Кибербезопасность в корпоративном управлении

Чаплыгин Роман

Солар - ведущий поставщик решений кибербезопасности

Солар – под защитой половина страны и ключевые инфраструктуры экономики

КРУПНЕЙШИЕ КОМПАНИИ:

Транспорт, металлургия, крупнейшие банки, онлайн-площадки, электроэнергетика

Крупнейшая телеком-инфраструктура страны – ПАО «Ростелеком»

КЛЮЧЕВЫЕ ИНФРАСТРУКТУРЫ:

Госуслуги, социальный блок, гособлака, значительная часть ФОИВов

Все крупнейшие мероприятия с участием Первого лица

ПМЭФ, ВЭФ, форум «Россия-Африка», Молодежный форум

«Выборная инфраструктура» во время выборов Президента Российской Федерации

ВЕНДОР | СЕРВИС-ПРОВАЙДЕР | ИНТЕГРАТОР

SOLAR

1,5 МЛРД
отраженных атак в год

8
офисов, охватывающих всю территорию России

200+ МЛРД
анализируемых событий ИБ

1000+
организаций под защитой

1400+
проектов по построению кибербезопасности в год

2000+
экспертов по кибербезопасности

Важность кибербезопасности для руководства, акционеров и СД

SOLAR

Кибербезопасность связана с защитой конфиденциальной информации компании, ее активов и репутации

1. ОТВЕТСТВЕННОСТЬ	Руководство организации несет ответственность за управление компанией. Законодательство предусматривает административную и уголовную ответственность для определенных категорий сотрудников и самих компаний
2. СТРАТЕГИЧЕСКОЕ ПЛАНИРОВАНИЕ	Кибербезопасность – область, которая требует существенных инвестиций и времени на получение возврата от них. Представители руководства должны учитывать кибербезопасность при разработке стратегии компании
3. РЕПУТАЦИЯ	Утечка конфиденциальной информации или кибератака могут повредить репутации компании. Руководители отвечают за сохранение репутации компании
4. ФИНАНСОВЫЕ РИСКИ	Кибератаки и утечки данных могут привести к нарушению операционной деятельности и значительным финансовым потерям. Руководство отвечает за операционное и финансовое здоровье компании
5. ЗАКОНОДАТЕЛЬНЫЕ ТРЕБОВАНИЯ	Закон требует выполнения компаниями требований по кибербезопасности, наиболее популярные: о КИИ, о ПДн. Представители руководства должны организовать работу компании в условиях применяемого Права
6. УПРАВЛЕНИЕ РИСКАМИ	Управление киберрисками требует полномочий и находится на уровне руководства компании. Руководство должно обладать компетенциями для принятия верных управленческих решений
7. КИБЕРКУЛЬТУРА	Этика и безопасное поведение в цифровом мире должны продвигаться руководителями компании. Руководство должно демонстрировать значимость кибербезопасности своим примером и поведением

Кибербезопасность в корпоративном управлении

ТЕХНИЧЕСКИЕ АСПЕКТЫ

Киберриски систем КУ определены и организована их защита от:

- Подмена результатов голосований
- Утечка материалов и протоколов СД
- Уничтожение материалов, протоколов и решений СД
- Подмена или неточность отчетных данных
- …

Корпоративное управление кибербезопасностью

УПРАВЛЕНЧЕСКИЕ АСПЕКТЫ

КУ влияет на кибербезопасность компании путем:

