Томас Паренти
Джек Домет

Кибер безопасность

Harvard Business Review Press

Что руководителям нужно знать и делать

Эта книга принадлежит

Контакты владельца

Thomas J. Parenty
Jack J. Domet

A LEADER'S GUIDE TO CYBERSECURITY

WHY BOARDS NEED TO LEAD — AND HOW TO DO IT

HARVARD BUSINESS REVIEW PRESS
BOSTON, MA

Томас Паренти
Джек Домет

КИБЕР БЕЗОПАСНОСТЬ

Что руководителям нужно знать и делать

Перевод с английского
Эльвиры Кондуковой и Светланы Давыдовой

Москва
«МАНН, ИВАНОВ И ФЕРБЕР»
2021

УДК 004.056:004.49
ББК 67.408.135.2
П18

Научный редактор Екатерина Гришина

Издано с разрешения Projex International LLC acting jointly with Alexander Korzhenevski Agency

На русском языке публикуется впервые

Паренти, Томас

П18 Кибербезопасность. Что руководителям нужно знать и делать / Томас Паренти, Джек Домет ; пер. с англ. Э. Кондуковой, С. Давыдовой. – Москва : Манн, Иванов и Фербер, 2021. – 272 с. : ил.

ISBN 978-5-00169-461-8

Компании тратят огромные средства, чтобы их активы и данные были под надежной защитой, однако киберриски только возрастают, что лишь усугубляет проблему. И никакие новые технологии или раздувание бюджета не в силах переломить эту ситуацию.

Томас Паренти и Джек Домет больше 30 лет занимаются вопросами кибербезопасности. В этом руководстве они систематизируют свой опыт, описывают все известные и популярные инструменты, обстоятельно объясняя, почему одни работают, а другие нет, а также делятся передовыми практиками.

Вы убедитесь, что защита от кибератак не сводится к набору задач для IT-отдела, а, наоборот, предполагает развертывание надежной сети, охватывающей все, что происходит в компании, – от стратегии и ключевых видов деятельности до бизнес-модели и рабочих процессов.

Если вы руководитель и хотите стать лидером по кибербезопасности – эта книга для вас.

УДК 004.056:004.49
ББК 67.408.135.2

ISBN 978-5-00169-461-8

Посвящается Копернику

Оглавление

Предисловие партнера издания

Мы все время думаем о безопасности. Мы хотим, чтобы наши дети ходили в безопасную школу, жили в безопасном районе. Мы покупаем детские кресла в машины и надеваем на малышей шлем, когда отпускаем их кататься на велосипеде. Мы ищем экологически безопасные продукты, считаем «химию» опасной и остерегаемся ее. Мы не смотрим близко телевизор, надеваем шапку, когда холодно, и переходим улицу по пешеходному переходу – все ради безопасности.

В обычной жизни это происходит на автомате, но мы учимся первым делом определять угрозу. Шлем на ребенке, когда он катается на велосипеде, нужен потому, что существует угроза упасть. На улице угроза – это автомобиль, а в районе – хулиганы.

И, как показывает опыт, без преувеличения, всего человечества, всякий раз изменение уклада жизни, создание чего-то нового, развитие жизни привносят новые, ранее неизвестные угрозы.

Когда-то наши очень далекие предки научились добывать и поддерживать огонь. В каком-то смысле это создало

угрозу пожаров. Промышленная революция навсегда изменила наш мир, ведь благодаря ей появилось все то, чем мы сейчас пользуемся. Но в то же время она породила и новые угрозы – аварии и травматизм на производстве, техногенные катастрофы, загрязнение окружающей среды. Автомобили перевернули наш мир и тоже породили новые угрозы – аварии, смерти на дорогах, загрязнение воздуха и ряд других.

Все эти угрозы оказались новыми для своего времени. И в этом их отличительная особенность. Первое время мало кто придавал существенное значение возросшей смертности на дорогах в результате автомобильных аварий. И понимание, как быть с этой проблемой, пришло далеко не сразу, ведь ни у кого не было готового решения, как с этой угрозой бороться, – она была новая для всего мира. Наша нынешняя эра – информационная – не исключение. Она тоже привносит свои и, что самое важное, неизвестные ранее угрозы.

Но есть еще один важный фактор угроз. С появлением каждой следующей обнаруживалось, что одни слои общества оказывались менее подготовлены и имели меньшую способность адаптироваться и противостоять угрозе, тогда как другие, наоборот, были более подготовлены и обладали большими возможностями справиться с ней. В наше время это звучит как само собой разумеющееся, но раньше было не так: риск пострадать в дорожно-транспортном происшествии выше у тех, кто едет в автомобиле или находится где-то рядом. Сейчас это всем понятно. В начале же XX века пешеходы и не думали, что они тоже «участники дорожного движения» и что в связи с этим количество

угроз для них возросло. Первые эскалаторы воспринимались как аттракцион, и люди, пользовавшиеся ими, были сродни счастливчикам, которым довелось прокатиться на новом инженерном сооружении, а не пользователями технического средства повышенной опасности, как сейчас.

Информационные технологии тоже порождают угрозы. Старое доброе «упал сервер» и «тыкнуть мышкой» живет уже более 25 лет, но тем не менее для многих остается непонятным жаргоном. Чего уж говорить о фишинге, SSL и сертификатах подписи. Отчасти это объясняется стремительностью развития IT, а отчасти их сложностью — ведь информационные технологии трудно визуализировать и представить. Это сплошь абстракции и железная, но порой очень сложная логика.

И основная категория риска в информационных технологиях — это люди, для которых все это не является профессией или хобби. Как следствие, они не владеют специализированными терминами и не способны оценить, какие риски могут нести те действия, которые они совершают. В особую подкатегорию можно выделить людей пожилого возраста: у многих из них консерватизм и традиции побеждают желание держать руку на пульсе и поспевать за стремительными переменами.

Эта книга поможет новичкам, желающим больше понимать об информационной безопасности, продвинуться в своих познаниях в этой области. Она будет полезна и опытным профессионалам, которые почерпнут в ней много интересных деталей и новых подходов к привычным вещам.

В любом случае, кем бы ни был читатель, занимаясь или просто интересуясь вопросами информационной безопасности, мы делаем этот мир лучше и добрее. Любые знания в этой области помогут обществу развиваться дальше, а незащищенным гражданам жить чуточку спокойнее.

Фёдор Дбар,
коммерческий директор компании «Код Безопасности»

Введение

Стратегическое руководство по цифровому управлению

За последнее десятилетие цифровизация окончательно захватила мир. И хотя правительства, компании и общественные организации тратят миллиарды долларов на кибербезопасность, финансовые последствия киберпреступлений растут пропорционально инвестициям в меры защиты.

