an accident.

1. Modernization and standardization of the IT

This was part of the main reasons why the system failed. If Care Group kept the system up to date, some of the looping issues that contributed to the total system failure might have been prevented. On top of that, modern hardware will streamline its operation.