Case Study – IT/CyberSec Governance

“Medicine for future” is the largest medical organization in the public sector working with many scientific institutes and laboratories to create a COVID-19 vaccine. “Medicine for future” operates with the license and under the supervision of ministry of health in the country.

“Medicine for future” tries to comply all regulatory requirements and best practices in healthcare, almost all polices, and producers are in place to protect customers data and privacy.

The board of “Medicine for future” consists of seven board members, responsible for governing, monitor and oversight the institution’s operations. Six of them are recognized doctors and scantiest and one of them has an experience in IA and Risk management.

There is an Internal Audit department, who’s main objective is to evaluate internal control processes.

There is an Audit and Risk committee in “Medicine for future”, which is the most active committee in the institution. One of the board members, who seats in this committee well-known professional in the country and has more than 20+ years of expertise in Risk management.

There is no IT and information/cyber security steering committee, and the board was responsible for the oversight of IT and cybersecurity risks.

IT DEPARTMENT

“Medicine for future” has a relatively big IT recourses and technologies. IT department consists of four divisions:

1. Network and system management,
2. DB and application management,
3. Banking technology development
4. Information security

Although head of IT department well informed about international best practices and standards for IT service delivery, IT management and IT governance, however he had his own individual vision about institution’s strategic development.

IT department recently developed strategic plan and shared with business-managers, however there was no formal process for review and feedback. From 15 business managers only 2 of them responded. Others sent a short message, that It’s not their duty to read IT strategy *(which is heavily technical document)* and give any feedback.

In the last year, the “Medicine for future” has been hacked two times and hackers managed to stole gigabytes of sensitive data. Although there were a backup plan and procedures, however the IT department did not manage to recover business processes on time, because the backup was outdated and there was a huge need to manually input of some important data to recover core business processes. Some data has been available on the internet which created a huge problem for “Medicine for future” and for ministry of health as well.

The ministry of health warned them that the license would be terminated if the board of directors do not take serious actions.

The board of directors "fired" the CEO of "Medicine for future" and appointed a new one. There was some debate among board of directors, to "fire" the Internal Audit staff as well, but some of the board members, who were the members of Audit and Risk committee, were against, and stated that in previous audit reports the Internal Audit mentioned several high risks, which could lead to serious problems. Some of the board members became incredibly angry, **why they are not aware of that**, if the Internal Audit found some serious risks, what were the actions of the management?

After a very difficult discussion, the board decided to "fire" only the head of internal audit department and appoint a new one from the outside of the "Medicine for future".

The new CEO in turn "fired" the previous CISO *(chief information security officer)* as he was in charge of business continuity and appointed a new CISO.

Question:

1. Based on the Cobit and NIST cybersecurity framework, what are the key actions of the new CISO?
2. What was the mistake of the former head of internal audit? Was she guilty?
3. What should the new CAE do?
4. What kind of governance issues were in the "Medicine for future"?
5. What else you mentioned based on the provided information?

NIST Cyber Security Framework

Cobit