Открыв газету в любой точке мира, вы наверняка найдете историю о какой-нибудь сокрушительной кибератаке. Например, в 2016 году, в результате киберограбления, Центробанк в Бангладеш лишился $81 млн — значительной части валютных резервов страны. В 2017 году группировка The Shadow Brokers (или кто-то от ее имени) похитила несколько важных разработок Агентства национальной безопасности США. Среди украденного был инструмент EternalBlue, который хакеры затем использовали, чтобы запустить вирус WannaCry. Этот червь заразил

более 230 000 компьютерных систем в 150 странах, а убытки, по оценкам, составили около $4 млрд. В 2018 году гостиничная империя Marriott объявила о взломе своей системы бронирования Starwood и об утечке личной и финансовой информации 500 млн гостей. А взлом индийской национальной идентификационной базы Aadhaar позволил хакерам украсть личные, финансовые и биометрические данные практически всего населения страны – 1,1 млрд граждан.

Очевидно, с этим нужно что-то делать.

Наш опыт консультирования клиентов по всему миру показал: ключевая причина, по которой миллиардные инвестиции в кибербезопасность до сих пор не окупились, – все упорно зацикливаются на технологической стороне проблемы. В центре внимания – главным образом компьютеры и компьютерные системы, а также их уязвимости, а не бизнес-риски для компаний и стратегическое управление в целом.

Конечно, у такого подхода есть причины – как исторические, так и логические. IT-специалисты первыми столкнулись с вопросами кибербезопасности. Они сосредоточились на особенностях атак и механизмах защиты, а также на том, как сделать операционную систему менее уязвимой. Да и в принципе без компьютеров не было бы киберрисков, так что технологические аспекты, несомненно, важны. Излишний фокус на устранении уязвимостей соблазнительно опасен именно потому, что в этом есть резон. Но по ряду причин акцент на технологиях в конечном счете не помогает повысить кибербезопасность, а скорее

наоборот – подрывает надежную защиту, как бы парадоксально это ни звучало.

Ни у одной компании нет ресурсов, чтобы решить все технологические проблемы в этой области, да и не все исправления одинаково ценны. Только определив ключевые процессы вашего бизнеса и проанализировав, как киберугрозы могут им навредить, вы расставите приоритеты грамотно и сумеете принять меры. Кроме того, когда специалисты по кибербезопасности вникнут, как именно функционирует ваш бизнес, они тоже смогут действовать правильнее. В частности, им удастся избежать решений и действий, которые, какими бы благими намерениями ни диктовались, не снижают рисков, а порой, наоборот, увеличивают их и ломают отлаженные бизнес-процессы.

Специфика технологий кибербезопасности и язык, которым о них говорят, – зачастую понятный только профессионалам – тоже играют свою роль. Технически не подготовленным стейкхолдерам, например руководству компании, нередко трудно вставить свое веское слово при обсуждении киберугроз. Но если дискуссии будут начинаться с защиты как операционной, так и стратегической деятельности, наиболее ценной для вашего бизнеса, ситуация изменится. Это позволит вам и вашим коллегам по совету директоров контролировать управление киберрисками.

Только начав с оценки критически важной бизнес-деятельности, а не с технологий, ваша компания поймет, как выстроить адекватную систему кибербезопасности: какие программы купить и какие действия предпринять.

Излишний фокус на технологиях также отвлекает внимание от других факторов, влияющих на эффективность продуктов кибербезопасности в значительно большей степени, чем сложность их функционала. Сюда относятся мотивация, стимулы и приоритеты людей, которые пользуются этими продуктами или играют иную роль в защите компании.

Мы не раз сталкивались с ситуациями, когда, например, сотрудники сознательно обходили меры безопасности, мешающие им работать. Иногда мы также наблюдали, как специалисты ослабляли киберзащиту, чтобы избежать дополнительной нагрузки и давления коллег: высокий уровень кибербезопасности вызывал ложные тревоги или нарушал бизнес-процессы. То, насколько эффективно работает команда кибербезопасности, зависит от ее места в структуре компании. Если у руководства другие приоритеты, сотрудники, отвечающие за борьбу с киберугрозами, могут не получить необходимого финансирования и полномочий.

Если компания собирается совершенствовать киберзащиту, необходим правильный катализатор — участие руководства, ваше участие в том числе. Мы считаем, что в основе многих проблем кибербезопасности лежат слабые стороны корпоративного управления, а значит, повысить его эффективность — лучший способ нивелировать риски.

Управление кибербезопасностью начинается «сверху», с совета директоров и топ-менеджмента. Отсюда оно распространяется на всю организацию, что влечет за собой как смещение ответственности (от технических специалистов к высшему руководству), так и смену угла зрения

(с технологий на бизнес, его процессы, стратегию и крупные ставки, а также риски, вызванные кибератаками).

Вы представляете ключевые интересы компании в долгосрочной перспективе. Вы отвечаете за ее состояние, развитие и рост. У вас есть полномочия, чтобы инициировать перемены в общей стратегии кибербезопасности. Вы можете вмешаться там, где не справляются рыночные механизмы и не помогают правительственные постановления.

Стратегическое цифровое управление

Многие директора говорили нам, что кибербезопасность — сфера сложная, если не непостижимая. Они признавались, что принимают инвестиционные решения, не опираясь на надежные данные и не до конца понимая суть тех или иных технологий. Многие считают, что кривая обучаемости в этой области слишком крута; другие рассказывают, что не знают, какие вопросы задавать и как оценивать ответы. Часто руководству приходится полагаться на пространные заявления IT-отдела или команды кибербезопасности в духе «здесь все в порядке, но нужно поработать там». Подкованные в технологиях руководители, возможно, и занимаются проблемой грамотнее, но далеко не всегда.

Так не должно быть, но вы можете улучшить ситуацию, просто выполняя свои обязанности по управлению и контролю. Надзор за кибербезопасностью в чем-то схож с «эффектом наблюдателя» в квантовой физике, когда

наблюдение за событием влияет на его результат. Ваши запросы мотивируют компанию обращать внимание на соответствующие факторы и процессы и проводить анализ, до которого в противном случае не дошли бы руки.

Взяв на себя ответственность за кибербезопасность, вы не должны нести ее как бремя. Несмотря на расхожее мнение, что это сложная для понимания сфера, наш опыт показывает: она — удел не только технических гениев. Хотя погружение в вопрос, безусловно, важно, для эффективного управления и контроля вам не нужно глубоко разбираться в проблемах кибербезопасности. Получение соответствующего образования даст ограниченные преимущества, отнимет много времени — и не факт, что поможет на практике. А вот в ходе привычной деятельности в совете директоров вы точно приобретете необходимые знания.

Чтобы помочь вам, мы разработали руководство по стратегическому управлению в цифровой сфере. Наша система включает четыре базовых принципа, три ключевые задачи и несколько памяток-помощников. Принципы помогут вам сориентироваться при обсуждении вопросов кибербезопасности и принятии решений. Задачи касаются наиболее важных действий, которые компания должна предпринять, и дают основу для контроля. Памятки содержат ряд вопросов-якорей, облегчающих исполнение ваших надзорных функций. Внедрив эту систему цифрового управления, вы станете лидером в области кибербезопасности и научитесь ставить перед коллегами правильные вопросы, а также интерпретировать информацию, которую они вам предоставляют.

Принципы

— *Если вы не понимаете, значит, вам плохо объяснили.* Руководство и сотрудники вашего отдела кибербезопасности обязаны предоставлять вам материалы и отчеты в форме, доступной пониманию неспециалистов.

