Connected Cyber Risk Platform (CCRP)

инструмент для достижения стратегических целей

Наша платформа по управлению киберрисками

1. Объединяет усилия ключевых игроков — советов директоров, владельцев рисков, менеджеров по ИБ и ИТ, для поддержки управления киберрисками.
2. Является единым центром отчетности и принятия решений по управлению киберрисками.
3. Обеспечивает переход к практике количественной оценки киберрисков, используя практичную и международно признанную методику количественной оценки, позволяющую учитывать финансовую отдачу от решений, принятых для минимизации киберриска.
4. Адаптирована к различным уровням зрелости и доступности необходимых данных.
5. Обладает возможностями, необходимыми для создания экосистемы управления рисками ИТ и непрерывности.

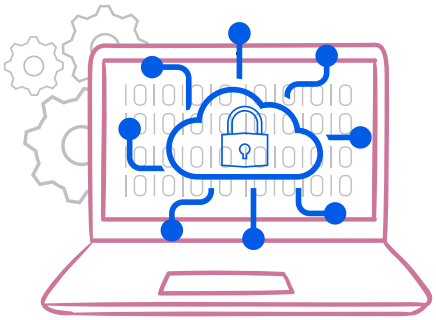
Ключевые факторы успеха

1. **Гибкая** — используется технология low-code (язык Power BI DAX), снижающая требования к навыкам программирования. Система может быть развернута локально или в виде SaaS-решения
2. **Наполненная опытом и IP** — мы не зависим от иностранного лицензирования и уже использовали нашу методику и инструментарий в нескольких крупных проектах
3. **Прагматичная** — наша модель данных подстраивается к уровню зрелости Клиента, связывает различные источники для достижения максимального результата
4. **Полноохватная** — элементы отчетности покрывают потребности Совета Директоров, владельцев бизнес-процессов и активов, и функционеров ИТ и ИБ
5. **Оперативная** — вы сможете получить первые результаты через 3-4 недели после запуска проекта

Помогает управляющим директорам*:

Синхронизировать управление киберрисками со стратегическими потребностями бизнеса по риск-аппетиту и дорожной карте развития

Интегрировать требования кибербезопасности в организационную структуру Компании, её культуру и в процесс принятия решений



Использовать управление киберрисками в качестве движителя стратегии развития бизнеса, позволяющего управлять доверием и ожиданиями

Обеспечить доступ к качественной экспертизе и отчетности, необходимой для управления киберрисками

* National Association of Corporate Directors, Principles for Board Governance of Cyber Risk, MARCH 2021.

Технологии Доверия

Концентрируемся на стратегических рисках

Увеличить EBITDA Компании **на 20 млрд. руб.** (пример)	Остановка операционной деятельности в ходе кибератаки	Длительный срок восстановления после атаки привел к снижению выручки во время инцидента **на 65%** (пример)
Расширить количество активных пользователей мобильных приложений **до 30 млн.** (пример)	Регулярные утечки пользовательских данных приводят к снижению рейтинга мобильных приложений и оттоку пользователей	**От 6% до 10%** (пример) активных пользователей удалили мобильные приложения после новостей о взломе и краже данных
Увеличить **инвестиционную привлекательность** Компании	Планы M&A и ранние отчеты о финансовых результатах стали доступны злоумышленникам	Изменение условий M&A привело к снижению привлекательности сделки. Стоимость акций снизилась на фоне заявлений об инсайдерской торговле

Реализуем современную и практичную методику

ОТОБРАТЬ

Критичные события риска

- Проанализировать контекст и бизнес-среду Компании
- Найти ИТ-зависимые компоненты бизнес-стратегии
- Выявить приоритетные кибер-события, способные нанести ущерб или нарушить стратегические планы

ОПИСАТЬ

Сценарии инцидентов

- Определить степень агрессивности внешней среды
- Определить приоритетных агентов угрозы
- Определить приоритетные цели и пути атаки
- Определить способность контрольной среды противостоять приоритетным сценариям инцидентов

РАССЧИТАТЬ

Симуляция и моделирование

- Определить наиболее вероятные сценарии развития инцидентов
- Определить компоненты и размер ущерба
- Определить финансовые показатели и полный профиль риска

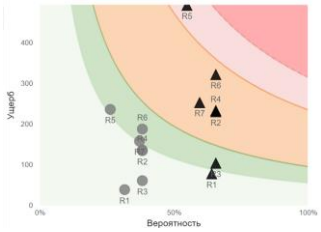
УПРАВЛЯТЬ

Решение и обработка

- Сравнить профиль риска с риск-аппетитом
- Определить снижаемые риски
- Сформировать программу по обработке рисков
- Детализировать инициативы по развитию контрольной среды
- Определить формат отчетности

Используем собственный инструментарий

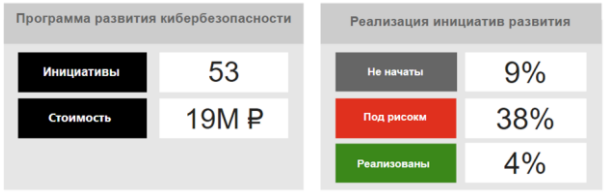
Карта киберриска



Корпоративный профиль киберриска

#	Киберриск	Единичный ущерб (SLE) млн. руб.	Среднегодовой ожидаемый ущерб (ALE), млн. руб.	Риск аппетит	ALE после снижения (ALE'), млн. руб.	Риск аппетит
R1	Случайная утечка информации о клиенте	120,00	76,95	✓	37,99	✓
R2	Кража конфиденциальной деловой информации	350,00	229,76	✗	133,90	✓
R3	Кража информации о клиенте	157,00	103,06	✓	60,06	✓
R4	Нарушение бизнес деятельности	354,00	232,39	✗	135,43	✓
R5	Нарушение работы онлайн-сервисов	895,00	491,27	✗	235,39	✗
R6	Кража денежных средств	489,00	321,01	✗	187,07	✗
R7	Потеря цифрового доверия	423,00	252,22	✗	157,37	✗

Программа управления киберриском



Всегда готовы прийти вам на помощь

Мы помогаем нашим клиентам сделать большой шаг от культурной модели «страх, неопределенность и сомнения», к связному и прозрачному восприятию профиля киберрисков Компании, позволяющему принимать финансово-оптимальные решения по управлению киберрисками.

Напишите нам, если хотите узнать о продукте больше, или увидеть его работу в ходе демонстрации.

Михаил Толчельников
Руководитель направления «Управление киберрисками»

+7 (495) 967 3382

+7 (968) 330 7219

mikhail.tolchelnikov@tedo.ru