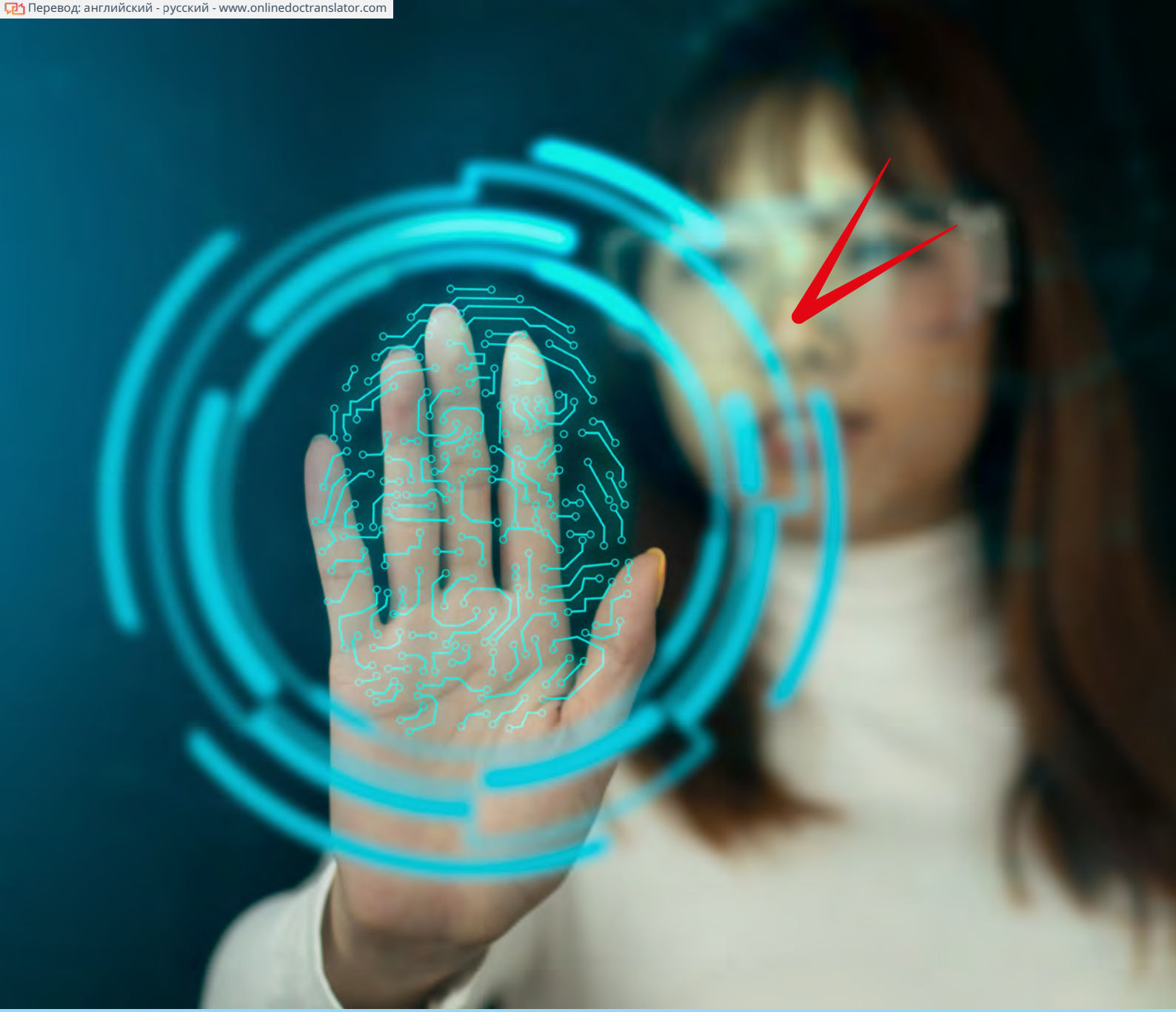


ФАКУЛЬТЕТ КОРПОРАТИВНЫХ ФИНАНСОВ

КИБЕРБЕЗОПАСНОСТЬ В КОРПОРАТИВНЫЕ ФИНАНСЫ

ICAEW

ACT TREASURY EXCELLENCE AS STANDARD

bvca Invested in a better future

Supported by The Law Society

LONDON STOCK EXCHANGE An LSEG Business

THE TAKEOVER PANEL

UK FINANCE

КОРПОРАТИВНОЕ ФИНАНСОВОЕ СООБЩЕСТВО

Для целей данной публикации под корпоративными финансовыми операциями понимаются операции, при которых структура капитала организации может быть изменена для приобретения или продажи элементов этого бизнеса, а также для инвестирования и развития областей бизнеса. К ним относятся рефинансирование вплоть до введения нового капитала или долга.

В число участников сделок – сообщество корпоративных финансов – входят консультанты, руководство компании, корпоративные казначеи, финансовые учреждения и инвесторы (список возможных участников см. на стр. 8–9). Комплексная проверка может проводиться группой, состоящей из внешних консультантов и группы внутреннего аудита приобретателя.

СОДЕРЖАНИЕ

За последнее десятилетие корпорации переместились этот вопрос стоит в списке приоритетов высшего руководства. Сейчас для бизнеса является хорошей практикой оценивать свою кибербезопасность.

рамки.

ПРЕДИСЛОВИЕ

Это второе издание *Кибербезопасность в корпоративных финансах* является отражением того, что за последнее десятилетие кибербезопасность развилась для борьбы с новыми и все более сложными угрозами.

Цель этой публикации – помочь предприятиям – с помощью опыта их консультантов – справиться с рисками, когда они привлекают финансирование, осуществляют слияния и поглощения (M&A) или участвуют в реструктуризации.

Операции корпоративного финансирования являются важной частью экономики. Инвестиции через государственные или частные рынки позволяют предприятиям внедрять инновации или развивать новые отрасли или регионы. Слияния и поглощения обычно повышают конкурентоспособность бизнеса и расширяют предложение его продуктов или услуг.

Успешные операции корпоративного финансирования требуют опыта финансовых и юридических консультантов, финансистов и ряда других консультантов. Поток информации и данных во время сделки делает бизнес уязвимым для нарушений кибербезопасности. Национальный центр кибербезопасности (NCSC) предупредил, что «потенциально разрушительное воздействие» кибератак означает, что их риск должен быть предметом озабоченности советов директоров и иметь такой же приоритет, как финансовые или юридические вопросы.

В этой публикации представлена информация о типах киберрисков, полезных передовых методах защиты от кибератак и о том, как реагировать на кибернарушения в ходе сделки. Он был написан рабочей группой под руководством ICAEW, в которую входит широкий круг сторон, участвующих в транзакциях корпоративного финансирования и кибербезопасности.

В рабочую группу входят Ассоциация корпоративных казначеев, Британская ассоциация прямых и венчурных инвестиций, Лондонская фондовая биржа, Общество юристов, Группа по поглощениям, британские финансовые и профессиональные компании BDO, Deloitte, EY, Grant Thornton, KPMG и PwC. От имени ICAEW я благодарю рабочую группу и NCSC за помощь в разработке этого ценного руководства для сообщества корпоративных финансов.

Дэвид Петри, руководитель отдела корпоративных финансов ICAEW

ЦЕЛЬ РУКОВОДСТВА

Кибербезопасность в корпоративных финансах призван помочь предприятиям понять и управлять киберрисками во время операций корпоративного финансирования.

Любому бизнесу свойственен киберриск. Потенциальные покупатели или инвесторы сталкиваются с конкретными киберрисками, в том числе:

- расширенный и сложный доступ к данным компании во время процесса транзакции, что может сделать бизнес более уязвимым для кибератак;
- повышенный интерес со стороны злоумышленников, которые видят возможность в проводимой транзакции, что может оставить место для упущения средств контроля кибербезопасности;
- приобретение бизнеса, который подвергся кибер-взлому, о котором он не знает и который может повлиять на стоимость этого бизнеса; или
- делиться последствиями исторического кибернарушения после интеграции, такими как репутационный ущерб, техническая инфекция или юридические последствия.

В руководстве освещаются вопросы, которые бизнес должен задавать самому себе, а консультанты должны задавать бизнесу о киберрисках, а также указывают читателям на дальнейшие рекомендации. В нем изложены передовые методы и соображения кибербезопасности, которые предприятиям следует учитывать в контексте транзакции корпоративного финансирования. Хотя эти соображения не являются предписывающими, их следует обсуждать на уровне совета директоров, поскольку они связаны со значительным бизнес-риском.

Существуют конкретные правила отчетности о последствиях кибератак. Однако обязательных норм по управлению киберрисками не существует. В компаниях сектора финансовых услуг регулирующий орган устанавливает требования к операционной устойчивости, которые охватывают различные области, включая кибербезопасность. Многие из предложений руководства уже принимаются организациями как передовая практика управления информацией.

ВВЕДЕНИЕ

Киберриски, с которыми сталкивается бизнес, выросли и продолжают расти. Чтобы защититься от этих растущих угроз системам и данным, организациям необходимо увеличить инвестиции в защитные меры безопасности. Последствия слабой кибербезопасности могут оказаться более дорогостоящими, чем инвестиции.

За последнее десятилетие корпорации подняли этот вопрос в списке приоритетов высшего руководства. Сейчас для предприятий является хорошей практикой оценивать себя на предмет соответствия структурам кибербезопасности, таким как Система киберoценки NCSC. Компании также все чаще стремятся нанять директора по информационной безопасности (CISO), который возьмет на себя ответственность за киберриски и будет отчитываться перед советом директоров.

На самом деле раскрывается очень небольшой процент киберпреступлений, и поэтому крайне важно, чтобы все предприятия серьезно относились к кибербезопасности, чтобы предотвратить успешную атаку. Даже если кибер-злоумышленник будет пойман, затраты компании, скорее всего, не будут возмещены. Операции предприятия могли быть серьезно нарушены, а его репутация на рынке могла серьезно испортиться.

Не менее важно и то, как компания реагирует на кибератаки или утечку данных: несообщение или неразглашение информации могут привести к репутационному ущербу. Клиенты и поставщики, покупающие или продающие компаниям, будут полагаться на безопасность, связанную с этим взаимодействием, для кибербезопасности своего собственного бизнеса. Во всем мире есть признаки того, что передовая практика регулируется, и все предприятия могут принять это во внимание, даже если они не подпадают под обязательные требования.

Когда дело доходит до сделок корпоративного финансирования – государственных или частных слияний и поглощений, инвестиций в акционерный капитал или привлечения долга – управление рисками является ключевой частью процесса. Кибербезопасность подпадает под этот зонтик бизнес-рисков. Точно так же, как с каждым днем это становится все большей долей общего делового риска, так и в транзакциях корпоративного финансирования это большая доля риска.

К корпоративным финансовым операциям применимы три аспекта кибербезопасности. К ним относятся риск до сделки, риск в течение периода транзакции и риск для приобретателя методов и средств контроля кибербезопасности (или их отсутствия), которые они внедряют в свой бизнес после сделки или в которые инвестируют.

В сделке могут участвовать потенциальные приобретатели, их консультанты и кредиторы, имеющие доступ к конфиденциальным данным и информации. Большое количество людей, участвующих в сделке, само по себе является риском. Большинство сторон будут иметь доступ к данным онлайн, и если информация будет перенесена в их собственные системы, это предоставит гораздо больше возможностей для киберзлоумышленников. Осведомленность общественности о транзакции также предупредит потенциальных злоумышленников о том, что в бизнесе происходят значительные изменения.

Транзакции корпоративного финансирования могут включать в себя различные типы информации, включая персональные данные (например, относящиеся к сотрудникам, клиентам или поставщикам) или неличные, но коммерческие данные (например, коммерческую тайну), или даже информацию о конкретных предложениях между различными контрагентами в рамках сделки. сделка. Это может быть очень привлекательно для киберпреступников.

Репутация консультанта по корпоративным финансам зависит от доверия и честности. Кибератака может обесценить репутацию фирмы, что приведет к возможной потере клиентов и/или финансовым потерям, а также к потенциальному нарушению ее деятельности.

Поскольку они будут хранить большие объемы конфиденциальной информации о деятельности, стратегиях и финансовых деталях многих компаний, сообщество корпоративных финансов рассматривается теми, кто имеет злонамеренные намерения, как выгодную возможность получить доступ к информации и использовать ее.

Кибербезопасность подпадает под категорию бизнес-рисков. Точно так же, как с каждым днем это становится все большей долей общего делового риска, так и в транзакциях корпоративного финансирования это большая доля риска.

Внутри пузыря сделок

В любой транзакции контроль над тем, кто имеет доступ к данным и к каким конкретным данным, имеет решающее значение для процесса. Сложность управления этим будет варьироваться в зависимости от типа транзакции.