— *На кону всегда бизнес.* Все вопросы кибербезопасности начинаются и заканчиваются проблемами бизнеса и рисками, связанными с его процессами и стратегией, а не с компьютерами и их уязвимостями.

— *Кибербезопасность должна быть у всех на слуху.* Рабочие процессы компании, ее деятельность и структура – все должно быть неотрывно от заботы о кибербезопасности. Выводите ее из тени, она – не просто часть чьего-то функционала.

— *Не забывайте о мотивации.* Знайте, чего хотят ваши сотрудники. Правильно мотивируйте их. Пусть они тоже будут заинтересованы в заботе о кибербезопасности.

Задачи

Управление киберрисками

Это наиболее важная задача; все остальные опираются на нее и зависят от четкого понимания последствий

кибератак. Эффективное управление киберрисками требует грамотной оценки взаимосвязей между наиболее значимыми бизнес-рисками для компании, типами кибератак, которые могут их вызвать, и мерами, способными предотвратить или минимизировать эти риски. Эффективный контроль включает выявление и учет всех нетехнических факторов, которые могут свести на нет даже самые мощные технологии.

Защита компании

Вы существенно укрепите систему кибербезопасности, если задействуете дополнительные инструменты: грамотный подход к организационной структуре компании, выстраиванию ее рабочих процессов и корпоративной культуры. Не менее важно учитывать мотивацию и интересы сотрудников, а процесс оценки угроз должен предполагать ответы на вопросы: «Насколько мы теперь в безопасности?» и «Насколько мы будем в безопасности завтра?» Корректный статус команды кибербезопасности в структуре компании и понимание, нуждаетесь ли вы и ваши коллеги по совету директоров в дополнительной киберэкспертизе, — также важные факторы. Именно от механизмов подотчетности зависит ваша возможность получать ценную информацию, необходимую для принятия обоснованных решений.

Лидерство в кризисе

Хотя компания не должна пренебрегать превентивными и защитными мерами, лучше быть во всеоружии: вдруг кризис, вызванный кибератакой, все же грянет? Здесь помогут планирование, подготовка и координация в двух взаимосвязанных областях. Во-первых, компании необходимо научиться распознавать атаки и защищаться от них – для этого нужна квалифицированная команда реагирования. Во-вторых, топ-менеджеры должны встать у руля во время киберкризиса, то есть понимать, как относиться к тем или иным ситуациям и какие решения принимать. Используя собранную информацию и материалы, разработанные в процессе снижения рисков, руководители смогут наметить план действий заранее.

Памятки

Каждая памятка состоит из четырех элементов. Первый – запрос, касающийся той или иной задачи в области кибербезопасности. Формулировки приведены так, чтобы вы могли сразу их использовать. Второй элемент – краткое обоснование запроса с точки зрения защиты вашей компании и деятельности по управлению киберрисками. Далее приводятся примеры и описания документов, отвечающих запросу. Последний элемент – действия, рекомендованные для контроля запроса. Чтобы использовать памятки, опыт в технической сфере не нужен. Зато эти материалы помогут

вам всесторонне оценить эффективность управления в области кибербезопасности и киберрисков.

Как пользоваться книгой

Мы написали эту книгу, чтобы помочь вам как руководителю компании осуществлять контроль над политикой кибербезопасности. Поскольку эта обязанность требует участия многих ваших коллег, здесь также есть рекомендации исполнительным директорам и руководителям, отвечающим за кибербезопасность, — как по защите компании, так и по выполнению их обязанностей перед вами и советом директоров. Принципы и советы, изложенные в книге, применимы и в других типах организаций, в том числе государственных учреждениях и некоммерческих организациях.

В книге четыре раздела. Каждый вносит вклад в ваше понимание кибербезопасности и того, чему нужно уделить внимание в этой сфере.

— Первая часть, «Проблемы», раскрывает причины, по которым меры в области кибербезопасности порой неэффективны, а разобраться в теме так сложно. Вы сможете критически взглянуть на решения, принимаемые вашей компанией.

— Следующая часть рассказывает о четырех принципах цифрового управления. Ими вы сможете руководствоваться, принимая решения в области

кибербезопасности, — особенно если столкнетесь с новыми и неожиданными проблемами.

— Третья часть посвящена основополагающим задачам в области кибербезопасности. Ваша компания должна их решать, а вы — контролировать процесс. Каждая задача затрагивает важнейшие факторы, необходимые для достижения успеха, но часто упускаемые из виду.

— Заключительный раздел, «Памятки», включает подробные таблицы, которые помогут вам проверить, как компания справляется с задачами.

В книге мы также расскажем о нашумевших киберпреступлениях и приведем примеры из собственного опыта работы. Все это призвано показать, как принципы и методы цифрового управления работают в реальной жизни, а также к каким последствиям может привести невнимательное отношение к ним.

Часть I

Проблемы

Начнем с двух вопросов

— *Вы замечали, что общеизвестная информация о кибербезопасности порой выглядит сомнительно, но эти сомнения трудно конкретизировать?*
— *Приходило ли вам в голову, что о киберугрозах обычно говорят языком, малопонятным для простых смертных, и это неоправданно?*

Если ваш ответ «да», то интуиция вас не подвела. Разница между тем, что кажется истинным в области кибербезопасности, и тем, что таковым является, огромна. Прежде чем перейти к принципам разумного управления в цифровой сфере и поговорить о связанной с этим ответственности, давайте сдернем завесу тайны с бытующих здесь банальных сентенций, теневых факторов и распространенных заблуждений. Именно они напускают тумана и превращают обсуждение проблем кибербезопасности в непроходимый темный лес.

Глава 1

Банальные сентенции

Сфера кибербезопасности переполнена суждениями, которые, может, и звучат разумно и убедительно, но на практике бесполезны и даже контрпродуктивны. К сожалению, их так часто повторяют, что они обрели статус непреложных истин и искажают многие представления об этой сфере и способах добиться в ней эффективных результатов.

Итак, вот три главных, наиболее вредных киберпредрассудка:

— Это все человеческий фактор!
— Спасайте бриллианты короны!
— Киберугрозы не стоят на месте!

Это все человеческий фактор!

«Проблема не в технологиях, а в людях». Иногда это утверждение звучит иначе: «В сфере кибербезопасности человек — самое слабое звено». Хотя люди время от времени забывают флешки в USB-портах, открывают письма

с вредоносными вложениями и в целом ведут себя беспечно, не стоит сводить все беды к этому. За многие возникающие проблемы ответственны сами специалисты по кибербезопасности: они не способны понять поведение рядового пользователя в цифровом мире, к тому же существующая система поощрения недостаточно мотивирует их на качественную работу.

Для полноты картины сравним, как человеческий фактор влияет на обеспечение безопасности в повседневной жизни и в мире компьютерных сетей. Проверим тезис на прочность.

