Hackers blackmail mahanta, spandan section b statement of the problem

Environment, Animals

Hackers Blackmail Mahanta, Spandan Section B Statement of the Problem: Implementation of EMR (Electronic Medical Records) to replace paper records in Sunnylake hospital was a visionary idea. However a major area in implementation oftechnologyi. e. Network Security was overlooked by the organisation. Moreover there was limited or no risk assessment done leaving Sunnylake's IT team ill equipped to handle a possible intrusion into their network.

The result was that the organisation was forced into a situation where they were on the verge of getting into myriad of legal problems including lawsuits amounting to millions. But more than the monetary damages, human lives were at stake which made it even more important for the Sunnylake team to arrive at an early and effective solution to the problem in hand. Analysis: Paul Layman had come to Sunny lake Hospital with the vision to transform the small hospital from a Community Care Centre to a role model for all small hospitals.

To turn his vision into reality Paul Layman, the CEO decided to use state of the art technology to replace paper records with Electronic Medical Records (EMR). Accordingly a plan was formulated leading to formation of an IT team in the organisation under theleadershipof a young IT Director Jacob Dale. Both Paul and Jacob gave in their best to implement a system which was initially not widely accepted by majority of the Doctors in the hospital. However with time, as the efficiency of the EMR's showed up the resistance became minimal.

For good three years Paul was basking under the glory of his successful implementation of EMR’s but was naive enough to overlook the technology security advancement and did not keep its security up to date and updated. Sunnylake Hospital was almost at a dead end mainly due to human and technological errors. The intrusion into their network was due to someone in the staff mistaking the threat to be an antivirus download or updation of an existing application. This can be a termed as a human error. But more importantly lack of an updated or upgraded security system hich is a major technology flaw was the major contributor to network invasion of the Sunnylake hospital network. The result of these mistakes resulted in Sunnylake hospital on the verge of losing millions in lawsuits, losing the reputation it had built up over the years of service to the community and most importantly a large number of human lives were at stake. Keeping in mind the repercussions of their mistakes, which were quite serious in nature the most immediate solution that I feel would be appropriate would be to pay the ransom amount to hackers thus securing the safety of the affected patients.

Having done this we can look at the future course of actions which should include stringent security/access policies, stronger network administration and safety and last but not the least educating the staffs of the network safety measures that needs to be taken care of while using or accessing the organisations network. While we are discussing about all these prominent problem statements, Paul Layman CEO of Sunnylake also has to deal with another long term effect of the fiasco. He had implemented a system for which he had received resistance from many quarters.

However with the passage of time as the EMR’s proved to be efficient, these resistances subsided. Now that the EMR’s failed after 3 years of efficient work, the people who had opposed the very implementation of technology including the chief of staff George Knudsen would have a free say to justify their resistance at the first place. And Paul has to see to it that the crisis is solved immediately as he is at a risk of not being able to convince the staff to trust the system or more importantly trust him. Recommendations:

In reference to the analysis of the problem above, the following solutions in order of priority along with recommendations are mentioned below. First and foremost Paul Newman will have to pay the ransom to the hackers in order to secure the lives of the affected patients as well as get back access to their network. However he should not overlook the adversities that may crop up later and I would recommend engagement of professionals with expertise in dealing with such situations including law enforcement agencies.

Once access to the network is gained, the organisations IT team should immediately put into place network safety policies. For this I would recommend that the IT team implement stricter security policies, access should be limited for the users as per the roles delivered, commonly known dangerous websites be blocked, training the staff on the security measures and finally up gradation of their systems to be able to avert such instances in future.