В частной сделке вне рынка, заключенной между двумя владельцами бизнеса с минимальным объемом комплексной проверки, участвует гораздо меньше людей, чем это было бы типично при трансграничном приобретении на публичном рынке с привлечением капитала и привлечения долга в национально стратегическом или чувствительном секторе.

По мере выполнения транзакции все больше людей будут иметь доступ к данным, которые должны тщательно контролироваться с точки зрения кибербезопасности.

В целом увеличилось количество аутсорсинговых сторон, участвующих в сделке. Понимание зрелости кибербезопасности консультантов и других сторон транзакций, например, проверка сторонних сертификатов, таких как Cyber Essentials Plus или ISO27001, рекомендуется для обеспечения уверенности в том, что они имеют определенный уровень безопасности данных.

Показанные здесь стороны могут быть вовлечены в транзакцию, и в этом случае их следует рассмотреть для включения в список доступа к данным.

БИЗНЕС

- Высшее руководство компаний, участвующих в сделке
- Персонал, занимающий критически важные для сделки роли (финансы, продажи, ИТ)
- Другой ключевой персонал
- Штатные юристы
- Команда внутреннего аудита

ЗАИНТЕРЕСОВАННЫЕ СТОРОНЫ

- Владельцы бизнеса
- Другие миноритарные акционеры бизнеса
- Инвесторы частного или венчурного капитала (VC) в продаваемой компании
- Банкиры и/или кредиторы компании

СОВЕТНИКИ

- Консультант по корпоративным финансам
- Финансовый советник
- Консультанты и консультанты по стратегии
- Правовой советник
- Советник по кибербезопасности
- Налоговый консультант
- Поставщик финансовой экспертизы
- Поставщик коммерческой комплексной экспертизы
- Поставщик комплексной проверки поставщиков
- Долговой консультант
- Советник по вопросам окружающей среды, социальной сферы и управления (ESG)
- Консультанты по связям с общественностью и связям с инвесторами
- Внешний аудитор и бухгалтер компании
- Бухгалтеры по отчетности

ДРУГИЕ ПОСТАВЩИКИ УСЛУГ

- Поставщик виртуальных комнат данных (VDR)
- Финансовые принтеры
- Поставщик облачных услуг
- Рейтинговые агентства
- Управляемые поставщики услуг безопасности
- Андеррайтеры/страховщики

СОВЕТНИКИ НА ПУБЛИЧНОМ РЫНКЕ

- Брокеры
- Спонсоры и ключевые консультанты на Основном рынке
- Назначенные советники на рынке альтернативных инвестиций (AIM)
- Корпоративные консультанты на других рынках

РЕГУЛЯТОРЫ И ПРАВИТЕЛЬСТВО

Другим сторонам, регулирующим и государственным органам может потребоваться предоставление информации во время транзакции в определенных обстоятельствах.

Они могут включать в себя:

- Например, правительственные ведомства для уведомления в рамках Закона о национальной безопасности и инвестициях 2021 года в Великобритании.
- Регуляторы отрасли и регуляторы рынка
- Международные регуляторы о трансграничной сделке
- Фондовые биржи
- Органы кибербезопасности за нарушение кибербезопасности – NCSC в Великобритании не обязывает предприятия сообщать им о нарушениях, но поощряет их делать это.
- Управление комиссара по информации (ICO) за утечку персональных данных в Великобритании

9

ПРИРОДА КИБЕРАТАК

Типы кибератак, реализуемых различными субъектами, постоянно развиваются. Здесь описан неисчерпывающий список атак. Широкий спектр вредоносных действий может поставить под угрозу компьютерные системы и сети, а киберпреступники могут комбинировать различные методы для создания более сложных атак. Предприятия должны сохранять бдительность, а лица, ответственные за кибербезопасность, должны быть в курсе событий. Любая кибератака может повлиять на стоимость бизнеса или быть использована против предприятий или их консультантов в процессе транзакции.

Многие, если не большинство, атак включают в себя элемент социальной инженерии. К контрольным признакам относятся случаи, когда сообщение приходит неожиданно, с необычным вопросом, с просьбой о потенциально вредном действии, или с необычным прикрепленным файлом или, возможно, с ощущением срочности сообщения. Предприятию следует пересмотреть использование любых каналов связи, которые были взломаны, и рассмотреть альтернативные варианты.

Расширенные постоянные угрозы (APT) — это долгосрочные целевые атаки, в которых используются несколько типов атак. Злоумышленник, скорее всего, поддерживаемый государством субъект, но, возможно, и хорошо финансируемая организованная преступная группа, остается в сети в течение длительного периода с целью сбора как можно большего количества информации.

ВРЕДОНОСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Вредоносное программное обеспечение, включая вирусы, черви, трояны, программы-вымогатели, шпионское и рекламное ПО, которые, если их запустить, могут причинить вред разными способами. Это включает в себя блокировку устройства или его непригодность для использования, кражу, удаление или получение контроля над данными, а также получение контроля над устройствами для атаки на другие организации.

программы-вымогатели

Особый тип вредоносного ПО, который предотвращает доступ к устройству и хранящимся на нем данным, обычно путем шифрования файлов. Затем злоумышленник потребует выкуп в обмен на расшифровку.

ФИШИНГ

Нецелевые, вводящие в заблуждение массовые электронные письма, которые запрашивают у получателей конфиденциальную информацию (например, банковские реквизиты) или побуждают их посетить поддельный веб-сайт. Фишинг используется, чтобы убедить людей раскрыть конфиденциальную информацию, такую как пароли или личные данные. Whaling — это целенаправленная фишинговая атака, направленная на руководителей высшего звена. Целенаправленный фишинг — это более целенаправленная форма фишинга, при которой электронное письмо создается так, будто оно отправлено человеком, которого получатель знает и/или которому доверяет. Смишинг (SMS-фишинг) — это атака социальной инженерии, в которой используются поддельные мобильные текстовые сообщения, чтобы заставить людей загрузить вредоносное ПО или поделиться конфиденциальной информацией.

ОТКАЗ В ОБСЛУЖИВАНИИ

Атаки, которые перегружают систему, сеть или веб-сайт большим объемом запросов, делая их недоступными для законных пользователей. Распределенная атака типа «отказ в обслуживании» (DDOS) включает в себя несколько скомпрометированных систем.

АТАКА ЧЕЛОВЕКА В СРЕДНЕМ

Злоумышленник перехватывает и изменяет связь между двумя сторонами без их ведома, возможно, между компанией и ее консультантами, что может привести к краже данных или компрометации.

ДОПОЛНИТЕЛЬНЫЕ ДОКУМЕНТЫ

Злоумышленники используют ранее украденные имена пользователей и пароли для получения несанкционированного доступа к учетным записям на других платформах. Общие пароли или неправильная практика создания новых паролей могут сделать компании и консультантов уязвимыми для подстановки учетных данных во время сделки.

ПОДДЕЛКА ДОМЕННОГО ИМЕНИ (DNS)

Это явление также известно как отравление кэша DNS. Записи на DNS-сервере перенаправляют целевого пользователя на вредоносный веб-сайт, который находится под контролем кибер-злоумышленника.

ВРЕДОНОСНАЯ РЕКЛАМА

Киберпреступники используют вредоносную рекламу для распространения вредоносного ПО или перенаправления пользователей на мошеннические веб-сайты.

Атаки на водопой

Создание поддельного веб-сайта или компрометация настоящего веб-сайта с целью эксплуатации пользователей.

ВЫРАБОТКИ

Злоумышленник выбирает подход, который, по его мнению, с наибольшей вероятностью приведет к выплате, например, «программа-вымогатель как услуга». Это будет включать в себя вымогательство посредством угрозы раскрытия данных или угроз отдельным лицам или их семьям.

КТО И ПОЧЕМУ?

Киберугрозы исходят из постоянно растущего числа источников. Данных и информации сейчас больше, чем когда-либо прежде, а виновники нападения могут руководствоваться множеством факторов, включая финансовую выгоду, шпионаж, хактивизм или стремление к политическому влиянию.

ГОСУДАРСТВЕННЫЕ АКТЕРЫ

Часто хорошо финансируемые, поддерживаемые национальными государствами и обладающие передовыми техническими возможностями, эти субъекты могут ориентироваться на международные транзакции по геополитическим, экономическим или стратегическим причинам. Они могут быть нацелены на сделки, связанные с отраслями, которые правительство, спонсирующее кибератаку, считает национальными важными. Целью будет защита или предоставление преимуществ местным предприятиям, работающим в этой отрасли. Спонсируемые государством субъекты также могут использовать криминальных доверенных лиц для проведения атак.

ОРГАНИЗОВАННЫЕ ПРЕСТУПНЫЕ ГРУППЫ

Мотивированные финансовой выгодой, преступные хакеры, зная о потенциальной транзакции, могут украсть финансовую информацию до того, как транзакция будет объявлена, или осуществить атаки с использованием программ-вымогателей, возможно, в критический момент процесса транзакции.

ХАКТИВИСТЫ

Осуществляя кибератаки по социальным, политическим или экологическим причинам, хактивисты нацелены на компании или стремятся сорвать определенные сделки или транзакции. Они либо хотят повысить осведомленность о своем деле, либо полностью саботировать транзакцию. Они могут портить веб-сайты, разглашать конфиденциальную информацию или нарушать работу онлайн-сервисов.

БИЗНЕС КОНКУРЕНТОВ

Конкуренты в конкурентном процессе слияний и поглощений потенциально могут использовать кибершпионаж для кражи финансовой информации, цен или данных о клиентах, а также конфиденциальной информации (например, интеллектуальной собственности или коммерческой тайны) с целью получения преимущество в переговорах по сделке. Конфиденциальная информация о торгах до того, как она будет обнародована, может стать целью взлома.

ХАКЕРЫ-ЛЮБИТЕЛИ

«Дети-скрипторы» или начинающие хакеры могут иметь меньше технических знаний и ресурсов, чем другие кибер-злоумышленники, но могут эффективно подорвать бизнес, используя уже существующие автоматизированные инструменты или сценарии для запуска атак на компьютерные системы или сети. Их труднее предсказать, они обычно мотивированы простыми личными причинами — развлечься, создать хаос или привлечь внимание.

ИНСАЙДЕРЫ

Это могут быть сотрудники или подрядчики, имеющие авторизованный доступ к системам и данным. Они могут злоупотреблять своим доступом для кражи информации, саботажа систем или утечки конфиденциальных данных. Неправомерное использование может быть непреднамеренным или преднамеренным злонамеренным действием со стороны сотрудника либо из-за его недовольства, либо ради финансовой выгоды. Это можно осуществить через третье лицо.

УПРАВЛЕНИЕ КИБЕРБЕЗОПАСНОСТЬЮ В КОРПОРАТИВНЫХ ФИНАНСАХ

Существуют практические шаги, которые предприятия и другие стороны корпоративных финансовых операций могут предпринять, чтобы защитить себя от киберрисков.

В иллюстративных целях в этом разделе предлагаются конкретные шаги, которые можно предпринять на типичных этапах приобретения бизнеса.

13

ФАЗА 1ПОДГОТОВКА

Тщательная подготовка является ключом к успеху сделки, а вопросы кибербезопасности следует учитывать на ранних этапах процесса. Прежде чем начать сделку, руководство поставщика должно иметь полное представление о рисках для бизнеса. Им следует решить, какую информацию они могут предоставить различным контрагентам, а затем собрать информацию и данные, чтобы позволить всем контрагентам принять обоснованные решения о том, продолжать ли сделку или нет. В этом сборе информации, скорее всего, будут участвовать высшее руководство и ключевые сотрудники, имеющие решающее значение для процесса корпоративных финансов, а также любые действующие стратегические консультанты бизнеса.

Информация, имеющая отношение к транзакции, будет представлять собой сочетание физической и цифровой информации.

На этом этапе стоит подумать о том, должны ли соглашения, такие как соглашения о неразглашении (NDA) или соглашения об обмене данными, содержать положения о защите данных и кибербезопасности.

Многие аспекты бизнеса – продажи, операции, человеческие ресурсы – становятся все более насыщенными данными. Возможно, неудивительно, что процессы слияний и поглощений теперь требуют большего объема данных. Простое объединение данных может предупредить людей, не входящих в рабочую группу по транзакциям, о том, что транзакция запланирована.