В офлайне мы давно поняли, что определенным сферам, локациям и ситуациям присущи повышенные риски, которым люди не всегда уделяют должное внимание. Чтобы нивелировать влияние опасных факторов, мы принимаем меры по защите и стремимся минимизировать возможный ущерб: например, устанавливаем отбойники на шоссе и «лежачих полицейских» возле школ. Мы учитываем поведенческие паттерны и не обвиняем людей в том, что они... скажем так, порой безответственны и неосторожны. Мы не ожидаем, что они исправятся только потому, что мы рекомендуем это сделать.

В цифровом мире все с точностью до наоборот: мы редко пытаемся уберечь или подстраховать людей от ошибок и необдуманных действий. Зато беспощадно ругаем их за случившееся, а в качестве решения проблемы предлагаем изучить правила компьютерной безопасности.

Тайна потерянной флешки

В 2007–2008 годах в Гонконге имело место девять случаев непреднамеренной утраты личных и медицинских данных граждан – в общей сложности 16 000 человек. В итоге Больничное управление Гонконга обратилось к нам за помощью. Перед нами стояла задача – разобраться в истинных причинах потери данных, скорректировать политику конфиденциальности и предложить меры по улучшению системы безопасности[1].

В одном случае сотрудница администрации в Больнице принца Уэльского (район Новые Территории) оставила флешку в такси. Сделать вывод, что всему виной отсутствие базовых знаний о кибербезопасности, так же легко, как во время просмотра фильма предположить, что человек с пистолетом, стоящий над трупом, и есть убийца.

Чтобы лучше разобраться в причинах инцидента, мы задали девушке всего два вопроса.

1. ***В чем состоят ваши рабочие обязанности?***

Как оказалось, сотрудница выставляла другим госпиталям счета за проведение клинических исследований в лабораториях больницы.

2. ***Зачем вы копируете информацию на флешку?***

В действиях девушки не было ничего ужасного; они диктовались логикой; многие сотрудники крупных компаний сталкиваются с подобным. На ее компьютере отсутствовала нужная для работы программа Excel. Поэтому она копировала

[1] "Report of the Hospital Authority Taskforce on Patient Data Security and Privacy," http://www.ha.org.hk/haho/ho/hesd/Full_Report.pdf.

на флешку электронные таблицы, полученные от других больниц, а затем переносила на компьютер коллеги, у которого Excel был. При этом она постоянно и безуспешно просила IT-отдел установить Excel на ее компьютер.

Итак, всему виной действительно человеческий фактор, но связанный не с делопроизводителем, а с сотрудниками IT-отдела, не удосужившимися установить коллеге необходимую программу. Когда они это сделали, риск утечки данных из-за потери флешки исчез, поскольку отпала потребность ее использовать.

Пример показывает, что люди стремятся хорошо выполнить свою работу, даже если при этом нарушают требования безопасности. Девушка не осознавала, что ставит под угрозу данные пациентов. Она просто не нашла другого решения проблемы.

Фишинг, бессмысленный и беспощадный

Люди часто открывают вложения в электронных письмах и кликают по ссылкам, что приводит к установке шпионских программ. Хакеры стали куда умнее: они нередко используют в рассылках информацию, почерпнутую из социальных и профессиональных сетей, а потому отличить фишинговые письма от обычных все труднее. Хотя несколько нигерийских принцев все еще жаждут вручить вам миллионы долларов, их сообщения постепенно вытесняются другими, гораздо более убедительными.

Калифорнийский университет в Беркли собирает базу данных о фишинговых атаках и пополняет ее образцами таких посланий. Нашлось даже поддельное письмо от HR-отдела самого университета (рисунок 1)[2].

Рисунок 1. Пример фишинговой атаки

От: <HR@berkeley.edu> <HR@berkeley.edu>

Subject: Message from human resources

Дата: 13 апреля 2017 Время: 21:29:54

Кому: XXXXX@berkeley.edu

Уважаемый XXXXX@berkeley.edu

Информационное письмо направлено HR-отделом.

Пройдите по этой ссылке, чтобы авторизоваться и просмотреть документ. Спасибо!

Калифорнийский университет в Беркли, HR-отдел.

[2] Berkeley Information Security Office, "Phishing Example: Message from Human Resources," https://security.berkeley.edu/news/phishing-example-message-human-resources.

Письмо кажется настоящим. Просьба авторизоваться для просмотра документа не вызывает подозрений: это стандартная практика для многих организаций, особенно при работе с конфиденциальной информацией. Отдел IT-безопасности университета Беркли в данном случае порекомендовал проверять достоверность ссылки, прежде чем переходить по ней. Наведите на нее курсор, и внизу экрана появится адрес веб-сайта. Затем нужно убедиться, что ссылка действительно ведет на страницу HR-отдела, а не на ресурс мошенников.

Такой совет одобрило бы большинство экспертов по кибербезопасности, но есть два нюанса. Во-первых, просмотр рабочих писем – рутина, с которой часто хочется покончить побыстрее. Многие решат, что наведение курсора на ссылку, изучение и проверка веб-адреса займут слишком много времени. Во-вторых, далеко не каждый рядовой пользователь сумеет проверить достоверность веб-адреса. Компания не может вменять это сотрудникам в обязанность.

Обучение основам безопасности

Это распространенный способ снизить риски фишинговых атак и внедрения вредоносного ПО в корпоративные компьютерные сети. Однако даже сотрудники компаний, специализирующихся на кибербезопасности, не могут похвастаться блестящими результатами подобных тренингов. Компания Intel Security (в прошлом McAfee)

протестировала 19 000 человек в 140 странах, и только 3% из них выявили все фишинговые имейлы в выборке из десяти сообщений, а 80% не нашли ни одного[3]. Никакое обучение основам безопасности не решит эту проблему: достаточно одному сотруднику кликнуть на вредоносную ссылку или зараженное вложение, чтобы фишинговая атака достигла своей цели.

Отстрел на подлете

Еще один инструмент борьбы с фишингом – современные технологии, предназначенные для выявления вредоносного ПО заранее, на этапе установки. Но как гарантированно поймать всех воров и шпионов? Первоначально здесь помогало составление списка сигнатур, то есть своего рода отпечатков пальцев известных образцов вредоносных программ, и их сравнение. Новая программа не прошла проверку на «отпечатки пальцев»? Система безопасности блокирует запуск. Продвинутые антивирусы принимают во внимание также дополнительные характеристики, в том числе поведение потенциально вредоносного ПО. Однако проблема остается, и разработчики антивирусов пытаются своевременно обновлять свои продукты, не отставая от ухищрений хакеров.

---

[3] Tom Reeve, "Even Security Experts Fail to Spot Phishing Emails, Finds Report," SC Media, May 19, 2015, https://www.scmagazineuk.com/even-securityexperts-fail-to-spot-phishing-emails-finds-report/article/537183/.

В конце 2017 года компания Malwarebytes, специализирующаяся на антивирусном ПО, проанализировала уровень кибербезопасности почти на 10 млн компьютеров. Выяснилось, что даже самые совершенные антивирусы не смогли выявить почти 60% участвовавших в эксперименте вредоносных программ[4].

Ранее, в 2013 году, корпоративная сеть New York Times была взломана с целью раскрыть источники информации[5]. Ее атаковали сорока пятью вредоносными программами. Антивирусы выявили лишь одну из них.

