«Фармацевтическая отрасль», ноябрь № 6 (77) 2019

PQE запускает новое бизнес-направление – DIGITAL GOVERNANCE (цифровое управление)

Думай
технологически

ОПЫТ

С помощью ключевых партнёров мы ставим цели, узнаём требования бизнеса и анализируем потребности и риски. Как улучшить и защитить свои бизнес-процессы? Как сократить время доставки партий? Достаточно ли гибок процесс, чтобы соответствовать требованиям конечного клиента и не нести больших потерь? Что нужно для более эффективной работы корпоративных активов? – Работая вместе, мы определяем возможные сценарии для достижения целей клиента.

Решай
технологически

СТРАТЕГИЯ

С помощью заинтересованных лиц внутри компании и, непосредственно, клиентов мы разрабатываем стратегию, основываясь на сценариях, определённых во время процесса «думай технологически». – Мы оцениваем самые выгодные сценарии, учитывая бизнес, перспективы информационных технологий и, самое главное, бизнес-цели клиента. Мы предоставляем численное решение с отражением результатов сопоставительного анализа, стоимости реализации и коэффициента окупаемости вложений, которые являются главными аспектами этого шага для оптимизации соотношения цены и качества.

Действуй
технологически

РЕАЛИЗАЦИЯ

Мы ведём проект и внедряем решение, используя проверенные методы компании PQE | Прозрачное преобразование конкурентного предложения в готовое решение, учитывающее соответствующее требованиям GxP и технологические инструменты. Надлежащая практика информационных технологий минимизирует усилия на достижение соответствия требованиям.

Живи
технологически

РАБОЧИЙ ПРОЦЕСС

Мы постоянно улучшаем процесс преобразования любого конкурентного предложения в действующее решение, обеспечивающее устойчивую работу | Непрерывный мониторинг, анализ KPI, отчеты, аналитика данных и программа осведомленности делаются в соответствии с требованиями бизнеса.

Мы находимся на пути к технологической революции, которая существенно меняет наш образ жизни, стиль работы, ведения бизнеса, и система здравоохранения не является исключением. Все мы знаем о «четвертой промышленной революции» и сегодня понимаем, что она неуклонно приближается. Глобальная коммуникация, бизнес и сотрудничество, движимые технологией, преобразуют способ, с помощью которого компании должны реагировать, чтобы обеспечить получение прибыли и оставаться конкурентоспособными. Скорость нынешних прорывов не имеет исторического аналога. Все больше отраслей промышленности принимают эти изменения, инвестируя в проекты раннего внедрения и в новые условия работы.

Облачные сервисы, IIoT, автоматизация, роботизированная автоматизация процессов – это лишь некоторые из новых технологий в рамках того, что называется Digital. Они играют решающую роль в продвижении инноваций и бизнеса, но киберугрозы все чаще становятся серьезным препятствием и риском для дальнейшего пути компании к прогрессу.

Сегодня промышленность сталкивается со все большим количеством угроз кибербезопасности. Для более эффективного решения этих систематических проблем компании повышают уровень доверия к цифровым технологиям, защищая свои инновации и интеллектуальную собственность. Для достижения этих целей и обеспечения безопасности система здравоохранения должна обеспечивать собственную устойчивость за счет повторного использования того же поведения в целях соблюдения строгого регламентированного стандарта и создания внутренней структуры управления кибербезопасностью.

Среда лекарственных средств и изделий медицинского назначения

Некогда независимая производственная среда была проприетарной и типичной индивидуальной системой без прямого подключения к Интернету, поэтому к ней нельзя было легко получить доступ извне. Подход, аналогичный ранее используемой ИТ-инфраструктуре, где в течение последних 10 лет постепенно исчезало понятие традиционной технологии, преобразовался в более гибридный виртуальный подход и облачные сервисы.

Сегодня в фармацевтической промышленности появилась возможность осуществить автоматизацию роботизированных процессов на производстве. Это то, с чем индустрия изделий медицинского назначения сталкивается благодаря мобильным устройствам, которые в свою очередь взаимодействуют непосредственно с самим изделием.

Стратегия и управление должны быть установлены для защиты данных, созданных в компании. Избегайте нежелательных изменений и позвольте этой информации стать интуицией компании для повышения производительности и минимизации потерь.

Как система здравоохранения может использовать преимуще-

ства новых технологий, одновременно минимизируя риск в отношении безопасности?