ВОПРОСЫ

- Какая информация собирается и где она хранится?
- Кто будет иметь доступ к собираемой информации?
- Четко ли определены их роли?
- Кто будет иметь доступ к неструктурированным данным, а кто будет иметь доступ к структурированным данным?
- Есть ли какие-либо уязвимости или слабые места в ИТ-инфраструктуре какой-либо компании, которые необходимо устранить до слияния?
- Участвуют ли какие-либо сторонние поставщики, поставщики или поставщики услуг в ИТ-инфраструктуре любой компании, и если да, то каковы их методы обеспечения кибербезопасности?
- Каков план реагирования на инциденты и стратегия обеспечения непрерывности бизнеса в случае инцидента кибербезопасности во время или после инвестиций или слияния?
- Какие конфиденциальные данные и системы присутствуют в обеих организациях и какие меры принимаются для их защиты?
- Можно ли применить стратегию классификации данных, при которой данные группируются по таким областям, как высококонфиденциальные, конфиденциальные, внутренние и общедоступные, а меры безопасности ориентированы на наиболее чувствительные?
- Актуальны ли соглашения о неразглашении с поставщиками ИТ-услуг и касаются ли они безопасности любой информации, которой они располагают и которой делятся?
- Каковы ключевые информационные риски в сделке для бизнеса?
- Какие меры безопасности соразмерны рискам и вряд ли приведут к неоправданной задержке транзакции?
- Могут ли данные передаваться анонимно или на агрегированной основе, чтобы снизить риск идентификации личных данных?
- Хранятся ли данные в облаке? Управляются ли эти риски должным образом?
- Какими информационными рисками может оказаться сложно управлять?
- Был ли привлечен к сделке человек, лучше всего понимающий связанные с этим риски, для консультирования по вопросам безопасности и потенциальных угроз?

СООБРАЖЕНИЯ

- Количество лиц, участвующих в сделке, должно тщательно контролироваться. С точки зрения кибербезопасности, чем больше ограничений, тем лучше, а уровень доступа, предоставляемый отдельным лицам, должен быть ясным, точным и соответствовать их обязанностям.
- Принцип наименьших привилегий является лучшей практикой. Это концепция безопасности, согласно которой пользователю предоставляется минимальный уровень доступа, необходимый для выполнения его работы.
- Высшее руководство – в частности, генеральный директор и финансовый директор – будут играть центральную роль на этапе формирования любой сделки. Также будут задействованы некоторые действующие или стратегические советники. Что касается ИТ, данных и кибербезопасности, главный технический директор (CTO), директор по рискам (CRO), директор по информационной безопасности или лицо, ответственное за надзор за кибербезопасностью организации, будут находиться внутри. При необходимости к сделке могут быть привлечены менее высокопоставленные сотрудники, возможно, включая людей, необходимых для сбора данных или помощи в анализе угроз кибербезопасности.
- Предприятия должны иметь коммуникационную стратегию на случай кибер-взлома во время транзакции.
- Встречи следует планировать конфиденциально – например, не следует использовать общие дневники старших сотрудников.
- Каждый член рабочей группы по сделке должен четко понимать уровень своего доступа к данным и быть проинформирован о важности обеспечения отсутствия утечек информации на протяжении всего процесса сделки. Эту процедуру следует документировать, чтобы ее можно было контролировать.
- Руководство бизнеса должно иметь полное представление о том, где находятся все его ИТ-системы и точки их входа, а также характер данных и информации, хранящихся в каждой системе. Компания уже должна иметь эти меры защиты и, в идеале, иметь эту информацию под рукой, регулярно просматривая и обновляя ее.
- Руководству следует подумать о том, где следует хранить данные о сделке и как следует контролировать доступ к ним.
- Поставщик должен решить, какие данные, вероятно, потребуется раскрыть, чтобы максимизировать стоимость продажи, одновременно защищая коммерчески конфиденциальную информацию. Это будет зависеть от характера сделки и ее чувствительности.
- Потенциальный покупатель захочет выяснить, какая информация потребуется для полной обоснованности его предложения. В конечном итоге это может быть список пожеланий: если к бизнесу есть большой интерес, поставщик будет иметь больший контроль над раскрываемой информацией.
- Руководство должно понимать, где находятся ключевые информационные риски в транзакции для их организации. Плохая ИТ-безопасность, скорее всего, затянет переговоры и повлияет на решение покупателей покупать или нет и по какой цене. Уже существующие меры кибербезопасности должны быть пропорциональны управлению рисками, но достаточно гибки, чтобы обеспечить плавное проведение транзакции. Лучше всего сосредоточить меры безопасности на наиболее конфиденциальной информации.
- Необходимо тщательно продумать ИТ-ресурс, необходимый для транзакции. Кто от компании потребуется и как это повлияет на деятельность? Для управления данными, сопоставляемыми для VDR, могут потребоваться дополнительные независимые ИТ-ресурсы или дополнительные ресурсы из отдела финансов, отдела кадров или продаж.
- Предприятие должно иметь безопасное управление информацией и ИТ-процессы, а персонал должен хорошо разбираться в процессах для оперативного сообщения о киберинцидентах. Однако сейчас самое время убедиться, что это происходит на практике, а не только на бумаге, обеспечив полную осведомленность сотрудников о процессе.

ВНЕШНЯЯ ПРОВЕРКА ДЛЯ ПОКУПАТЕЛЯ

На этапе подготовки покупатель или инвестор не будет иметь доступа или будет иметь крайне ограниченный доступ к потенциальному объекту приобретения.

Для сбора информации на этом самом раннем этапе можно провести внешнюю кибер-проверку, известную как разведка с открытым исходным кодом (OSINT). Это не то же самое, что полная комплексная проверка, но она, например, выявит любые зияющие дыры в онлайн-инфраструктуре объекта. Возможно, это единственный доступный подход.

Если присутствие в Интернете или использование технологий является ключом к достижению цели, безопасность вокруг этого в конечном итоге станет основой стоимости сделки. Опять же, возможно, можно использовать что-то вроде мониторинга разведки с открытым исходным кодом.

Могут быть недавние регистрации доменных имен, которые могут привести к подделке доменных имен в процессе слияний и поглощений. Эти регистрации можно искать до начала серьезного процесса.

Поиск в даркнете, проверка информации в базе данных ICO, цифровое профилирование и цифровая разведка, а также любая общедоступная информация, которая может быть доступна, — все это будет частью внешней проверки. Он будет включать в себя проверку:

- взломанные учетные данные и пароли, относящиеся к домену высокого уровня цели, которые могут быть обнаружены в даркнете;
- были ли скомпрометированы адреса электронной почты ключевых лиц;
- случаи утечек данных в отношении домена высокого уровня, которыми также можно торговать в даркнете;
- болтовня на темных веб-сайтах с использованием согласованных условий, связанных с целевым бизнесом; и
- общедоступные точки данных.

Покупатель должен обеспечить актуальность существующих уведомлений о конфиденциальности объекта. Внешний анализ также будет включать анализ внешнего воздействия объекта. Это оценка онлайн-инфраструктуры бизнеса с проверками, включая уровень безопасности связи, технические уязвимости, распространенные открытые порты, проблемы с брандмауэром и небезопасные порталы входа.

В обзоре следует учитывать человеческий фактор киберриска. Есть ли у цели директор по информационной безопасности? Как долго они находятся на посту? Какая у них квалификация и опыт?

Вполне возможно, что внешняя проверка может выявить значительные киберриски, которые станут тревожным сигналом для продолжения сделки.

ДАЛЬНЕЙШАЯ ИНФОРМАЦИЯ

Определение критически важных активов в вашей организации

www.ncsc.gov.uk/collection/board-toolkit/идентификация-the-critical-assets-in-your-organisation

Планирование реагирования на киберинциденты

www.ncsc.gov.uk/collection/board-toolkit/Planning-your-response-to-cyber-incidents

ФАЗА 2 ПРИВЛЕЧЕНИЕ, ОТБОР И НАЗНАЧЕНИЕ ВНЕШНИХ СОВЕТНИКОВ

Внешние консультанты могут быть назначены в тот момент, когда компания решает приступить к сделке. Некоторые консультанты, возможно, были вовлечены в стратегическое мышление, приведшее к сделке.

Возможно, консультант по ИТ или кибербезопасности уже имеется, но если его нет, то сейчас самое время сделать это. Это важная роль, поскольку они могут оказывать помощь, среди прочего, в обеспечении кибербезопасности на протяжении всего процесса.

Мандаты могут быть формализованы и может начаться обмен информацией. Конфиденциальные данные начнут поступать от бизнеса к консультантам, и средства контроля уже должны быть на месте. При назначении внешнего консультанта компания должна получить гарантии своей зрелости в области кибербезопасности и рассмотреть вопрос о необходимости конкретных подходов к управлению данными.

СООБРАЖЕНИЯ

- Обмен информацией требует тщательного управления, чтобы обеспечить ясность относительно того, что является конфиденциальным, как к ней можно получить доступ и как ею можно поделиться. Все участвующие стороны должны подумать, кто в их организациях должен иметь доступ к общей информации и на каком основании.
- Официальные соглашения о том, как информация передается и используется, рекомендуются и считаются общепринятыми.
- Ответственность за надзор за процессом обмена данными и информацией должна быть возложена на конкретных лиц или небольшую команду в каждой организации.
- Рекомендации по выбору VDR можно найти на стр. 25.
- Система входа в VDR будет записывать сведения о том, кто имел доступ к информации с момента их назначения, а также информацию, загруженную в VDR. Однако некоторая информация может быть передана до того, как будет назначен поставщик VDR.
- Необходимо тщательно продумать передаваемую информацию и то, как она будет фильтроваться на каждом этапе процесса. В первую очередь необходимо учитывать, насколько подробная информация будет необходима на начальном этапе, с учетом того, что в конечном итоге будет передано предпочтительному участнику торгов.
- Покупателю и его консультантам необходимо установить, как осуществляется мониторинг информационной безопасности и используются ли системы мониторинга. адекватный.
- Важно установить процедуру и согласовать триггер уведомления всех сторон о кибератаке. Часто стороны создают общий форум для сообщения об инцидентах.
- Возможно, было бы целесообразно полагаться на заявления компаний, консультантов и агентов, участвующих в сделке, о том, что соблюдаются адекватные и подходящие стандарты безопасности. Могут существовать соответствующие отчеты третьих сторон о стандартах безопасности, которые покупатель должен просмотреть.
- Любая транзакция может иметь повышенный риск кибербезопасности. Высшее руководство может быть осведомлено о конкретных атаках в своей отрасли или стране.
- Все стороны должны иметь приемлемые процедуры использования личных или мобильных устройств, принадлежащих компании и используемых за пределами офиса. Необходимо установить новейшие пакеты кибербезопасности и использовать их для обмена информацией. Должны быть ограничения на использование личной электронной почты или приложений для обмена сообщениями для переписки по сделке.
- Должен быть согласован процесс решения проблем кибербезопасности, возникающих в результате комплексной проверки.

ПРОВЕРКА ПОСТАВЩИКОВ И КИБЕРБЕЗОПАСНОСТЬ

Комплексная проверка поставщиков кибербезопасности (VDD) позволяет потенциальным покупателям получить надежную информацию от доверенной третьей стороны в форме отчета, фокус которого определяется поставщиком. Поставщик может принять меры по устранению проблем, поднятых в отчете.

Решение о том, будет ли поставщик взимать комиссию за VDD, часто зависит от характера бизнеса и от того, предусматривается ли продажа через торговлю или через частный акционерный капитал. Если будет принято решение подготовить отчет VDD, кибербезопасность должна стать его частью.

Объем работ VDD охватывает все вопросы, которые покупатель может ожидать от комплексной проверки кибербезопасности и ИТ/технологий, поэтому по сути он будет таким же, как тот, который покупатель заказал бы в отчете о комплексной проверке на стороне покупателя.

ВОПРОСЫ

- Существует ли полис киберстрахования? Если да, то что оно охватывает? И если нет, то почему? Каков лимит покрытия полиса? Подавала ли компания когда-либо претензии по своему полису киберстрахования? Если да, то каков был результат?
- Может ли поставщик предоставить документацию и доказательства своих методов кибербезопасности, такие как политики безопасности, планы реагирования на инциденты, планы обеспечения непрерывности бизнеса и планы аварийного восстановления?
- Какие меры безопасности приняты для защиты конфиденциальных данных и предотвращения несанкционированного доступа?
- Имели ли место в прошлом кибер-нарушения, и если да, то какова была реакция бизнеса, каковы были последствия и как о них сообщалось? Повлияло ли это на полис киберстрахования?
- Была ли проведена независимая оценка рисков кибербезопасности?
- Какие данные являются ключевыми для бизнеса? Например, в процессе продаж, цепочке поставок, разработке продуктов или услуг, финансовой функции или HR?
- Как защищены данные и другие важные активы, такие как интеллектуальная собственность?
- Владеет ли предприятие интеллектуальной собственностью, связанной с его деятельностью?
- Есть ли сторонние поставщики, которые вводят кодирование в ИТ-систему предприятия?
- Насколько бизнес зависит от сторонних услуг?
- Каковы риски, связанные с этими третьими сторонами – например, кибернарушения или неплатежеспособность?
- Какова политика, обучение и культура поставщика в отношении управления кибербезопасностью?
- Какая технология критически важна для бизнеса и как достигается ее устойчивость?
- Будут ли некоторые элементы ИТ- и кибербезопасности требовать капитальных затрат для обеспечения непрерывного управления безопасностью?
- Каковы потенциальные прямые финансовые последствия нарушения и косвенные финансовые последствия репутационного ущерба в результате нарушения?