Вернемся далеко в прошлое — к заре сферы кибербезопасности. Следует отметить, что основатель индустрии антивирусных программ уже тогда понимал: их возможности не безграничны. За два года после того, как в 1986 году был создан первый вирус, на бурно развивавшемся рынке антивирусного ПО появилось без малого сорок игроков[6]. Видя, как они множатся, разработчик первого коммерчески успешного антивируса Джон Макафи подсчитал, что «около 75% продуктов, предлагающихся на рынке, не эффективны, поскольку не способны ни защитить

[4] Steve Ragan, "Malwarebytes Is Tracking Missed Detections in Traditional Antivirus," CSO, November 7, 2017, https://www.csoonline.com/article/3236254/security/malwarebytes-tracking-missed-detections-in-traditional-anti-virus.html.

[5] Gerry Smith, "Why Antivirus Software Didn't Save the New York Times from Hackers," *Huffington Post*, January 31, 2013, https://www.huffingtonpost.com/2013/01/31/antivirus-software-hackers_n_2589538.html.

[6] "Happy Birthday Brain, the World's First PC Virus," *Computer Active* 388 (2013): 9.

компьютер от значительной части вирусов, ни даже выявить их»[7]. Он публично выражал обеспокоенность из-за того, что «недостаток понимания со стороны пользователей привел к распространению недостоверной информации, излишне эмоциональной реакции и мошенничеству»[8]. В 2018 году в мире было продано антивирусного ПО больше чем на $15 млрд. Ожидается дальнейший рост на уровне 10% в год[9].

В борьбе с фишингом и прочими киберугрозами хорошо зарекомендовало себя одно технологическое решение. Оно эффективно тем, что освобождает рядовых сотрудников от лишней ответственности (например, переходить ли по ссылке, открывать файл или нет). «Белый список приложений» формируется по принципу: если программа не будет запущена на компьютере, то не сможет причинить никакого вреда. Это немного напоминает список гостей — практику, применяющуюся для ограничения доступа в клубы, на вечеринки и закрытые мероприятия. Вместо того чтобы оценивать каждую программу с точки зрения вредоносности, «белый список» разрешает установку только проверенного ПО, запуск которого точно

---

[7] *Inventors and Inventions*, vol. 4 (Tarrytown, NY: Marshall Cavendish, 2007), 1033; Laura DiDio, "Antivirus Vendors Form Industry Regulation Group," *Network World* 5, no. 28 (1988): 17.

[8] DiDio, "Antivirus Vendors."

[9] MarketsandMarkets, "Endpoint Security Market Worth 17.38 Billion USD by 2020," press release, accessed May 19, 2018, https://www.marketsandmarkets.com/PressReleases/endpoint-security.asp; Technavio, "Global Antivirus Software Package Market 2016–2020," accessed May 19, 2018, https://www.technavio.com/report/global-enterprise-application-global-antivirussoftware-package-market-2016–2020.

не нанесет ущерба. В таких условиях не имеет значения, по каким ссылкам переходят пользователи и какие вложения они открывают. Если вредоносной программы нет в «списке гостей», она останется «за порогом».

Стимулирование IT-персонала

Концепции обеспечения безопасности на основе списка разрешенных приложений известны давно. Есть соответствующие коммерческие продукты, даже операционные системы Windows и Mac OS содержат подобные инструменты защиты. Отсюда первый вопрос: «Почему мы не используем антивирусы, работающие по принципу "белого списка", максимально широко?» И второй: «Почему так мало людей вообще о нем знают, в то время как антивирусные и антифишинговые программы широко известны?» Ответы сводятся к «Зачем это надо?» и «Так будет только хуже».

Поскольку современные антивирусы недостаточно эффективны, периодическое заражение считается естественным и неизбежным. Когда такое случается, никто не винит ни антивирусные программы, ни их поставщиков; компании не винят и сотрудников IT-отдела, которые выбрали эти продукты. Таким образом, у последних нет причин отказываться от неэффективных подходов к обеспечению безопасности и искать альтернативы.

Более того, IT-отдел и команда кибербезопасности приведут вам немало аргументов против «белых списков». Внутри корпоративной среды проще установить

антивирусное ПО и управлять им в автоматическом режиме. Никто не обвинит IT-специалистов в том, что оно не работает, – оно же есть! Развертывание приложений на основе «белого списка» потребует куда больше усилий и внимания. Придется постоянно пополнять перечень свежими авторизованными бизнес-приложениями, а также вносить туда обновления установленных программ и приложений, иначе коллеги не смогут использовать необходимое ПО или компьютеры вообще. В этом обвинят именно IT-специалистов – и заставят лихорадочно устранять возникшую проблему.

Главные камни преткновения здесь – ответственность за создание безопасной цифровой среды и вопрос, кто ее несет. На сегодняшний день компании возлагают ответственность на сотрудников, не имеющих никакой возможности защитить себя и других, а также на технологии, подтвердившие свою неэффективность. Глубинные причины такого подхода связаны с мотивацией и ответственностью персонала, вернее с их отсутствием. Мантра «Это все человеческий фактор» – лишь удобное прикрытие.

Спасайте бриллианты короны!

Чаще всего мы слышим о кражах личных данных (например, финансовой и медицинской информации, паспортных данных, кредитных карт и паролей) в результате взлома корпоративных и государственных систем. Чуть реже «утекают» коммерческие тайны, интеллектуальная

собственность, планы стратегического развития и внутренняя финансовая документация. Если учесть, что не все цифровые активы одинаково ценны, имеет смысл сосредоточиться на защите важнейших, тех самых «бриллиантов короны». Но есть проблема: зачастую следование этому принципу приводит к действиям, не только неэффективным для снижения киберрисков, но и попросту неприемлемым.

Пытаясь уберечь «бриллианты короны», мы невольно воспринимаем конфиденциальность информации как безоговорочный приоритет. Иными словами, нам кажется, что лучше замедлить или затруднить работу с данными, если такой ценой они не попадут в чужие руки. Однако некоторым видам бизнеса подобный подход серьезно навредит.

Если вы разрабатываете многопользовательские онлайн-игры, приоритетами вашей компании станут пропускная способность сети и мощность серверов, ведь вы хотите сделать игры доступными для сотен тысяч пользователей, в любой момент. Иначе вы быстро потеряете бизнес.

Если ваша компания использует промышленные системы контроля для управления, например, нефтепереработкой, производством нефтехимии или электроэнергии, для вас приоритетна скорость коммуникаций. Такие системы объединяют множество отдельных компьютеров, зачастую довольно старых и очень чувствительных к задержкам в передаче информации по сети. Если один компьютер не получит сообщение от другого в определенный момент, в его работе может произойти сбой. Далее последует эффект домино, что приведет к нарушениям производственного процесса или его полной остановке.

Скорость критична и для работы медицинских учреждений. Хотя в сфере здравоохранения защита конфиденциальных сведений важна, в чрезвычайной ситуации приоритеты существенно меняются. Если пациент находится в отделении неотложной помощи или на операционном столе, врачи хотят получить как можно больше информации из его истории болезни и как можно быстрее. От этого зависит его жизнь. Если в цейтноте операции кто-то посторонний также получает к этой информации доступ, с инцидентом можно будет разобраться потом, когда пациент пойдет на поправку.