Снижение риска

Задача состоит в том, чтобы определить необходимые действия, которые должны быть выполнены правильно. Область IT (информационные технологии) отличается от OT (операционных технологий). Несколько факторов приводят к разным уровням конфиденциальных данных, которые нужно тщательно учитывать.

В природе самого бизнеса система здравоохранения является хранилищем ценной информации (персональные данные, сведения о разработке лекарств, результаты конфиденциальных исследований). Вся эта конфиденциальная информация находится в руках одной из крупнейших экономик, которую киберпреступники считают привлекательной целью.

OT-система имеет определенные алгоритмы действия, контролируемые в режиме реального времени системой, такой как SCADA или PLC, в том числе и большое количество сообщений, которыми обмениваются многие датчики. Характер подобного сотрудничества приложений усложняет управление сквозным производственным процессом. Организация мониторинга, аутентификации и сбора данных помогает лучше понять процесс, но этот тип подключения дает киберпреступникам возможность проникновения в систему и предоставляет дальнейший доступ к «плодородной земле».

Производственный процесс должен строго соблюдаться. Необходимо обновлять систему, участвующую в процессе, что обеспечит базовую защиту путем устранения уязвимостей. Иногда процесс обновления откладывают или вовсе его избегают, так как для этого требуются дополнительные усилия по квалификации и соответствующее вложение финансовых средств.

Система здравоохранения должна задаться вопросом: насколько она готова проиграть, если кибератака завершится успехом и интеллектуальная собственность будет похищена? Или если производственная линия будет повреждена в течение нескольких дней?

В июне 2017 г. кибератака на компанию Merck нанесла ей ущерб в размере USD 670 млн.

Систематический подход к средствам соответствия

Следует разработать систематический подход к соблюдению кибербезопасности, в котором будут учтены все аспекты проблемы, включая нормативную. На рынке широко доступны технические меры для устранения уязвимостей OT-системы, такие как управление портами USB, удаленным доступом и необходимый мониторинг сетевых угроз. Важно помнить, что их внедрение интегрировано в контекст корпоративного соответствия.

Различные международные регулирующие органы публикуют обновленные стандарты в отношении влияния новых технологий и кибербезопасности. Начиная со «старого» FDA 21 CFR Part 11, посвященного фармацевтической промышленности, и заканчивая самыми последними 2017/745–746 в отношении изделий медицинского назначения, путем применения данной политики и определения контрольных точек можно обеспечить первую линию защиты кибербезопасности. Однако необходимо разработать методологию определения вмешательств, которая имеет глобальное значение для кибербезопасности. В этом отношении, например, можно сослаться на «Систему кибербезопасности» Национальной лаборатории кибербезопасности (CINI) или ISO 27001, целью которой являются управление и контроль безопасности компании. Следует разработать модель для создания, реализации, эксплуатации, мониторинга и поддержания информационной безопасности внутри компании. Также ISO 27001 поможет с другим фундаментальным аспектом – организацией и управлением.

Необходимо выбрать программу вмешательств с четко определенными ролями и обязанностями. Это не должно быть в руках только ИТ-отделов и инженерных подразделений. Корпоративная безопасность начинается с того, что каждый сотрудник осознает, каким образом его действия могут оказать негативное влияние на корпоративную безопасность. Ответственность за осведомленность лежит на высшем руководстве. Ею нужно управлять посредством проведения различных тренингов об основах социальной инженерии и просвещения в рамках данных вопросов. Их цель – убедить персонал задуматься о мерах безопасности, поскольку в конечном счете это выгодно для компании.

Кибербезопасность от PQE

Четыре этапа PQE Group нацелены на то, чтобы помочь системе здравоохранения адаптироваться к изменениям и быть готовыми войти в эру «четвертой промышленной революции» и внедрения «Индустрии 4.0». PQE Group обладает проверенной, рациональной методологией, целью которой является решение проблем для достижения ощутимого результата с помощью структуры, процессов и мышления. ◘

Контактная информация:

Сандлер Юрий
Управляющий директор
Тороповский Александр
Менеджер по развитию бизнеса
Тел.: +7 (929) 616 - 53 - 23
РФ, 127015, г. Москва
ул. Новодмитровская, 2к2
БЦ Савеловский Сити, башня Davis
Тел.: +7 (495) 133 - 98 - 36
e-mail: a.toropovskiy@pqegroup.ru
www.pqegroup.ru