ЭТАП ЗНАЧАЛЬНЫЕ ПОДХОДЫ

После того, как компания и ее консультант по корпоративным финансам составили список потенциальных покупателей, следующим шагом является обращение к потенциальным покупателям. С точки зрения кибербезопасности, чем меньше эта группа, тем лучше, но это, возможно, не способ максимизировать ценность.

На этом этапе продаваемый бизнес, скорее всего, будет подготовлен к процессу комплексной проверки. В этом подходе могут быть установлены объем, характер и сроки доступа, который будет предоставлен потенциальным участникам торгов.

Некоторыми сделками можно управлять очень жестко, и внутри пузыря сделок находится лишь горстка представителей бизнеса. Если бизнес очень востребован, имеет конфиденциальный IP-адрес или обрабатывает конфиденциальные данные, могут потребоваться более значительные усилия для сохранения контроля над данными.

Все больше сторон начнут получать доступ к информации, и характер этой информации станет более коммерчески конфиденциальным.

СООБРАЖЕНИЯ

- Следует тщательно продумать, как и какая информация предоставляется предприятиям, с которыми осуществляется контакт. Поставщикам необходимы гарантии того, что информация будет обрабатываться безопасно: необходимо согласовать протоколы. Ограничьте количество людей, получающих информацию, насколько это практически возможно, применяя принцип «необходимости знать» или «наименьших привилегий» для обеспечения конфиденциальности в целом и кибербезопасности, стремясь при этом максимизировать ценность, обращаясь ко всем заслуживающим доверия покупателям.
- VDR обеспечит контроль и контроль того, кто имел доступ к данным – сквозное шифрование теперь является стандартной процедурой для VDR. Прежде чем раскрывать конфиденциальную информацию другой стороне, необходимо получить соответствующие разрешения и подписанные соглашения о конфиденциальности, касающиеся доступа к VDR. Они будут включать соглашения о том, какая информация будет передаваться, кому и как она будет использоваться, а также о принципах эскалации нарушений. Он также должен охватывать практику кибербезопасности. Должна передаваться только информация, необходимая для транзакции.
- Должны быть предусмотрены специальные меры контроля в тех редких случаях, когда данные предоставляются в бумажном формате для просмотра в защищенном помещении для сделок.
- Следует найти баланс между необходимостью предоставления адекватной информации и защитой конфиденциальных данных. Передача конкретных конфиденциальных данных только окончательным участникам торгов является обычной практикой.
- Тем, кто работает с конфиденциальными или конфиденциальными данными, рекомендуется заключить необходимые соглашения с этими сторонами.
- Некоторые заинтересованные стороны могут быть из разных юрисдикций. Следует учитывать профиль риска сектора или страны, из которой они родом. Они могут быть более уязвимы для кибератак. Этот сектор может представлять особый местный интерес, например, природные ресурсы или технологии. В сделке могут участвовать активы, которые могут рассматриваться как имеющие стратегическое значение для конкретной страны.
- Необходимо учитывать местные нормативные нормы. – разрешены ли некоторые обычные меры безопасности в юрисдикциях потенциальных претендентов? Например, в некоторых юрисдикциях действуют разные законы об использовании шифрования.

РАБОЧАЯ ПРАКТИКА

После карантина из-за COVID-19 работа на дому (WFH) стала новой нормой для многих людей. После пандемии возросшая гибкость и удобство побудили предприятия (в том числе консультационные) продолжать практику WFH в разной степени. Хотя удаленная работа, которая не обязательно происходит «из дома», не является чем-то новым, ее частота и масштабы намного выше, чем до пандемии.

Должно быть проведено комплексное обучение по вопросам безопасности и осведомленности для персонала, участвующего в операциях и планировании коммуникаций.

Удаленная работа может вызвать обеспокоенность по поводу кибербезопасности, и крайне важно, чтобы соответствующие протоколы были согласованы между всеми сторонами сделки. Виртуальное рабочее пространство может быть более восприимчивым к более широкому спектру киберугроз, а удаленные сотрудники больше не будут защищены мерами безопасности корпоративной сети.

Мобильные устройства, используемые во время сделки, должны быть устройствами компании, контролируемыми и управляемыми компанией, или персональными устройствами с соответствующим мобильным приложением, контролируемым корпорацией.
управленческие решения (MAM).

Типичными минимальными ожидаемыми мерами контроля являются шифрование при хранении, антивирус, централизованный мониторинг, многофакторная аутентификация, контроль доступа и контроль над передаваемыми данными.

Вероятно, существует больший риск для тех, кто работает в кафе, в поезде или самолете, используя общедоступный Wi-Fi. Обучение по вопросам безопасности имеет решающее значение для всех сотрудников, участвующих в сделке.

Точно так же, как важно не отвечать на звонки, связанные со сделкой, в присутствии посторонних лиц, документы, связанные со сделкой, не следует открывать в месте, где неуполномоченные лица могут увидеть содержание документа.

Администраторы с привилегированным доступом к службам или системам, используемым для сделки, очевидно, также будут иметь доступ к информации о сделке и должны знать о своей рабочей среде, а также о рисках работы на дому, а также удаленной работы.

ОСНОВНЫЕ МЕРЫ КИБЕРБЕЗОПАСНОСТИ ДЛЯ РАБОТЫ ВНЕ ОФИСА:

- **Безопасные виртуальные частные сети (VPN).**следует использовать для шифрования данных, передаваемых между удаленными устройствами и корпоративной сетью.

- **Многофакторная аутентификация (MFA).**может предотвратить несанкционированный доступ, даже если учетные данные для входа скомпрометированы.
- **Безопасность конечных точек**, включая антивирусные программы, программы защиты от вредоносного ПО и брандмауэры, должны регулярно обновляться с исправлением известных уязвимостей. Инструменты предотвращения и обнаружения утечек данных могут быть полезны, особенно в случае внутренних угроз.

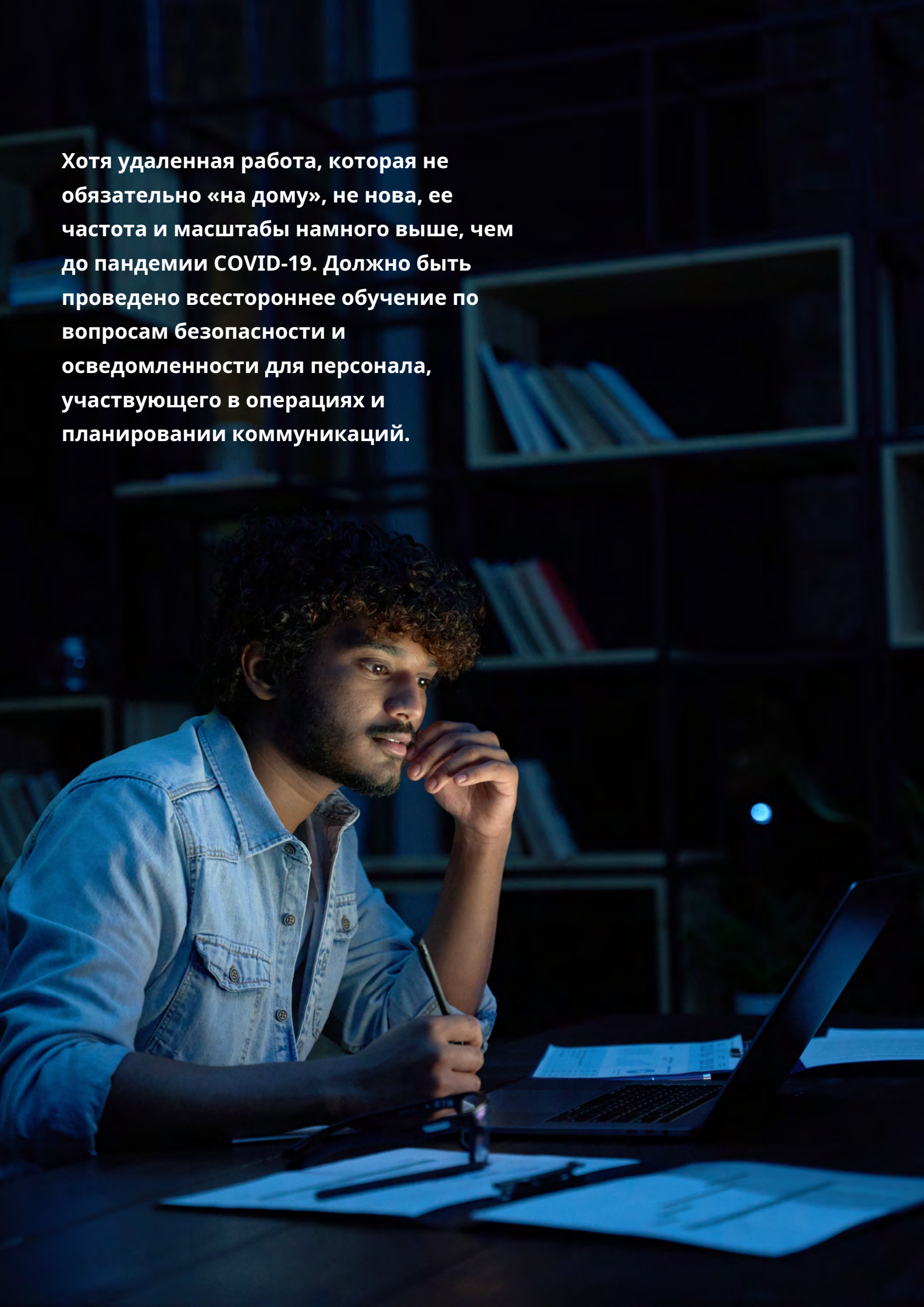
- **Безопасное использование устройства.**следует обеспечить, чтобы рабочие устройства использовались исключительно для профессиональных задач и не использовались совместно. Эти устройства должны автоматически блокироваться после определенного периода бездействия и требовать аутентификации для доступа.
- **Шифрование данных**абсолютно критичен в ситуациях заключения сделок. Шифрование преобразует данные в нечитаемые форматы.
- **Безопасный обмен файлами и совместная работа.** обеспечивает безопасную среду для совместной работы удаленных команд, не подвергая конфиденциальные данные потенциальным взломам.
- **Регулярное резервное копирование**защита от потери данных из-за кибератак, сбоев оборудования или аварий, что позволяет быстро восстановить данные.
- **Планы реагирования на инциденты**должен четко обозначить шаги, которые следует предпринять в случае нарушения кибербезопасности при работе из дома.

ДАЛЬНЕЙШАЯ ИНФОРМАЦИЯ

Работа на дому: подготовка вашей организации и персонала

www.ncsc.gov.uk/guidance/home-working

Хотя удаленная работа, которая не обязательно «на дому», не нова, ее частота и масштабы намного выше, чем до пандемии COVID-19. Должно быть проведено всестороннее обучение по вопросам безопасности и осведомленности для персонала, участвующего в операциях и планировании коммуникаций.



ЭТАП 4 СБОР ИНФОРМАЦИИ О БИЗНЕСЕ

ПОДГОТОВКА БИЗНЕС-ИНФОРМАЦИИ

В рамках мандата на продажу предприятие или его консультант по корпоративным финансам свяжутся с любым количеством потенциальных покупателей по поводу сделки. Владельцы бизнеса, высшее руководство или акционеры и ведущий консультант согласуют список контактов. Вероятно, они имели доступ к некоторой конфиденциальной информации. Некоторые потенциальные покупатели, возможно, начали собственную проверку бизнеса, используя общедоступную информацию или конфиденциальную информацию о бизнесе, принадлежащую третьим лицам. Они также могли провести внешнюю проверку мер контроля кибербезопасности предприятия.

К этому моменту большой объем информации и данных будет собран воедино и затем передан наибольшему числу участников, которые будут участвовать в транзакции в любой момент. Сюда могут входить документы о раскрытии информации, информационные меморандумы, проспекты, пакеты комплексной проверки поставщиков и информация для соответствующих регулирующих органов. Риск того, что посторонние узнают о сделке, является существенным, учитывая участие в ней многочисленных организаций. Риск кибератаки возрастет, если информация о транзакции станет более доступной, поскольку ценные и потенциально конфиденциальные данные и информация будут храниться и распространяться во время процесса.