Эти примеры доказывают: далеко не все киберриски имеют отношение к конфиденциальности; фокус на ней отвлекает от не менее важных проблем. Он также ничего не гарантирует, потому что часто защита «бриллиантов короны» ограничивается их непосредственным хранилищем. Вот почему после утечки задается стандартный вопрос: «Была ли информация зашифрована?» Обычно это касается первичной базы данных. Но чтобы информация стала ценностью, ее необходимо еще извлечь, распространить и использовать. Уровень риска на этих этапах намного выше. Поэтому, чтобы определить приоритетность задач IT-специалистов и оптимизировать защиту, компания должна сосредоточиться на отладке наиболее важных для нее бизнес-процессов. Решив эту задачу, вы обеспечите и надлежащий уровень конфиденциальности данных.

Рассмотрим в качестве примера бизнес-процессы, связанные с работой клиентского отдела: создание новой учетной записи, ее использование и удаление из базы. Для

всего этого требуется доступ к конфиденциальным персональным и финансовым данным (почтовый адрес и ID-карта, номер кредитной карты и банковского счета) клиента. Проследив перечисленные механизмы, ваша компания будет знать, на каких компьютерах хранится та или иная информация, через какие сети проходит и кто имеет к ней доступ. Вы сможете не только эффективнее защитить конфиденциальные данные клиента, но и снизить непредвиденные риски, подрывающие его доверие к вам.

Фокус на ключевых бизнес-процессах позволяет также выявить информацию, ценность которой критична — однако раньше вы этого не осознавали. Здесь хорошим примером послужит низкотехнологичный бизнес вроде выращивания и продажи орехов в Калифорнийской долине. Миндаль, грецкие орехи и фисташки очень даже привлекательны для воров, ведь один грузовик таких сокровищ может стоить до $500 000! А еще орехи — это вам не IT-оборудование: у них нет серийных номеров, съел — и никаких доказательств.

Продвинутые воры уже отказались от захвата грузовиков на пустынных дорогах и подались в хакерство. Они начинают с того, что взламывают компьютеры «ореховых» компаний и крадут информацию о планируемых отгрузках. После этого аккуратно фальсифицируют документы и... посылают собственные грузовики на склад поставщика до того, как приедут реальные покупатели. В некоторых случаях воры нанимают водителей (те и не подозревают, что участвуют в преступлении!)[10].

[10] Geoffrey Mohan and Richard Winton, "In Sophisticated Shell Game, Thieves Hit Central Valley Nut Growers," *Los Angeles Times*, April 14, 2016, https://www.latimes.com/business/la-fi-nut-theft-20160414-story.html.

Идея «спасать бриллианты короны», так же как и другие банальные сентенции о кибербезопасности, создает иллюзию, что мы разобрались в проблеме и знаем, как с ней справиться. А ведь это мешает посмотреть на нее шире и найти максимально эффективное решение.

Киберугрозы не стоят на месте!

Непрерывный рост количества киберугроз — или в некотором смысле иллюзия роста? — дезориентирует компании и толкает к двум типичным ошибкам. Во-первых, многие считают, что инвестиции в защиту должны соответствовать масштабам угроз и темпам их развития: если угроза стремительно нарастает, нужно скорее увеличить «защитные» вложения. Во-вторых, существует убеждение, что борьба с прежде неизвестными угрозами требует дополнительных вливаний. Поскольку эти соображения существенно влияют на принятие финансовых решений, рассмотрим их подробнее.

Скорость вращения Земли зависит от того, где вы стоите

Динамичное развитие киберугроз считается веским основанием для постоянных брифингов по кибербезопасности. Бесспорно, эта тема заслуживает внимания, но не из-за того, с какой скоростью плодятся вирусы

и прочие угрозы, а по причине глобальности и важности проблемы в целом.

Оценивая темпы нарастания рисков, часто используют такой показатель, как объем новых вредоносных программ. Считается, что в 2017 году их насчитывалось от 15 107 232 до 128 160 000, и это только те, которые удалось обнаружить[11]. Хотя это колоссальные цифры, они бессмысленны. Нет принципиальной разницы, как компании защищаются от миллиона, 10 миллионов или даже 100 миллионов угроз. Насущная задача – нейтрализовать любую из них.

Хорошо забытое старое

Термин «кибербезопасность» на слуху не так давно, вот почему угрозы, с которыми мы сталкиваемся, кажутся чем-то сравнительно новым. Однако история сферы насчитывает более 50 лет. Еще в 1960-е ВВС США озаботились риском, о котором и сегодня вовсю кричат газеты, – возможной атакой иностранного государства на важнейшие объекты инфраструктуры США. Под иностранным государством имелся в виду СССР, а под важнейшими объектами инфраструктуры – ядерный арсенал США. Риск заключался

[11] "2017 in Figures: The Exponential Growth of Malware," Panda Security Mediacenter, January 4, 2018, https://www.pandasecurity.com/mediacenter/malware/2017-figures/; Tara Seals, "360K New Malware Samples Hit the Scene Every Day," *Infosecurity*, December 14, 2017, https://www.infosecurity-magazine.com/news/360k-new-malware-samples-every-day/.

в использовании программ, способных вызвать сбой в работе компьютерных сетей. Звучит на удивление современно, правда? По словам полковника ВВС США в отставке Роджера Шелла, вредоносные программы, проникнув в компьютеры, контролировавшие запуск ядерных ракет наземного базирования, могли перенаправить их на американские города. Этого стоило опасаться[12].

Компьютерные сети 1960-х и близко не напоминали нынешние; интернет еще не захватил мир, поэтому неудивительно, что основным источником заражения являлись внешние носители и инструменты, при помощи которых программисты преобразовывали написанные коды в понятные для машин инструкции. Чтобы нивелировать риски, разработчики проводили специальные исследования в фоновом режиме, а все необходимое программное обеспечение создавали локально, на одной машине. Хотя механизмы разработки ПО с годами изменились (многое делается на аутсорсе), эксперты по кибербезопасности еще в 1960-х выявили риски, снова ставшие актуальными в наши дни.

Apple предлагает разработчикам приложений для iOS (прежде всего для iPhone и iPad) продукт под названием Xcode. Скачать его можно со специализированных сайтов для программистов. На одном таком сайте – Baidu

[12] Private conversation, February 15, 2018. Additional detail on cybersecurity concerns during the 1960s can be found in Roger R. Schell, *Oral History Interview with Roger R. Schell* (Charles Babbage Institute, May 1, 2012), https://conservancy.umn.edu/handle/11299/133439.

Yunpan[13] – разместили вредоносную версию Xcode под названием XcodeGhost, в которую были добавлены инструкции без ведома разработчика[14]. Они встраивались в мобильные приложения, а затем похищали личные данные пользователей и пересылали на неизвестный сервер.

Специалисты ВВС США распознали этот тип кибератаки 50 лет назад. Отсюда можно сделать вывод: очень важно понимать, от кого и в чем мы зависим при отражении угроз. Компании интересуются этим вопросом гораздо реже, чем следовало бы, и пора исправить ситуацию.