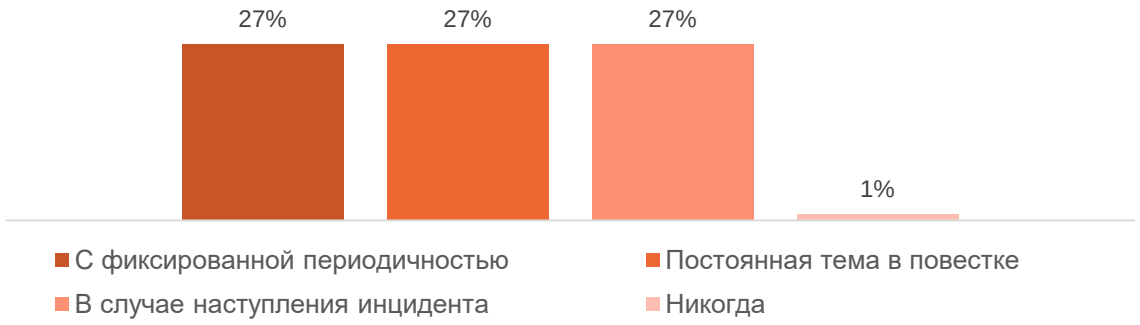
- Кибербезопасность регулярно в повестке СД
- Киберриски определены, отслеживаются и понятны СД
- Ответственность СД по киберрискам установлена
- Роль по подготовке отчётности и взаимодействию с СД по кибербезопасности назначена
- Независимость, полнота и достоверность анализа кибербезопасности обеспечены
- Надзор СД за развитием кибербезопасности осуществляется
- …