Нарушения безопасности могут также повлиять на поставщиков, клиентов или сотрудников, а не только на транзакцию. Это может даже повлиять на рынки, в зависимости от характера транзакции и передаваемой информации.

ВОПРОСЫ

- Какую документацию необходимо подготовить для поддержки процесса и максимизации стоимости продажи?
- Какую информацию и данные необходимо включить в документацию? В частности, какая конфиденциальная информация и данные?
- Были ли в недавнем прошлом какие-либо киберинциденты? Как с ними поступили? Какие изменения в процессы были внесены, чтобы защититься от повторения?
- Была ли проведена независимая оценка рисков кибербезопасности?
- Документируются ли продукты и услуги, предоставляемые партнерами/поставщиками?
- Известны ли критически важные активы, хранящие эту информацию?
- Что требуется для удовлетворения соответствующих нормативных и законодательных требований?
- Какая дополнительная информация и данные помогут поддержать более высокую оценку?
- Кто получит документы – потенциальные участники торгов и их консультанты?
- Где будет храниться информация и контролироваться доступ к ней? ВДР? Кто будет контролировать VDR и безопасность доступа и загрузки информации? (См. рамку на стр. 24.)
- Можно ли адаптировать информацию в зависимости от профиля риска каждого получателя или типа получателя?
- Требуются ли особые полномочия для раскрытия информации или данных в отношении клиентов, поставщиков или сотрудников? Увеличивает ли это вероятность нарушения безопасности?
- Нужны ли дополнительные меры защиты для передачи каких-либо данных о клиентах или поставщиках?

СООБРАЖЕНИЯ

- Предприятию следует подумать о том, следует ли предоставлять информацию в разном формате разным потенциальным покупателям. Покупатели прямых инвестиций и торговых компаний, скорее всего, будут иметь немного разные взгляды при рассмотрении приобретения.
- Некоторые стороны могут быть привлекательными покупателями, но считаются высокими рисками, когда речь идет о нарушениях кибербезопасности (или любой утечке, если уж на то пошло). Предоставление им доступа к VDR и содержащимся в нем данным может быть небезопасным. Могут быть альтернативные способы предоставления информации, например, приглашение получить доступ к информации в отдельном контролируемом хранилище данных или в бумажном формате в физической комнате данных.
- Существует ли вероятность того, что частная транзакция станет достоянием общественности во время процесса транзакции? Если это так, бизнес может подвергаться более высокому риску кибератаки против них, и не только на этапе завершения.
- Сторонам сделки всегда следует опасаться риска чрезмерного раскрытия информации. Должны раскрываться только те данные или информация, которые повышают ценность или конкретно позволяют покупателю принять решение о том, следует ли и по какой цене продолжать сделку. Это важно в целом, но особенно актуально в контексте кибербезопасности. Одним из примеров является личная информация, которая может создавать проблемы с защитой данных, но не добавляет никакой ценности к цене продажи и обычно не требуется потенциальным покупателям. Персональные данные, вероятно, являются ключевым риском для многих предприятий.
- Компания должна разработать план интеграции ИТ после сделки, который также включает планы по кибербезопасности и учитывается во всех переходных соглашениях об обслуживании (TSA), связанных с ИТ и кибербезопасностью. АСП должны определить, какие услуги будут предлагаться кем, кому и в какое время.

ПРОВЕРКА КИБЕРБЕЗОПАСНОСТИ

Покупатель мог провести внешнюю проверку (см. стр. 16). В противном случае эти области и любые дополнительные вопросы о кибербезопасности объекта следует задавать в рамках комплексной проверки. Потенциальным покупателям может быть предоставлен отчет VDD, который охватывает объем работ, которые поручил бы типичный покупатель.

Отчет VDD ответит на такие вопросы, как:

- Когда совет в последний раз рассматривал вопросы кибербезопасности?
- Кто в конечном итоге несет ответственность за управление кибербезопасностью в компании?
- Проходила ли компания аудит на соответствие каким-либо основам кибербезопасности, например, системе кибербезопасности Национального института стандартов и технологий США (NIST CSF), системе кибероценки NCSC или принципам «10 шагов к кибербезопасности»?
- Насколько компания уверена в том, что ее самая ценная информация управляется должным образом и защищена от киберугроз?
- Когда компания в последний раз сталкивалась с нарушением кибербезопасности или информационной безопасности?
- Какова была цена нарушения – штраф регулирующих органов?
- Какие шаги предприняла компания для смягчения последствий этого нарушения?

Комплексная проверка обычно предоставляет информацию, которую можно использовать в качестве рычага в переговорах. Различные схемы сертификации кибербезопасности (в том числе Cyber Essentials и Cyber Essentials Plus NCSC) обеспечивают некоторую гарантию, если они существуют. Они гарантируют, что бизнес имеет хотя бы минимальный уровень безопасности, а также дают покупателям уверенность в том, что бизнес серьезно относится к кибербезопасности и работает над защитой своих ИТ. Однако они не гарантируют, что у бизнеса есть какие-либо средства контроля, специфичные для GDPR.

ВИРТУАЛЬНАЯ КОМНАТА ДАННЫХ

Большинство предприятий имеют гораздо больше данных, чем десять лет назад. Транзакции корпоративного финансирования предполагают широкий обмен данными с конечными и потенциальными контрагентами по сделке, а также их консультантами. Предприятие соберет огромное количество данных, которые по самой своей природе играют центральную роль в принятии решения о покупке/продаже и ценообразовании и будут включать конфиденциальную информацию. Он будет сопоставлен и передан соответствующим участникам на первом этапе тендерного процесса.

В процессах комплексной проверки все чаще используются VDR. Передаваемая информация, скорее всего, будет включать данные о ценах, затратах, клиентах и поставщиках, данные о дизайне и спецификациях продукции, а также информацию о сотрудниках личного и финансового характера. Если в процессе участвует конкурент, его доступ к конфиденциальным данным может быть ограничен или отложен до более позднего этапа процесса. Помимо того, что большая часть информации является коммерческой и очень чувствительной для бизнеса, она может подпадать под действие правил защиты данных. Крайне важно, чтобы безопасность оставалась высокой на этом этапе процесса.

Должны быть протоколы относительно того, что люди могут скачивать. Весь доступ к VDR должен регистрироваться вместе с указанием того, для чего люди используют загруженные данные. Следует следовать передовой отраслевой практике по предотвращению потери данных — например, загрузка большого объема информации должна вызывать тревогу.

Протоколами будет управлять тот, кто отвечает за комнату данных по согласованию с поставщиком и его консультантами. Ключевое значение имеет правильный баланс между безопасностью и практичностью. Безопасность должна быть прагматичной и рискованной, чтобы время работы над сделкой не сокращалось. В конечном итоге речь идет об обнаружении аномальных событий. Некоторые из ключевых проблем кибербезопасности, связанных с использованием VDR, включают риски утечки данных и неадекватное шифрование.

Конфиденциальность третьих сторон является еще одним соображением. Например, некоторая информация или данные о поставщиках или клиентах, а также деловые отчеты, написанные профессиональными консультантами, могут подлежать конфиденциальности. Если это абсолютно необходимо для процесса транзакции, следует запросить согласие соответствующей третьей стороны, зная, что этот запрос предупредит поставщика или клиента о предстоящей транзакции.

VDR упростили и повысили эффективность процесса обработки данных, а также во многих отношениях обеспечили больший контроль над данными, которые являются общими, и тем, к каким сторонам предоставляется доступ. Но безопасность полностью зависит от установленных средств контроля. Любые недостатки в системе или процедурах могут привести к нарушениям безопасности. Возможно, было бы легче определить, откуда произошли нарушения, но еще лучше, когда нарушений просто не происходит.

VDR БЕЗОПАСНОСТЬ Y

Ключевым моментом является обеспечение безопасности доступа к помещению данных и использования информации. Компании должны назначить сотрудника или консультанта, который будет активно отслеживать и управлять этим, а также обеспечивать четкий процесс эскалации сообщений о проблемах.

Водяные знаки и динамические водяные знаки

Водяные знаки будут отображать имя получателя, адрес электронной почты или другую идентифицирующую информацию. Динамические водяные знаки уникальны для каждого пользователя, что позволяет отслеживать источник любых утекших документов.

Шифрование данных

В VDR обычно используется шифрование данных, поэтому его может прочитать только целевая аудитория.

Отслеживание активности и журналы аудита

Комплексные журналы отслеживания активности и аудита обеспечивают подробную запись всех взаимодействий пользователей с VDR: доступ к документам, их загрузка, редактирование и действия по совместному использованию.

Многофакторная аутентификация (MFA)

MFA все чаще применяется к доступу к VDR для решения проблемы использования сторонами общих паролей и логинов в комнатах данных. Перед предоставлением доступа также следует провести проверку паролей и логинов, чтобы гарантировать, что никакие логины не используются совместно и что пароли были недавно обновлены.

ВЫБОР ВДР

Для решения проблем кибербезопасности компаниям следует учитывать:

- выбор надежного поставщика VDR с хорошей репутацией в области безопасности;
- внедрение надежных механизмов контроля доступа и аутентификации пользователей;
- шифрование данных в состоянии покоя и во время передачи;
- регулярный мониторинг и аудит действий пользователей в VDR;
- проведение оценки безопасности и тестирования на проникновение в VDR или, что чаще, запрос информации об этом у провайдера VDR;
- информирование пользователей о потенциальных рисках безопасности и передовом опыте;
- наличие строгих соглашений о хранении данных; и
- наличие четко определенного плана реагирования на инциденты.

В конечном счете, сочетание технологий, политик и осведомленности пользователей имеет важное значение для смягчения проблем кибербезопасности, связанных с виртуальными комнатами данных.

Сторонам сделки всегда следует опасаться риска чрезмерного раскрытия информации. Должны раскрываться только те данные или информация, которые повышают ценность или которые необходимы покупателю для принятия решения. Это важно в целом, но особенно актуально в контексте кибербезопасности.

ЭТАП 5 ОКОНЧАНИЕ УСЛОВИЙ СДЕЛКИ

Сейчас сделка находится на продвинутой стадии. Окончательные участники торгов будут стремиться уточнить детали своих предложений. Уровень детализации повысится, и характер передаваемой информации, скорее всего, снова станет весьма конфиденциальным.

Такие участники сделки, как участники торгов, столкнутся с рисками. Были случаи, когда очень конфиденциальная информация участников торгов, такая как цены предложений и условия финансирования, была перехвачена конкурирующими участниками торгов еще до того, как были представлены подробности их окончательного предложения. Это явно наносит ущерб участнику торгов и продавцу, поскольку может поставить под угрозу сделку или повлиять на ее стоимость.

В рамках соглашения должно быть требование о том, что участники торгов не смогут получить доступ к данным после выхода из процесса. Однако профессиональным консультантам может потребоваться сохранить доступ к информации для целей профессионального регулирования. Большинство VDR предлагают возможность блокировать загрузку данных, в том числе посредством шифрования данных.

ВОПРОСЫ

- Насколько высок риск компрометации или кражи на данном этапе? Будет ли она увеличиваться по мере завершения торгов?
- Если до сих пор транзакция имела относительно низкий риск и применялся подход к транзакции с низким уровнем риска, следует ли сейчас ужесточить меры кибербезопасности путем дальнейшего ограничения доступа?
- Нужно ли пересматривать вопросы, поднятые в отношении кибербезопасности на более ранних этапах сделки?
- Каковы последствия нарушения на данном этапе? Каков худший сценарий?
- Как можно эффективно управлять этой ситуацией и смягчить последствия взлома?

СООБРАЖЕНИЯ

- Соглашения о неразглашении и конфиденциальности в отношении особенностей финансирования могут оказаться целесообразными.
- Некоторая информация может храниться в автономном режиме. Одним из примеров может быть аукцион, на котором окончательная сумма в предложении стороны хранится в автономном режиме и представляется старшим членом группы по сделке на собрании.
- Если запрашиваемая информация выходит за рамки стандартной рыночной практики, поставщики следует тщательно рассмотреть вопрос о том, следует ли раскрывать эту информацию.
- При приобретении бизнеса важно провести комплексную проверку его прошлого опыта борьбы с нарушениями кибербезопасности. Многие предприятия и другие организации уже подверглись нападениям. В зависимости от серьезности атак и того, как с ними удалось справиться, это может оказать существенное влияние на стоимость бизнеса или даже на то, стоит ли продолжать транзакцию.
- Многие компании, возможно, еще не следуют практикам, отвечающим ожиданиям или требованиям покупателя. Если да, то следует учитывать риски прошлых или будущих атак, а также меры, которые могут потребоваться для вывода компании на уровень, соответствующий склонности покупателя к риску.
- Если план управления инцидентами для сделки еще не был разработан, возможно, именно на этом этапе его следует составить, особенно если сделка носит резонансный, публичный характер или считается конфиденциальной.
- Участники торгов должны иметь четкую оценку любых необходимых инвестиций немедленно или после завершения строительства. Имея полный доступ к целевому бизнесу, они подтвердят все предыдущие выводы и проведут анализ пробелов. Каков уровень операционных и капитальных затрат на устранение любых пробелов в кибербезопасности, выявленных в ходе комплексной проверки? Подробная информация о проблемах, которые необходимо решить при передаче управления, должна быть включена в TSA.

