Рассмотрение конкретного примера – управление ИТ/кибербезопасностью

"Медицина для будущего" - крупнейшая медицинская организация в государственном секторе, работающая со многими научными институтами и лабораториями над созданием вакцины против COVID-19. "Медицина для будущего" работает по лицензии Министерства здравоохранения страны и под его надзором.

"Медицина для будущего" старается соответствовать всем нормативным требованиям и передовой практике в области здравоохранения, в организации действуют практически все политики и процедуры, направленные на защиту данных клиентов и сохранение их конфиденциальности.

Правление организации "Медицина для будущего" состоит из семи членов, отвечающих за управление, мониторинг и надзор за деятельностью учреждения. Шесть из них являются врачами и учеными, а один из них имеет опыт работы в области внутреннего аудита и управления рисками.

Существует отдел внутреннего аудита, основной задачей которого является оценка процессов внутреннего контроля.

В "Медицине на будущее" существует комитет по аудиту и рискам, который является самым активным комитетом в учреждении. Один из членов правления, одновременно являющийся членом этого комитета, хорошо известный в стране профессионал с более чем 20-летним опытом работы в области управления рисками.

В организации нет руководящего комитета по ИТ и информационной/кибербезопасности, а за надзор в сфере ИТ-рисков и кибербезопасности отвечает правление.

ПОДРАЗДЕЛЕНИЕ ИТ

"Медицина для будущего" располагает относительно крупным массивом ИТ-ресурсов и технологий. Подразделение ИТ состоит из четырех отделов:

1. Управление сетями и системами,
2. БД и управление приложениями,
3. Разработка банковских технологий
4. Информационная безопасность

Несмотря на то, что руководитель ИТ-отдела хорошо знаком с лучшими мировыми практиками и стандартами предоставления ИТ-услуг, оперативного и стратегического управления ИТ, у него было собственное видение стратегического развития организации.

ИТ-подразделение недавно разработало стратегический план и поделилось им с бизнес-менеджерами, однако при этом никакой официальный процесс рассмотрения и обратной связи задействован не был. Комментарии поступили только от двух из 15 бизнес-менеджеров. Другие прислали короткое сообщение, что изучение ИТ-стратегии (*глубоко*

технический документ) и предоставление каких-либо отзывов на нее не входит в круг их обязанностей.

За последний год "Медицина для будущего" была взломана дважды, и хакерам удалось украсть гигабайты конфиденциальных данных. Несмотря на то, в организации имеется план и процедуры резервного копирования, ИТ-службе не удалось вовремя восстановить бизнес-процессы, так как резервная копия устарела, и для восстановления ключевых бизнес-процессов необходимо было вручную вводить большие массивы важных данных. Некоторые данные попали в интернет, что создало огромную проблему для "Медицины для будущего" и для министерства здравоохранения.

Министерство здравоохранения предупредило организацию, что если ее правление не предпримет серьезных действий, лицензия будет отозвана.

Правление "уволило" генерального директора организации и назначило нового. Члены правления также рассматривали вопрос об "увольнении" сотрудников службы внутреннего аудита, но некоторые из членов правления, которые являлись членами комитета по аудиту и рискам, были против, и заявили, что в предыдущих аудиторских отчетах служба внутреннего аудита упоминала о ряде серьезных рисков, которые могли привести к возникновению серьезных проблем. Некоторые члены правления были чрезвычайно возмущены тем фактом, **что им было неизвестно** о том, какие действия были предприняты менеджментом для реагирования на обнаруженные внутренним аудитом серьезные риски.

После очень трудного обсуждения правление решило "уволить" только начальника отдела внутреннего аудита и назначить нового, не имевшего отношения к "Медицине для будущего".

Новый генеральный директор в свою очередь "уволил" предыдущего *директора по информационной безопасности*, так как он отвечал за непрерывность бизнеса, и назначил нового директора по информационной безопасности.

Вопросы:

1. Исходя из концепции кибербезопасности Cobit и NIST, какие основные действия должен предпринять вновь назначенный директор по информационной безопасности?
2. В чем была ошибка бывшего руководителя службы внутреннего аудита? Была ли она виновна?
3. Что следует предпринять новому руководителю службы аудита?
4. Какие проблемы управления были в организации "Медицина для будущего"?
5. Что еще вы могли бы сказать в связи с представленной информацией?


ВОССТАНОВИТЬ
ВЫЯВИТЬ
ОТРЕАГИРОВАТЬ
МЕХАНИЗМ КИБЕРБЕЗОПАСНОСТИ, ВЕРСИЯ 1.1
ЗАЩИТИТЬ
ОБНАРУЖИТЬ


Корпоративное управление
Управление ИТ
Адаптация ИТ к бизнесу
Оценивать
Направлять
Контролировать