Зимой 1970 года рабочая группа по информационной безопасности при Научном совете Министерства обороны США опубликовала доклад «Обеспечение безопасности компьютерных систем»[15]. Он известен как «Доклад Уэра», поскольку его основным автором был Уиллис Уэр. Он перечисляет и описывает большинство уязвимостей и рисков, с которыми мы сталкиваемся по сей день. Мы обобщили информацию о них в таблице 1.

---

[13] Облачная платформа для хранения данных, обмена ими и их совместного использования, была запущена в марте 2012 года. Предназначалась как для простых пользователей, так и для разработчиков. В 2016 году Baidu Yun получила новое имя – Baidu Wangpan, под которым работает и сегодня. *Прим. ред.*

[14] Joseph Cox, "Hack Brief: Malware Sneaks into the Chinese IOS App Store," *Wired*, September 18, 2015, https://www.wired.com/2015/09/hack-brief-malware-sneaks-chinese-ios-app-store/.

[15] Willis H. Ware, "Security Controls for Computer Systems," Rand Corporation (Rand Report), https://www.rand.org/pubs/reports/R609-1.html.

Таблица 1. Примеры уязвимостей

Источник	Конкретная проблема	Актуальность
Файлы	Похищение, копирование и несанкционированный доступ к конфиденциальной информации	По-прежнему наиболее серьезный риск для компаний
Программное обеспечение	Неэффективность антивирусной защиты, сбои контроля доступа к информации	Являются основной причиной внутренней кражи информации
Пользователи	Неэффективная аутентификация пользователей	Преступники выдают себя за сотрудников компании, используя украденные пароли. Они преследуют пользователей и шантажируют компании
Сетевые подключения	Возможность перехватывать сетевой трафик	Риск по-прежнему существует, но, к счастью, появилось множество решений для шифрования информации
Системное администрирование	Ошибки системных администраторов приводят к раскрытию конфиденциальной информации	Один из главных рисков интернета вещей и широкого внедрения технологий, неподконтрольных IT-отделу. Нередко сами пользователи не знают, как безопасно управлять своими устройствами. Также во многих случаях утечка корпоративных данных из облачных хранилищ происходит из-за ошибок конфигурации
Программисты	Программисты модифицируют ПО, отключая функции безопасности, оставляя всевозможные лазейки и снижая уровень защиты приложений другими способами	Эти угрозы по-прежнему актуальны

Наиболее серьезные уязвимости отнюдь не новы. Инновационные способы применения и сочетания цифровых технологий порождают новые проблемы, но все они — лишь потомки существовавших раньше.

Компьютеры теперь чрезвычайно разнообразны — начиная от привычных стационарников и ноутбуков, заканчивая умными часами и холодильниками. Они требуют обновленных подходов к защите, но в целом бреши кибербезопасности остаются прежними, как и угрозы. Конечно, они обрели новые черты, но суть осталась. Вспомним имейлы со ссылками, переход по которым приводил к установке вредоносных программ. Теперь уже достаточно открыть подозрительную СМС — и какой-нибудь шпион или воришка проникнет на ваш смартфон. Способы внедрения вредоносных программ эволюционировали. Сами программы тоже стали немного другими, например адаптировались для запуска на мобильных устройствах, но это все та же старая добрая кибератака. Напоминает магазин, заявляющий о сорока вариантах рубашек в продаже... а на деле продающий одну модель в четырех размерах и десяти расцветках.

Итак, мы показали, как банальные, заезженные суждения отвлекают внимание от действительно важных проблем. В следующей главе мы рассмотрим теневые факторы, от которых зависит кибербезопасность, и разберемся, где правда, а где предрассудки.

Глава 2

Теневые факторы

Чтобы обеспечить эффективную киберзащиту, важно не забывать о ряде нетехнических факторов, или скрытых движущих сил. Речь не о бесконечных кодах и контурах микросхем, понятных лишь программистам и инженерам. Напротив, мы поговорим о вещах предельно доступных. Просто до сих пор они не рассматривались в контексте кибербезопасности.

Сначала мы познакомимся с так называемой химерой соответствия: разберем внутренние ограничения стандартов кибербезопасности и основанных на них законодательных норм, оценим их роль в стратегии компании. Далее обсудим мотивацию сотрудников и те способы «блеснуть» на работе, которые создают дополнительные риски для компании. Затем мы рассмотрим экономику кибератак — финансовые стимулы развития этого рынка — и попытаемся ответить на вопрос: «Так ли важно, кто именно нас атаковал?» Наконец, мы проанализируем асимметричность атак и защиты — взаимосвязь между мощью удара и необходимого отпора. И, конечно же, порассуждаем о том, почему кибератака — совсем не то же самое, что сражение в традиционном понимании.

Химера соответствия

Занимаясь проблемами кибербезопасности, вы ставите во главу угла надежность защиты от атак. «Действительно ли наша компания в безопасности?», «Правильно ли мы действуем?», «Делаем ли мы достаточно?» — такие вопросы вы постоянно задаете.

Чтобы ответить на них правильно, киберриски стоит оценивать в условиях реальной бизнес-среды; об этом мы поговорим далее в книге. Но зачастую компании оценивают свое положение дел с опорой не на реальность, а на общие стандарты кибербезопасности. На этой основе они делают выводы о том, насколько надежна их защита и сколько средств в нее инвестировать. Безусловно, стандарты полезны. Но чтобы использовать их эффективно, следует понимать цели их разработки и внутренние ограничения. У попыток соответствовать требованиям множества стандартов и законодательных норм могут быть самые непредвиденные последствия.

Внутренние ограничения стандартов кибербезопасности

Соответствовать всему и ничему

Стандарты кибербезопасности предназначены для широкой аудитории; один из показателей их успешности — масштабы внедрения. Однако, пытаясь быть полезными всем, на практике эти стандарты не помогают ни одной отдельно взятой категории пользователей.

Концепция Национального института стандартов и технологий США по совершенствованию кибербезопасности критично важной инфраструктуры (или просто Концепция NIST) изначально разрабатывалась, чтобы снизить риск нанесения ущерба ключевым объектам инфраструктуры[16]. Однако во введении утверждается, что концепцию может использовать любая организация, поэтому она активно внедряется в разных отраслях, вплоть до розничной торговли и гостиничного бизнеса. А ведь приоритеты кибербезопасности для атомной электростанции явно отличаются от приоритетов отеля или супермаркета. Никакой стандарт, независимо от того, насколько удачно он разработан, не подойдет *всем*.

Даже стандарт, разработанный представителями вашей отрасли, не гарантирует вам полезных и адекватных рекомендаций. Например, Американский химический совет опубликовал руководство по внедрению кодекса безопасности управленческих практик «Ответственная забота»[17]. Возможно, там и содержатся полезные советы по менеджменту в области кибербезопасности, зато нет ничего об уникальных проблемах, характерных для систем управления производством. Иными словами, руководство настолько

---

[16] Matthew P. Barrett, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," National Institute of Standards and Technology paper, April 16, 2018, https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11.

