Наращивание потенциала кибербезопасности Набор инструментов для финансовых организаций

Инструкции для генерального директора: Лидерство в сфере кибербезопасности

Управление

Кибербезопасность организации начинается и заканчивается на высшем уровне руководства. Генеральный директор и совет директоров должны понимать риски и нести полную ответственность за деятельность организации в области обеспечения кибербезопасности и подбора соответствующего персонала. Вы должны сделать следующее.

⇒ Нанять директора по информационной безопасности (CISO) или, если ресурсы слишком ограничены, назначить сотрудника организации для выполнения этой функции.
⇒ Сотрудничать с директором по информационной безопасности или другими техническими специалистами, чтобы разработать и обеспечить поддержку стратегии и структуры кибербезопасности, адаптированные к конкретным киберрискам организации, используя международные, национальные и отраслевые стандарты и руководящие принципы.
⇒ Четко формулировать роли и обязанности персонала, обеспечивающего внедрение и управление кибербезопасностью организации.

- Совместно с директором по информационной безопасности определять надлежащие роли в сфере кибербезопасности и права доступа для всех сотрудников.
- Контролировать взаимодействие и сотрудничество с целью обеспечения целостности процесса управления кибербезопасностью, особенно если обязанности по обеспечению кибербезопасности передаются нескольким сотрудникам или подразделениям внутри организации (например, при наличии отдельных вертикалей управления информационной безопасностью, рисками и технологиями).

⇒ Убедиться, что директор по информационной безопасности имеет четкую прямую линию коммуникации для своевременного уведомления вас и совета директоров об угрозах.
⇒ Приглашать директора по информационной безопасности или другого технического специалиста для регулярного информирования высшего руководства.
⇒ Обеспечивать единообразие политик, стандартов, механизмов принудительного исполнения и процедур обеспечения безопасности организации во всех подразделениях и направлениях деятельности.

Оценка рисков и управление ими

Обеспечение высокого уровня осведомленности о кибербезопасности и готовности к работе зависит от непрерывного анализа рисков. Для повышения уровня кибербезопасности организации сделайте следующее.

⇒ Установите приоритет оценки рисков и управления рисками кибербезопасности в рамках более широкого процесса управления рисками в организации. Организуйте сотрудничество с директором по информационной безопасности или другим техническим специалистом по плану проведения оценки рисков, предусматривающему:

- описание активов организации и различных уровней их зависимостей от технологических ресурсов;
- оценку зрелости организации и неотъемлемых рисков, связанных с зависимостями ее активов от технологических ресурсов;
- определение желаемого состояния зрелости организации;
- анализ приоритетных областей для обеспечения кибербезопасности в организации;
- выявление несоответствий между текущим состоянием и желаемым целевым состоянием кибербезопасности;
- реализацию планов для достижения и поддержания зрелости;
- постоянную переоценку зрелости кибербезопасности организации, рисков и целей;
- рассмотрение проведения проверки на проникновение третьих лиц или с привлечением «красной команды»,
- рассмотрение возможности принятия защитных мер, таких как приобретение киберстраховки.

⇒ Руководите работой сотрудников во время процесса оценки рисков, чтобы обеспечить своевременное реагирование по всей организации.
⇒ Обеспечьте анализ и отчетность по результатам оценки рисков к рассмотрению исполнительным руководством, в том числе ключевыми заинтересованными сторонами и советом директоров.
⇒ Контролируйте любые изменения, необходимые для поддержания или повышения готовности вашей организации к обеспечению готовности систем кибербезопасности, гарантируя, что любые меры по улучшению систем кибербезопасности соотносятся с рисками и доступны для вашей организации.
⇒ Контролируйте текущий мониторинг, который должен обеспечивать быстрое реагирование и гибкость в отношении возникающих киберрисков.

Организационная культура

Кибербезопасность организации не является единовременным процессом или ответственностью нескольких сотрудников. Этот фактор необходимо учитывать во всех деловых решениях и операциях, а практика должна поддерживаться всеми сотрудниками. Поощряйте непрерывное и целостное обеспечение кибербезопасности в организации:

⇒ Начните с обсуждения вопросов кибербезопасности с руководством и регулярно общайтесь с персоналом, отвечающим за управление киберрисками.
⇒ Сделайте обучение принципам кибербезопасности частью процесса адаптации сотрудников и убедитесь, что все сотрудники осведомлены и подписали документы, подтверждающие соблюдение политик кибербезопасности организации, а также что ИТ-отдел или другой технический персонал провели их обучение передовым практикам.
⇒ Проводите периодические тренинги по кибербезопасности для всех сотрудников в отношении их краткосрочных и долгосрочных обязательств.
⇒ Убедитесь, что вопросы кибербезопасности всегда учитываются при оценке организацией потенциальных поставщиков и передаче данных третьим сторонам.
⇒ Ежегодно пересматривайте политики кибербезопасности организации.
⇒ Поощряйте добровольный обмен информацией об угрозах кибербезопасности и инцидентах в пределах организации и с доверенными партнерами.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE · SWIFT INSTITUTE · FS-ISAC · Standard Chartered · CYBER READINESS INSTITUTE · GLOBAL CYBER ALLIANCE