ПРИМЕР: ПУБЛИЧНАЯ СДЕЛКА

Британский бизнес стал жертвой кибератаки во время процесса транзакции, сразу после того, как об этом стало известно в прессе. Компания была уязвима, поскольку не внедрила эффективную систему безопасности устройств, устаревших ИТ и программного обеспечения. Сделка была продолжена, но эта слабая безопасность оказала значительное влияние на затраты, стоимость и сроки. Это также означало, что на период после приобретения необходимо было выделить серьезные инвестиции и ресурсы.

Управление инцидентами
Должен быть составлен план сделки. Если план еще не разработан, то это можно будет сделать, когда будут окончательно определены условия.

ЭТАП 6ЗАВЕРШЕНИЕ

Транзакция может стать общедоступной только во время или после ее завершения. Если это так, и транзакция по какой-либо причине является конфиденциальной или представляет общественный интерес, информационный риск может усилиться на этом этапе.

Также будет повышенный риск, поскольку средства переводятся для завершения транзакции. Надежные банковские системы снижают риск перехвата перемещаемых средств. Однако в переводе будут задействованы и дополнительные сотрудники, что увеличит число внутренних сотрудников, которые узнают о происходящем.

Кроме того, у компаний будут стратегические документы, подробно описывающие, какую выгоду они могут получить от сделки и их следующие шаги, например, интеграция нового бизнес-подразделения, отделение компании от ее материнской компании, как она выйдет на новые рынки, а также 100-дневные планы. . Большая часть этой информации будет очень ценна для конкурентов и стран, стремящихся защитить и укрепить интересы национальных компаний.

ПРИМЕР: РЕГУЛИРУЕМЫЙ БИЗНЕС СЕКТОРА ТЕЛЕКОММУНИКАЦИЙ

Частное внерыночное приобретение в телекоммуникационном секторе сорвалось в период от подписания до завершения после того, как в ходе комплексной проверки было обнаружено нераскрытое нарушение. О нарушении стало известно, и в дело вмешался регулятор Ofcom. Однако покупатель решил не завершать сделку. Это показало важность тщательной кибер-проверки со стороны покупателя. Это также показало важность того, чтобы бизнес и поставщик действительно были начеку в случае кибератак и обеспечивали полное раскрытие информации.

ПРИМЕР: ОНЛАЙН-ПОТРЕБИТЕЛЬСКИЙ БРЕНД

Потребительский бизнес со значительным присутствием в Интернете не заявлял о предыдущих нарушениях. Это стало известно еще до объявления о сделке. Негативное воздействие на бренд уничтожило его ценность, поскольку кибербезопасность была ключом к их потребительской бизнес-модели.

По завершении должны быть созданы TSA, охватывающие ИТ и кибербезопасность.

ВОПРОСЫ

- Кто будет заниматься переводом средств и подписанием документов?
- Есть ли стороны или отдельные лица, которые до сих пор не участвовали в этом?
- Управлялось ли информационными рисками надлежащим образом на протяжении всей транзакции?
- Является ли транзакция общедоступной?
- Существует ли теперь больший риск для передаваемой и хранимой информации? Какие меры можно было бы практически принять для его защиты?
- Какова политика хранения конфиденциальной информации после завершения?
- Как будут обновляться и проверяться любые ИТ-системы, приобретенные в рамках сделки?
- Были ли системы приобретенных сторон скомпрометированы? Требуются ли на этом этапе более детальные проверки?

СООБРАЖЕНИЯ

- Должен осуществляться постоянный мониторинг доступа к документам, связанным со сделкой.
- Даже после транзакции риск вторжения может сохраняться, например, со стороны вредоносного ПО, которое до сих пор бездействовало в системах.
- Необходимо установить наличие или отсутствие каких-либо недостатков в системах, используемых для перевода и хранения денежных средств, особенно если были открыты счета для конкретных сделок или лимиты платежей были увеличены выше нормального уровня.
- Может возникнуть необходимость пересмотреть политику управления информацией и безопасности во всей организации.
- После сделки расширенная организация может оказаться под повышенной угрозой кибератак, поэтому при необходимости политики и процедуры следует усилить.

ЭТАП 7ИНТЕГРАЦИЯ ПОСЛЕ ЗАВЕРШЕНИЯ

100-дневный план обычно представляет собой подробный план, который имеет покупатель для интеграции своего нового актива в существующий бизнес.

Результаты комплексной проверки могут послужить основой и руководством для любых усилий, связанных с кибербезопасностью после сделки. Разумно далее разбить план интеграции на тактические и стратегические усилия, чтобы обеспечить максимальную защиту на ранних этапах.

Интеграция будет включать в себя объединение ИТ-систем, сетей и данных двух или более организаций, масштабы которого во многом зависят от стратегии объединения двух предприятий. Это может вызвать проблемы.

Если приобретенный бизнес будет отдельной дочерней компанией, то, например, могут быть интегрированы только некоторые элементы финансовой функции. С другой стороны, может потребоваться полное слияние: все ИТ-системы, связанные с персоналом, операциями, дизайном и разработкой продуктов, продажами и финансовыми функциями, должны быть интегрированы. Поглощение может включать что-то среднее между этими двумя крайностями.

Должен осуществляться эффективный надзор со стороны материнской компании независимо от того, является ли приобретенный бизнес интегрированным или самостоятельным дочерним предприятием. Структура управления/отчетности в сфере кибербезопасности должна включать руководство как материнской, так и приобретаемой организации.

Первое действие, которое будет в некоторой степени реализовано до завершения строительства, заключается в утверждении плана интеграции систем после анализа пробелов. Какие системы будут интегрированы и в какой степени? Следующим действием является выделение адекватных ресурсов для проведения интеграции, что может включать привлечение дополнительных внешних ИТ-ресурсов для оказания помощи в этом процессе.

Интеграция может включать в себя двойную эксплуатацию систем в течение определенного периода времени, чтобы гарантировать отсутствие проблем или возможность решения любых возникающих проблем.

Часто это регулируется генеральным соглашением об оказании услуг, но оно должно включать любые услуги, которые приобретаемый бизнес все еще приобретает, и то, как они могут пересекаться с услугами, приобретенными покупателем.

Приобретаемый бизнес может иметь лучшие системы, чем приобретатель, поэтому ИТ приобретателя могут быть интегрированы в системы приобретаемого бизнеса.

В ходе этого процесса необходимо решить несколько проблем кибербезопасности, чтобы обеспечить безопасность и целостность цифровых активов обеих организаций. Сюда входят утечки и потеря данных, несоответствие политик безопасности и средств контроля, а также подверженность уязвимостям.

ПРИМЕР: ИС

Компания была приобретена за стоимость ее интеллектуальной собственности. Однако после завершения было обнаружено, что киберпреступник имел доступ к сети в течение нескольких лет. Киберзлоумышленник продавал IP-адрес, который копировался на другом рынке, чтобы предлагать более дешевые услуги. Это могло быть выявлено в результате более тщательной проверки кибербезопасности или, возможно, в ходе коммерческой проверки на этом рынке.

КИБЕР-ВОПРОСЫ ПОСЛЕ СДЕЛКИ

Есть некоторые конкретные проблемы кибербезопасности, которые могут возникнуть в процессе трансформации после сделки:

- **Безопасность и конфиденциальность данных**: Во время интеграции может потребоваться перенести, совместно использовать или консолидировать данные обеих организаций. Это может привести к раскрытию данных, несанкционированному доступу или неправильному обращению с конфиденциальной информацией, если не будут приняты надлежащие меры безопасности. С командами по защите данных следует консультироваться по вопросам передачи данных, особенно трансграничной, и обеспечивать их соответствие правилам защиты данных.
- **Сегментация сети**: Интеграция различных ИТ-сетей может привести к пробелам в безопасности, если сегментация сети не управляется должным образом. Неспособность изолировать критически важные системы может привести к распространению атак по интегрированной сети.
- **Контроль доступа и управление идентификацией**: Обеспечение надлежащего контроля доступа для сотрудников и систем становится сложным при слиянии двух организаций. Неадекватное управление доступом может привести к несанкционированному доступу, утечке данных и инсайдерским угрозам.
- **Управление уязвимостями**: Объединение ИТ-систем разных предприятий может привести к появлению новых уязвимостей или усугубить существующие. Регулярные оценки уязвимостей и управление исправлениями имеют решающее значение для предотвращения эксплуатации.
- **Культурное и политическое согласование**: Различные предприятия часто имеют разную культуру и политику кибербезопасности. Гармонизация культур и политик важна для всех бизнес-операций в целом и особенно, когда дело касается ИТ, для поддержания единообразных методов кибербезопасности во всей интегрированной организации.

- **Риски третьих лиц и цепочки поставок:**В процессе интеграции могут участвовать общие сторонние поставщики или поставщики, включая подрядчиков. Эти внешние организации могут создать угрозу безопасности, если их стандарты кибербезопасности не будут на должном уровне.
- **Планирование реагирования на инциденты**: Интегрированной организации необходим четко определенный план реагирования на инциденты, учитывающий возросшую сложность и потенциал новых типов атак. Быстрое реагирование и восстановление необходимы для минимизации ущерба.
- **Соблюдение требований и нормативные проблемы**: Различные отрасли и регионы имеют разные требования к соблюдению требований. Интегрирующиеся предприятия должны гарантировать, что их методы обеспечения кибербезопасности соответствуют применимым нормам юрисдикций и отраслей, чтобы избежать каких-либо юридических и финансовых последствий.
- **Мониторинг и обнаружение**: Консолидация ИТ-среды может включать в себя возможности мониторинга и обнаружения для выявления аномального поведения и потенциальных нарушений безопасности в более широкой зоне атак с большим количеством точек входа для кибератак. 100-дневный план может также включать поиск информации в электронной почте или других ИТ-системах на предмет нераскрытых судебных исков против приобретенной компании или нарушений нормативных требований.
- **Безопасная связь**: Каналы связи, созданные во время интеграции, должны быть безопасными, чтобы предотвратить перехват или манипулирование конфиденциальной информацией.
- **Обучение и осведомленность**: Сотрудники обеих организаций должны быть осведомлены о любых новых протоколах безопасности, потенциальных угрозах и важности следования передовым практикам кибербезопасности.
- **Теневые ИТ и неавторизованные системы**: Интеграция предприятий может привести к появлению собственных неавторизованных или неконтролируемых систем, которые могут создать уязвимости в системе безопасности и усложнить управление рисками.
- **Использование социальных сетей**: Необходимо пересмотреть управление использованием социальных сетей, чтобы гарантировать, что приобретенный бизнес не создаст большего потенциала для фишинговых атак.
- **Управление активами**: После интеграции отслеживать все ИТ-активы и системы становится сложнее. Неуправляемые или забытые активы могут стать мишенью для злоумышленников.
- **Непрерывность бизнеса и аварийное восстановление**: Руководство должно обеспечить наличие у интегрированных организаций надежных планов по поддержанию операций в случае киберинцидентов или катастроф.

Чтобы эффективно смягчить эти опасения, организациям крайне важно проводить тщательную оценку рисков, разрабатывать комплексную стратегию кибербезопасности для интеграции и привлекать экспертов и консультантов по кибербезопасности для дополнения внутренних ресурсов, где это необходимо. Им следует постоянно отслеживать и адаптировать меры безопасности по мере продвижения интеграции, чтобы гарантировать, что реальность соответствует теории.

РЕГУЛИРОВАНИЕ КИБЕР И ДАННЫХ

Создание целостного и общепризнанного набора правил кибербезопасности сталкивается со многими проблемами.

К ним относятся:

- разнообразные правовые системы;
- быстрый технологический прогресс;
- соображения суверенитета и конфиденциальности данных;
- отсутствие консенсуса; и
- национальный протекционизм.

В Организации Объединенных Наций есть несколько групп, занимающихся нормами, правилами и принципами ответственного поведения государств в киберпространстве. Целью является создание стабильной и безопасной нормативно-правовой базы в цифровой сфере.

Конвенция Совета Европы о киберпреступности (также известная как Будапештская конвенция) направлена на гармонизацию законов о киберпреступности в разных юрисдикциях и была ратифицирована 70 странами.

