Наращивание потенциала кибербезопасности Набор инструментов для финансовых организаций

Инструкции для совета директоров: Лидерство в сфере кибербезопасности

Основы управления киберрисками

Подтвердите, что вы можете утвердительно ответить на следующие вопросы:

1. Соответствует ли ваша организация **применимым законодательным и нормативным требованиям**?

2. Выполнила ли ваша организация **количественную оценку киберрисков и проверку финансовой устойчивости**?

3. Имеет ли ваша организация действующий **план по улучшению**, гарантирующий, что воздействие находится в приемлемых пределах рисков?

4. Регулярно ли совет **обсуждает лаконичную, четкую и действенную информацию касательно предоставляемой руководством устойчивости организации к угрозам кибербезопасности**?

5. Имеет ли ваша организация **планы реагирования на недавно протестированные инциденты**, в том числе на уровне совета директоров?

6. Являются ли **роли ключевых сотрудников, ответственных за управление киберрисками,** четкими и согласованным с тремя линиями защиты?

7. Получили ли вы **независимую аттестацию и гарантию** устойчивости вашей организации к киберрискам?

Надзор

Являясь высшим звеном руководства организации, совет директоров несет полную ответственность за управление киберрисками и, следовательно, должен контролировать стратегию, политику и деятельность организации в этой области. В частности, совет директоров должен:

⇒ Нести полную ответственность за контроль киберрисков и устойчивости как в качестве правления в полном составе, так и в случае делегирования надзора конкретному комитету совета директоров.
⇒ Назначить одного корпоративного директора, как правило, главного директора по информационной безопасности, ответственным за отчетность о способности организации управлять киберустойчивостью и развитием в достижении целей устойчивости к угрозам кибербезопасности. Убедиться, что этот сотрудник имеет регулярный доступ к совету директоров, обладает достаточными полномочиями, имеет в распоряжении соответствующий коллектив, опыт и ресурсы для выполнения этих обязанностей.
⇒ Ежегодно определять допустимость рисков организации; обеспечить согласованность с корпоративной стратегией и приемлемыми пределами рисков.
⇒ Обеспечьте проведение ежегодного официального независимого анализа киберустойчивости организации.
⇒ Обеспечить контроль над созданием, внедрением, тестированием и постоянным усовершенствованием планов киберустойчивости, обеспечением согласованности во всей организации, а также регулярностью отчетов перед советом директоров, предоставляемых главным директором по информационной безопасности или другим ответственным должностным лицом.
⇒ Интегрировать процедуры киберустойчивости и оценки рисков в общую бизнес-стратегию организации, управление рисками, планирование бюджета и распределение ресурсов с целью полной интеграции киберрисков в общие операционные риски.
⇒ Периодически проверять собственную эффективность и учитывать независимые рекомендации по непрерывному усовершенствованию.

Будьте в курсе

Эффективный контроль киберрисков зависит от коллектива участника и актуальной информации.

⇒ Убедитесь, что все члены совета директоров имеют применимые и актуальные навыки и знания, позволяющие понимать связанные с киберугрозами риски.
⇒ Регулярно консультируйтесь с руководством по текущим и будущим рискам в организации, соответствующим нормативным требованиям, а также отраслевым и социальным ориентирам для снижения приемлемых пределов риска. Также участвуйте в регулярных брифингах по последним разработкам в отношении ландшафта угроз и нормативно-правового регулирования, в совместном планировании и во встречах с коллегами и ведущими специалистами в области кибербезопасности, а также организуйте обмен опытом по вопросам управления и отчетности.
⇒ Возложите на руководителей ответственность за предоставление количественно выраженной и доступно изложенной оценки киберрисков, угроз и событий в виде повестки дня во время заседаний совета директоров.
⇒ Будьте всегда в курсе текущих системных проблем, например уязвимостей в цепи поставок, общих зависимостей и недостатка информации при обмене данными по вопросам управления киберрисками между советами директоров.

Создание атмосферы

Помимо руководства высшего звена, совет должен определять и соблюдать основные ценности организации, культуру рисков и ожидания в отношении киберустойчивости.

⇒ Поощряйте культуру, в которой сотрудники на всех уровнях осознают важность своих обязанностей по обеспечению киберустойчивости организации. Подавайте пример.
⇒ Контролируйте роль руководства в формировании и поддержании в организации культуры рисков. Продвигайте, контролируйте и оценивайте культуру рисков, принимая во внимание влияние культуры на безопасность и надежность, а также при необходимости вносите необходимые корректировки.
⇒ Четко объясните, что вы ожидаете от всех сотрудников добросовестного отношения и незамедлительного информирования обо всех случаях несоблюдения нормативных требований в организации или за ее пределами.

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