Совет директоров и кибербезопасность: результаты опроса С-уровня

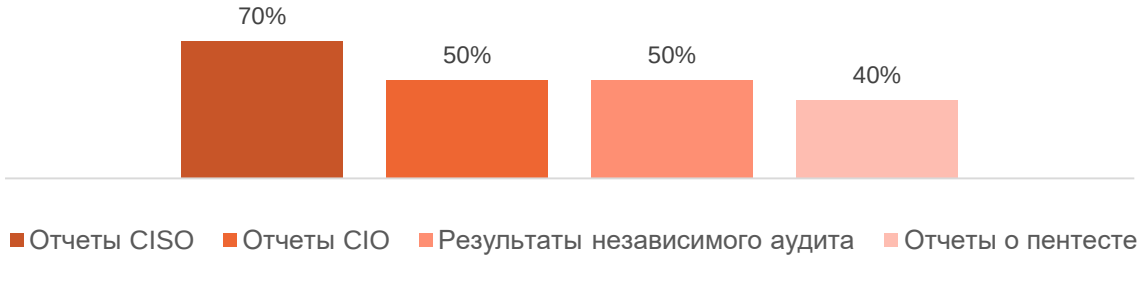
SOLAR

50% ПРЕДСТАВИТЕЛЕЙ С-УРОВНЯ И СД ПРИНИМАЮТ ЛИЧНОЕ УЧАСТИЕ В СТРАТЕГИЧЕСКОМ УПРАВЛЕНИИ ИБ

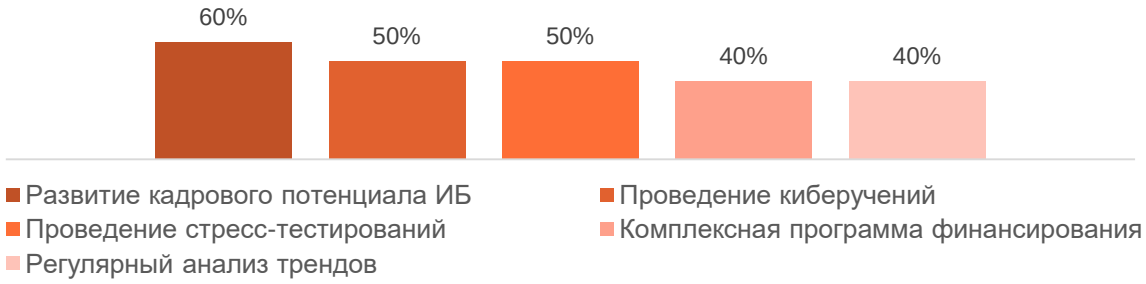
КАК ЧАСТО НА СОВЕТЕ ДИРЕКТОРОВ ОБСУЖДАЕТСЯ КИБЕРБЕЗОПАСНОСТЬ



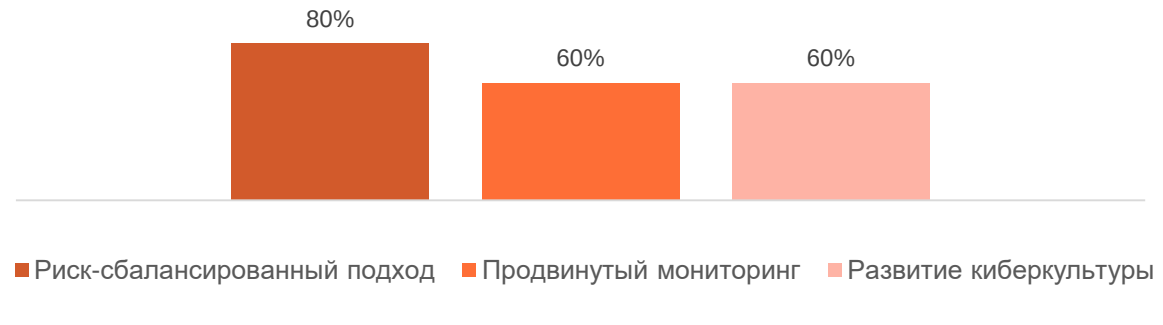
НАИБОЛЕЕ ПОПУЛЯРНЫЙ ИНСТРУМЕНТ ОЦЕНКИ ЭФФЕКТИВНОСТИ КИБЕРБЕЗОПАСНОСТИ



ЧТО МОЖЕТ ПОВЫСИТЬ ЭФФЕКТИВНОСТЬ КИБЕРБЕЗОПАСНОСТИ КОМПАНИИ



КЛЮЧЕВЫЕ ЭЛЕМЕНТЫ РАЗВИТИЯ СТРАТЕГИИ КИБЕРБЕЗОПАСНОСТИ

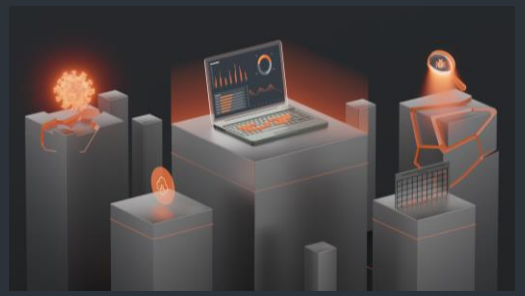


Как вы оцениваете уровень киберзащищенности Корпоративного управления?

1. Выполняем гигиенические требования
2. Проводим тестирование защищенности систем КУ
3. Регулярно поддерживаем осведомленность в вопросах ИБ
4. Не знаю, этим занимаемся другая функция

Берем на себя заботу о комплексной кибербезопасности вашей организации

SOLAR



CLOUD

Наиболее быстрые, простые и эффективные мероприятия по ИБ

- Облачная защита почты
- Security Awareness
- Базовая защита Web
- Мониторинг DNS
- Контроль внешнего периметра
- Базовые сервисы AURA

СЕРВИСЫ

Внешние сервисы по ИБ позволяют работать с задачами требовательными к экспертизе ИБ при её отсутствии in house

- SOLAR MSS
- SOLAR JSOC

ТЕХНОЛОГИИ

On-premise – построение классической ИБ

- Dozor
- inRights
- webProxy
- appScreener
- NGFW и др.

КОНСАЛТИНГ

Стратегия, риски, процессы, методология, построение ИБ и SOC

- Обучение
- Консалтинг
- Построение

35+ решений и услуг

SOLAR

ПОЖАЛУЙСТА,
ПРИМИТЕ УЧАСТИЕ В ОПРОСЕ
О КИБЕРБЕЗОПАСНОСТИ
В КОРПОРАТИВНОМ УПРАВЛЕНИИ

СПАСИБО!

+7 (499) 755-07-70
info@rt-solar.ru

Центральный офис.
125009, Москва,
Никитский переулок, 7с1