Политика НАТО в области киберзащиты направлена на защиту своих сетей и укрепление потенциала коллективной защиты от кибербезопасности. На саммите НАТО 2023 года это было дополнено возможностью виртуальной поддержки киберинцидентов для поддержки национальных мер реагирования на серьезные вредоносные кибердеятельности.

Международная организация по стандартизации и Международная электротехническая комиссия разработали стандарты кибербезопасности, основанные на передовом опыте отрасли.

Региональные соглашения, такие как Общий регламент ЕС по защите данных (GDPR), обеспечивают соблюдение прав на защиту данных и конфиденциальность в ЕС. В Великобритании GDPR реализуется Законом о защите данных 2018 года. Он влияет на глобальные стандарты защиты данных.

Вопросы совместного использования данных могут стать приоритетом, когда слияние или поглощение или другое изменение в организационной структуре предполагает передачу данных в другую организацию.

Приобретатели должны:

- обеспечить, чтобы обмен данными рассматривался как часть комплексной проверки;
- устанавливать и соблюдать законную основу для обмена данными;
- установить, какие данные передаются;
- определить цели, для которых данные были первоначально получены;
- обеспечить соблюдение принципов обработки данных;
- документировать обмен данными;
- обращаться за технической консультацией, прежде чем обмениваться данными, касающимися различных систем; и
- рассмотреть, когда и как субъекты данных будут проинформированы о происходящем.

Возможность продемонстрировать ICO, что соблюдение Закона о защите данных 2018 года является достаточным, должна быть нормальной частью ведения любого бизнеса.

Положения о сетевых и информационных системах (NIS) в Великобритании, а также NIS2 и Закон о проверке цифровых операций (DORA) в ЕС определяют основы операционной устойчивости предприятий.

Растет понимание того, что международное сотрудничество имеет важное значение для эффективной борьбы с киберугрозами. Идеальным сценарием является принятие странами общих рамок для основных принципов, норм и стандартов кибербезопасности. Следует поощрять своевременный и прозрачный обмен информацией об угрозах между странами. Нормы ответственного поведения государства и сотрудничество между правительствами и бизнесом необходимы для решения глобальных проблем кибербезопасности.

УПРАВЛЕНИЕ ПРОИСШЕСТВИЯМИ

Несмотря на все шаги, описанные в этом руководстве, риск кибератаки невозможно исключить. Инциденты кибербезопасности, такие как утечка данных или заражение программами-вымогателями, могут оказать огромное влияние на организацию с точки зрения затрат, производительности, репутации и потери клиентов. Готовность к обнаружению инцидентов и быстрому реагированию на них не позволит злоумышленнику нанести дальнейший ущерб и может снизить финансовые и операционные последствия.

Руководство должно эффективно справиться с инцидентом, что может усложниться, если речь идет о публичной сделке.

У предприятия должен быть план реагирования на инциденты, поскольку он сведет к минимуму воздействие инцидентов и поможет как можно быстрее возобновить нормальную работу. Его следует регулярно пересматривать и поддерживать, чтобы гарантировать его актуальность при изменении ролей и структуры организации.

План реагирования на инциденты должен включать:

- как определяется серьезность инцидента;
- делегирование полномочий по принятию ключевых решений;
- обязанности по установлению связи с ключевыми лицами в организации (включая членов совета директоров), поставщиков и регулирующих органов для обмена информацией об инциденте; и
- четкие роли, обязанности и требования к отчетности.

Во время кризиса качество принятия решений может быть поставлено под угрозу, поэтому жизненно важно, чтобы каждый заранее имел четкое представление о своей роли и ответных мерах организации. Реагирование на инцидент может потребовать принятия важных решений, например, отключать ли системы (например, веб-сайт или другие критически важные для эксплуатации системы). Люди должны знать, какими полномочиями они обладают, особенно если инцидент происходит в нерабочее время.

Мониторинг должен поддерживаться на высоком уровне.

ВОПРОСЫ

- Имеется ли в компании план реагирования на инциденты, который регулярно применяется? Должны быть задействованы члены совета директоров, а также любые консультанты по кибербезопасности и сторонние поставщики, где это применимо.
- Каждый ли член правления понимает, что требуется во время инцидента?
- Если в недавнем прошлом произошел значительный киберинцидент, может ли лицо, ответственное за кибербезопасность, сообщить о достигнутых улучшениях?
- Учитываются ли киберинциденты при разработке планов аварийного восстановления и обеспечения непрерывности бизнеса?
- Знают ли ключевые люди в бизнесе, куда обратиться за помощью в случае киберинцидента?
- Знают ли все сотрудники, к кому обращаться в случае киберинцидента?

СООБРАЖЕНИЯ

- Компания должна была подготовить и согласовать план управления киберинцидентами задолго до атаки. Киберриски должны были быть рассмотрены, обновлены и проведены мероприятия на уровне совета директоров.
- Операционная группа по кибербезопасности увидит первые признаки атаки, такие как увеличение количества предупреждений, указывающих на серьезную угрозу системам.
- Немедленным ответом должно стать сдерживание атаки на сети и системы.
- Следует обращаться к сторонним экспертам и использовать их для получения помощи и совета. У NCSC есть список опытных компаний по реагированию на инциденты с сертификатами (CIR), которые помогают своим клиентам справиться со сложностями серьезного киберинцидента. В дополнение к этому следует использовать Службу указателей киберинцидентов (CISS) для информирования соответствующих органов, таких как правоохранительные органы, ICO и NCSC.
- Чтобы оценить затраты на исправление ситуации, а также на консультации третьих лиц, предприятиям необходимо будет рассмотреть вопрос о выплате злоумышленникам-вымогателям в сравнении с затратами на продолжающиеся сбои в работе и репутационный ущерб. Предприятию следует проконсультироваться по поводу конкретных затрат на исправление ситуации. Рекомендуемая лучшая практика — никогда не платить программам-вымогателям.

ОТЧЕТНОСТЬ О КИБЕР-ИНЦИДЕНТАХ

От предприятий может потребоваться уведомить несколько организаций о кибернарушениях, поскольку разные организации имеют разные полномочия. Если вы не знаете, кому сообщить, Служба указателей киберпроисшествий (CISS) правительства Великобритании предоставит рекомендации. Он ответит на несколько вопросов и определит соответствующие организации, о которых вам необходимо сообщить, а также любые сроки для уведомления о нарушениях.

Об инциденте можно сообщить непосредственно в NCSC, используя егоСообщить о киберинциденте' и занимает около 15 минут. Это следует использовать, если компания предупреждает NCSC только для информации или требует технической помощи. Отчет должен быть составлен, если инцидент затронул:

- данные о сотрудниках, клиентах или поставщиках;
- встроенное, программное или аппаратное обеспечение компьютера организации;
- персональные данные Великобритании, Нормандских островов или острова Мэн.

В отчете должны быть подробно описаны бизнес, основные сведения об инциденте и его последствиях, а также идентификаторы атак. Инциденты кибербезопасности, о которых сообщается с помощью этой формы, круглосуточно отслеживаются офицером NCSC Defense Watch, который постарается ответить при первой же возможности.

Предприятиям необходимо будет сбалансировать ресурсы, необходимые для сбора информации и предотвращения или локализации нарушений.

ДАЛЬНЕЙШАЯ ИНФОРМАЦИЯ

Разработка вашего IR-плана

www.ncsc.gov.uk/collection/incidentmanagement/cyber-incident-response-processes/developing-your-plan

Сообщить о киберинциденте

report.ncsc.gov.uk

РЕАГИРОВАНИЕ НА ИНЦИДЕНТ

Если бизнес подвергается кибератаке, крайне важно отреагировать быстро и эффективно, чтобы минимизировать ущерб и предотвратить дальнейший компрометации. Это применимо как в ходе обычной деятельности, так и в ходе транзакции. Признаками того, что система подверглась кибератаке, являются:

- компьютеры работают медленно;
- пользователи блокируются в своих учетных записях;
- пользователи не могут получить доступ к документам;
- сообщения с требованием выкупа за выпуск файлов;
- люди, получающие странные электронные письма из-за пределов своего домена;
- перенаправленный поиск в Интернете;
- запросы на несанкционированные платежи; и
- необычная активность аккаунта.

Лица, ставшие свидетелями любой такой деятельности, должны связаться с соответствующим персоналом и получить совет относительно конкретных действий, которые им следует предпринять.

КЛЮЧЕВЫЕ ДЕЙСТВИЯ:

- **Изолировать и содержать**: Как только атака обнаружена, пораженная система должна быть изолирована от сети, чтобы злоумышленник не мог переместиться вбок и нанести больший ущерб.
- **Уведомить соответствующий персонал**: ИТ-команда, сотрудники службы безопасности и высшее руководство должны быть проинформированы об атаке. Должны быть установлены четкие линии связи для постоянного обновления.
- **Привлеките команду реагирования на инциденты**: Если есть группа реагирования на инциденты или сторонняя фирма по кибербезопасности, их следует привлечь немедленно. Они могут направлять бизнес в процессе реагирования и помогать ему принимать обоснованные решения.
- **Сохраните доказательства**: Любые потенциальные доказательства, связанные с нападением, должны быть сохранены. Это может иметь решающее значение для идентификации злоумышленника и потенциальных судебных исков.
- **Оцените воздействие**: Необходимо определить масштаб атаки и то, какие данные или системы были скомпрометированы. Это будет определять усилия по реагированию.
- **Уведомить правоохранительные органы**: Если конфиденциальные данные или информация о клиентах были скомпрометированы, регулирующие органы по защите данных должны быть уведомлены соответствующим образом.
- **Уведомить затронутые стороны**: Если данные клиента были скомпрометированы, возможно, потребуется уведомить пострадавших лиц. Требование об уведомлении может варьироваться в зависимости от отрасли и юрисдикции.
- **Исправление уязвимостей**: Уязвимости, которые позволили осуществить атаку, должны быть выявлены и исправлены. Это может включать обновление программного обеспечения, изменение конфигураций или установку исправлений безопасности.
- **Изменить учетные данные**: Пароли и учетные данные доступа для затронутых систем и учетных записей должны быть изменены. Это помогает предотвратить дальнейший несанкционированный доступ.
- **Мониторинг и анализ**: Системы должны постоянно контролироваться на предмет любых признаков продолжающейся вредоносной активности. Атака должна быть проанализирована, чтобы понять тактику, методы и процедуры, используемые злоумышленником.
- **Соблюдение законодательства и нормативных требований**: Убедитесь, что компания соблюдает все законодательные и нормативные требования, связанные с утечками данных и кибератаками.
- **Реализуйте меры по восстановлению**: На основе анализа необходимо принять необходимые меры по исправлению ситуации, чтобы закрыть бреши в безопасности и предотвратить подобные атаки в будущем.
- **Повышение зрелости безопасности**: Инцидент следует использовать как возможность оценить и улучшить общую зрелость безопасности бизнеса. Это может включать в себя переоценку политик безопасности, обучения сотрудников и технологической инфраструктуры.
- **Обновление заинтересованных сторон**: Компания должна информировать сотрудников, клиентов, партнеров и заинтересованные стороны о ситуации, мерах по реагированию и любых изменениях, которые им, возможно, потребуется внести в конечном итоге.
- **Коммуникационная стратегия**у: Должна быть разработана коммуникационная стратегия для управления связями с общественностью и поддержания доверия с клиентами, партнерами и другими сторонами сделки.
- **Учитесь и адаптируйтесь**: После устранения инцидента необходимо провести тщательную проверку. Следует определить, что сработало хорошо, а что можно улучшить, и извлечь уроки для улучшения плана реагирования на инциденты.
- **Обучение персонала**: Сотрудники должны быть обучены передовым методам кибербезопасности, чтобы предотвратить будущие атаки. Сотрудники часто являются первой линией защиты.

СТРАХОВАНИЕ

ЧТО ПОКРЫВАЕТСЯ?

Киберстрахование сейчас является важным покрытием для большинства предприятий, особенно во время любого процесса сделки. Обычно он покрывает прямые убытки, возникшие в результате повреждения или потери информации в ИТ-системах и сетях предприятия в результате кибератаки. Потери могут быть связаны с прямой финансовой кражей или затратами, возникшими в результате кражи данных или повреждения систем.

Он также может покрывать обязательства и расходы, связанные с третьими сторонами в результате кибератаки, такие как расходы на расследование и защиту, гражданский ущерб и компенсационные выплаты пострадавшим сторонам. Как правило, он покрывает большую часть затрат на помощь и восстановление систем после кибератаки.

Как страхование может помочь бизнесу, когда дело касается кибербезопасности?

В преддверии каких-либо инцидентов страховщики обычно предлагают предприятиям доступ к консультациям специалистов для помощи в управлении рисками кибербезопасности, что снижает вероятность возникновения киберинцидентов.

Какое покрытие киберстрахования может быть доступно?

Полис киберстрахования обычно покрывает расходы на устранение любого нарушения безопасности в соответствии с условиями. Затраты могут включать уведомление клиентов об атаке, найм ресурсов для обработки запросов клиентов, консультации по связям с общественностью, ИТ-криминалистику, судебные издержки или консультации по реагированию на запросы регулирующих органов.

Страховщики предложат судебную экспертизу или поддержку после инцидента. Эти специалисты оценят ИТ-системы, определят источник любого нарушения и предложат профилактические меры. Они также проконсультируют о законодательных и нормативных требованиях и о том, как лучше всего уведомить клиентов о любой утечке данных.

Прикрытие от кибервымогательства защитит бизнес в случае злонамеренной атаки, когда киберзлоумышленник требует вознаграждения, взяв под контроль операционные или персональные данные. Обычно речь идет о возмещении сумму выкупа и любые гонорары консультанта, связанные с переговорами и переводом средств. Эта защита особенно актуальна для предприятий, которые работают в Интернете и уязвимы для программ-вымогателей. Прежде чем выплачивать выкуп, об инциденте следует сообщить в полицию и обсудить его со страховщиком предприятия, чтобы, где это возможно, были выполнены все условия возмещения.

NCSC рекомендует не выплачивать выкуп. Предприятиям следует проконсультироваться со своими консультантами, чтобы определить наилучший подход к их конкретным обстоятельствам, и проверить веб-сайт NCSC на наличие последних рекомендаций по вопросам выкупа.

Киберстрахование также может покрыть ущерб цифровым активам. Это особенно важно для предприятий, которые полагаются, например, на онлайн-продажи или автоматизированные производственные системы.

Страхование от перерыва в работе покроет упущенную выгоду во время любого перерыва, который может быть вызван увеличением затрат на ведение бизнеса после инцидента и до возобновления нормального обслуживания.

Что не покрывает киберстрахование?

В политике будет указано, какие юрисдикции она охватывает, а какие исключены. Он часто применяется в Великобритании и ЕС, тогда как Северная Америка часто исключается.

Полис вряд ли покроет претензии сотрудников или подрядчиков в связи с потерей их личной информации в результате утечки данных. Оно не покрывает ущерб физическому имуществу или телесные повреждения в результате киберинцидента.

Потери из-за выхода из строя критически важной национальной инфраструктуры, такой как электричество, газ, вода, спутниковая связь или телекоммуникации, будут исключены. Точно так же, как война и терроризм исключены, поскольку размер риска намного превышает возможности любого отдельного страховщика, так и кибервойна сейчас исключена. Никакая политика не покрывает уголовные, гражданские или нормативные штрафы, штрафы или санкции. И, наконец, киберстрахование не покрывает некомпетентность.

ВОПРОСЫ

- Есть ли у цели киберстрахование?
- Если нет, то почему? Является ли это незастрахованным для кибербезопасности? Почему?
- Если он застрахован, что именно покрывает полис, а что исключается? Какие юрисдикции включены?

- Включает ли полис покрытие киберинцидентов, которые могут возникнуть в процессе слияния или поглощения?
- Насколько дорого стоит киберстрахование?
- Какова дата продления?
- Как на политику влияет смена собственника? Каков период перехода политики?

ПОДАЧА ЗАЯВКИ НА КИБЕРСТРАХОВАНИЕ

Страховщики будут задавать индивидуальные вопросы, относящиеся к конкретному бизнесу. Компания должна позаботиться об ответах и убедиться, что ответы максимально точно отражают реальность кибербезопасности, применяемой в бизнесе.

Страховщик предоставит обширный список требований для наилучшей практики. В нем будет подробно описан подход, который организация уже должна использовать для обеспечения кибербезопасности.

- Осуществляет ли предприятие мониторинговую проверку?
- Существует ли подробная политика кибербезопасности?
- Полностью ли сотрудники осведомлены об этой политике?
- Регулярно ли компания проводит обучение персонала по вопросам кибербезопасности?

Список требований передовой практики страховщика намеренно обширен и исчерпывающ. Руководство должно тщательно изучить условия полиса, детали покрытия и исключения. Страховщики очень четко указывают, что покрывается, а что нет. Обычно в основе политики лежит пункт, в котором говорится, что если они проведут

Если расследование и выяснится, что компания виновата или у нее не было достаточного компенсирующего контроля, компания будет привлечена к ответственности, а страховка будет аннулирована.

На практике это ничем не отличается от любого другого страхования и подчеркивает важность понимания высшим руководством и внедрения протоколов кибербезопасности в их бизнесе.

ДАЛЬНЕЙШАЯ ИНФОРМАЦИЯ

Руководство по киберстрахованию

www.ncsc.gov.uk/guidance/cyberinsurance-guidance

КАКАЯ ЦЕНА?

Несмотря на увеличение числа организаций, занимающихся киберстрахованием, рост спроса и затрат на восстановление опередили предложение страхового покрытия и привели к росту премий.

Киберстрахование как продукт относительно молод, а характер кибератак и потенциальные финансовые последствия продолжают меняться. Страховщики все еще собирают информацию, чтобы понять проблему. Рост финансовых потерь является результатом более изощренных и частых атак, которые становятся все более амбициозными по своим масштабам. Повышенная сложность кибератак привела к увеличению затрат на восстановление. Затраты на кибератаку также могут выходить за рамки очевидных участников.

Стоимость киберстрахования зависит от многих факторов, включая размер и тип бизнеса, сектор, в котором он находится, насколько технологии важны для основной деятельности бизнеса, профиль риска компании и любых сторонних поставщиков услуг, история претензий и требуемый уровень покрытия.

Частный капитал или торговля?

Для большинства крупных частных инвестиционных компаний, желающих инвестировать в бизнес, киберстрахование стало не обсуждаемым вопросом. Это может оказаться сложной задачей для некоторых компаний, поскольку они, возможно, ранее застраховались от кибербезопасности либо потому, что руководство оценило затраты как непомерно высокие, либо потому, что бизнес не смог получить страховку.

Частный акционерный капитал, безусловно, будет нервничать по поводу инвестирования в бизнес, который не имеет покрытия от киберстрахования, и сначала захочет проверить ситуацию, чтобы убедиться, что компания подлежит киберстрахованию.

Поскольку киберстрахование может оказаться дорогостоящим, многие предприятия занимаются самострахованием, беря деньги, которые они обычно хотели бы заплатить за страховые взносы в киберпространстве, и вкладывая их в план «управляемой защиты и реагирования» – упреждающий подход к защите и обнаружению киберстрахования. потенциальные кибератаки и компрометации. Чтобы частный капитал поддерживал такой подход самострахования, бизнесу потребуется такой уровень контроля кибербезопасности, который позволил бы стороннему страховщику предложить ему полис.

Торговые покупатели могут использовать аналогичный подход или попытаться включить приобретенный бизнес в свою собственную политику. Однако объект приобретения должен будет иметь тот же уровень контроля кибербезопасности, что и покупатель, иначе премии могут вырасти непропорционально.

Изменения в сфере регулирования, например, в ЕС, Великобритании и США, увеличили стоимость соблюдения требований и размер потенциальных штрафов, что делает киберстрахование более экономически обоснованным.

Конечно, меры по исправлению ситуации в области кибербезопасности могут снизить киберриски и стоимость киберстрахования.

ДАЛЬНЕЙШАЯ ИНФОРМАЦИЯ

Пять способов распознать социальную инженериюblog.knowbe4.com/five-signs-of-social-engineering

Кибербезопасность: практические советы по защите вашей организации в Интернете www.ncsc.gov.uk/files/NCSC_SME%20Cards.pdf

ICO-вымогатели и соответствие требованиям защиты данныхico.org.uk/for-organisations/uk-gdpr-guidanceand-resources/security/a-guide-to-data-security/security/ransomware-and-data-protectioncompliance/#scenario-7

ДРУГИЕ ССЫЛКИ

https://www.ncsc.gov.uk/section/products-services/cyber-essentials

https://www.ncsc.gov.uk/collection/risk-management

БЛАГОДАРНОСТИ

Мы благодарны следующим лицам, которые щедро пожертвовали свое время и знания своих организаций для разработки этого руководства:

Адам Авардс, UK Finance

Анкит Панди, PwC

Карлтон Ллойд Кристи, LSEG

Шарлотта Девлин, Грант Торнтон

Киаран Харрис, BVCA

Дэвид Петри, ICAEW

Элизабет Хатман, КПМГ

Эстер Маллоу, ICAEW

Ян Уотерворт, AFME

Джеймс Артур, Грант Торнтон

Джеймс Рэшли, PwC

Джейми Айлс, Deloitte

Дженис Вонг, Общество юристов

Джейсон Готшалк, BDO

Джош М., NCSC

Катерина Джоанну, ICAEW

Люк Хеббес, LSEG

Лин Уэбб, EY

Марк Маллен,*Корпоративный финансист*журнал

Маркус Корри, AFME

Марк К1, НЦСК

Мартин Дэвис, Общество юристов

Нареш Аггарвал, АКТ

Роз Грей, Группа по поглощению

Сара Бойс, АСТ

Сьюзан Шарави, Deloitte

Иветт Аллен, Deloitte

О ICAEW

Дипломированные бухгалтеры – это талантливые, этичные и преданные своему делу профессионалы. ICAEW представляет более 202 450 членов и студентов по всему миру. Во всех 100 крупнейших мировых брендах работают дипломированные бухгалтеры ICAEW.*

Основанная в 1880 году, ICAEW имеет долгую историю служения общественным интересам, и мы продолжаем работать с правительствами, регулирующими органами и лидерами бизнеса по всему миру. И, как ведущий мировой регулятор по совершенствованию, мы контролируем и контролируем около 12 000 фирм, обеспечивая их, а также всех членов и студентов ICAEW, соблюдением самых высоких стандартов профессиональной компетентности и поведения.

Мы продвигаем инклюзивность, разнообразие и справедливость и даем талантливым специалистам навыки и ценности, необходимые для построения устойчивых предприятий, экономики и общества, обеспечивая при этом устойчивое управление ресурсами нашей планеты.

ICAEW является первой крупной профессиональной организацией, которая придерживается нулевого уровня выбросов углерода, демонстрируя нашу приверженность решению проблемы изменения климата и поддерживая Цель ООН в области устойчивого развития 13.

ICAEW является одним из основателей организации Chartered Accountants Worldwide (CAW), глобальной семьи, объединяющей более 1,8 миллиона дипломированных бухгалтеров и студентов в более чем 190 странах. Вместе мы поддерживаем, развиваем и продвигаем роль дипломированных бухгалтеров как доверенных бизнес-лидеров, отличителей и консультантов.

Мы считаем, что дипломированная бухгалтерская служба может стать движущей силой позитивных изменений. Делясь своими знаниями, опытом и пониманием, мы можем помочь создать устойчивую экономику и лучшее будущее для всех.

Charteredaccountantsworldwide.com
globalaccountingalliance.com

ICAEW
Зал дипломированных
бухгалтеров Моргейт Плейс
Лондон
EC2R 6EA Великобритания

T +44 (0)20 7920 8100
Электронная почта Generalenquiries@icaew.com
icaew.com

О ФАКУЛЬТЕТЕ КОРПОРАТИВНЫХ ФИНАНСОВ

Факультет корпоративных финансов является центром профессиональных знаний ICAEW в области корпоративных финансов. Он способствует разработке политики и реагирует на консультации международных организаций, правительств, регулирующих органов и других профессиональных организаций. Он предоставляет своим членам широкий спектр услуг, информации, рекомендаций, мероприятий и средств массовой информации, включая высоко ценимый журнал «Корпоративный финансист» и популярную серию руководств по передовой практике.

Тремя основными темами инициатив факультета являются: глобальные инвестиции и слияния и поглощения; Инновации и устойчивое восстановление; и будущие консультативные специалисты.

Международная сеть факультета включает организации-члены и отдельных лиц из крупных групп профессиональных услуг, специализированных консультационных фирм, компаний, банков и альтернативных кредиторов, прямых инвестиций, венчурного капитала, юридических фирм, брокеров, консультантов, политиков и академических экспертов. Более 40% преподавателей являются выходцами из-за пределов ICAEW.

T +44 (0)20 7920 8902 Электронная
почта cff@icaew.com

Chartered Accountants Worldwide
Member

Global Accounting Alliance

ICAEW – это
углеродно-нейтральный

* включает материнские компании. Источник: данные членов ICAEW, март 2023 г., Interbrand, Best Global Brands 2022.