[17] American Chemistry Council, "Implementation Guide for Responsible Care® Security Code of Management Practices: Site Security & Verification," 2002, https://www.nj.gov/dep/enforcement/security/downloads/ACC%20Responsible%20Care%20Site%20Security%20Guidance.pdf.

обобщенное, что дает примерно одинаковые рекомендации и IT-системам фронт-офиса, и IT-системам химического производства, для которых его, собственно, и писали.

В качестве альтернативы некоторые компании разрабатывают собственные рекомендации. Это разумно, но важно, чтобы такие «внутренние стандарты» соответствовали условиям и темпам роста вашего бизнеса. Если вы приобретаете другие компании и создаете новые продукты, то подходы к кибербезопасности потребуется скорректировать.

Например, наш клиент из сферы финансовых услуг разработал стандарт кибербезопасности в тот период, когда вычислительные мощности десятков серверов располагались в его собственных дата-центрах. Система отлично работала долгое время. Однако условия рынка менялись, менялся спектр услуг и форма их предоставления. Стандарт неумолимо устаревал. Вопрос встал ребром после поглощения индийской компании, где транзакции проводились с помощью облачных технологий. Первая проблема заключалась в том, что существующий стандарт не содержал рекомендаций по защите от рисков в такой ситуации. Вторая – в том, что поглощенная компания работала не по требованиям стандарта и руководители вынуждены были тратить массу времени на урегулирование неизбежных претензий по результатам аудита.

Всегда на шаг назад

Стандарты никогда не идут в ногу со временем. Например, широко известный международный стандарт

кибербезопасности ISO 27001 был опубликован в 2005 году[18], а впервые пересмотрен — лишь через восемь лет. В 2018 году компания North American Electric Reliability Corporation объявила о выпуске пятой версии стандарта защиты критично важной инфраструктуры (CIP). Он заменил ранее действовавший стандарт 1200, одобренный в далеком 2003 году. Прошло 15 лет![19]

Дело не в том, что стандарты не успевают за постоянно меняющимися угрозами. В главе 1 мы объяснили, почему значение этих изменений сильно преувеличено. Но стандартам просто не угнаться за развитием бизнеса. Изменения в процессах и в наборе предлагаемых услуг и продуктов приводят к появлению новых киберрисков.

Финансовые стимулы

Проверка соответствия компании стандарту кибербезопасности — показательный процесс. Ведь финансовые стимулы, влияющие одновременно на проверяющего и проверяемого, способны поставить результат и его значимость под вопрос.

Компании обычно платят внешним аудиторам, которые подтверждают соответствие их практик нормативным документам и отраслевым стандартам, а также выявляют потенциальные противоречия и «слепые зоны».

---

[18] International Organization for Standardization, "ISO/IEC27000 Family-Information Management Systems," https://www.iso.org/isoiec-27001-information-security.html.

[19] North American Electric Reliability Corporation, "1200-Cyber Security (Urgent Action)," https://www.nerc.com/pa/Stand/Pages/1200Cyber_Sec_Renewa.aspx.

Стандарт безопасности информации в индустрии платежных карт (PCI DSS) – прекрасный пример[20].

Вскоре после публикации PCI DSS в 2004 году мы стали проводить аудит в азиатском сегменте этой отрасли, привлекая самых квалифицированных специалистов. Первое, на что мы обратили внимание, – для многих компаний, хранящих или обрабатывающих информацию о платежных картах, ее защита – отнюдь не безусловный приоритет. Куда важнее им получать формальный отчет, подтверждающий, что они соответствуют необходимым требованиям кибербезопасности. Вдобавок они хотели получить такой отчет подешевле, без особых усилий. Даже работая с лидерами отрасли, мы сталкивались с тем, что стоимость аудита для них важнее качества. В результате мы вынуждены были прекратить сотрудничество. Невозможно нанять хороших экспертов за предлагаемые такими компаниями смешные деньги.

С другой стороны, компании и индивидуальные предприниматели, проводящие оценку соответствия, мотивированы повышением эффективности и максимизацией прибыли. Прежде всего это бизнес. Квалифицированному аудитору систем безопасности (QSA) проще работать с постоянными клиентами, тем более что такой аудит проходит ежегодно. Однако QSA вряд ли пригласят для проверки в ту же компанию в следующем году, если в этом он даст негативное заключение. Мы беседовали со многими аудиторами в области кибербезопасности, и зачастую они

[20] Security Standards Council, "Securing the Future of Payments Together," https://www.pcisecuritystandards.org/.

говорили, что их руководство неоднократно напоминало им об этих реалиях деловой практики.

Еще один фактор, влияющий на качество аудита в индустрии платежных карт, – затрачиваемое на него время. Количество проведенных аудитов непосредственно влияет на зарплату специалиста. Trustwave – одна из крупнейших компаний, занимающихся аудитом систем безопасности. Ее бывший сотрудник признавался: «Чем больше аудитов вы проводите в квартал, тем приятнее будет ваш бонус». Например, сотрудник с базовым окладом $100 000 в год может заработать премию от $30 000 до 50 000 за счет именно количества, а не качества аудитов[21].

Защита информации о платежных картах, безусловно, важна, и аудиты соответствия стандартам безопасности – одна из форм этой защиты. Однако нетехнические факторы, в том числе финансовые, существенно снижают ее надежность. Например, Home Depot имел положительное заключение о соответствии стандартам, когда произошла утечка информации об операциях по кредитным картам 56 млн его покупателей[22].

---

[21] Jennifer Bjorhus, "Clean Reviews Preceded Target's Data Breach, and Others," Star Tribune, March 31, 2014, http://www.startribune.com/clean-reviewspreceded-target-s-data-breach-and-others/252963011/.

[22] Julie Creswell and Nicole Perlroth, "Ex-Employees Say Home Depot Left Data Vulnerable," New York Times, September 19, 2014, https://www.nytimes.com/2014/09/20/business/ex-employees-say-home-depot-left-data-vulnerable.html.

Стандарты vs защищенность

Быстрое распространение новых стандартов кибербезопасности принесло некоторые результаты: компании прилагают больше усилий к защите активов и клиентов. Однако есть и непредвиденные последствия. Из-за обилия нормативных актов и существенных затрат на выполнение их требований компании упускают из виду многие серьезные риски.

Тут есть несколько важных моментов. Во-первых, пример уже упоминавшейся компании Home Depot показывает, что соответствие стандартам и реальная защищенность – не одно и то же. Определить достаточность защиты от киберугроз гораздо сложнее, чем декларировать соответствие утвержденным нормативам.

Второй момент связан с тем, что люди по-разному реагируют на реальную сиюминутную боль и возможную боль в будущем. Выявленные нарушения стандартов обещают немедленные последствия: штрафы, санкции и прочие карательные меры. Корпоративные отделы внутреннего аудита существуют, как раз чтобы не допускать этого. С другой стороны, ни последствия потенциальной утечки информации, ни ее точные сроки не известны. Это лишь *возможная* боль в будущем; никто не отрицает ее опасности, но для многих она куда менее страшна, чем немедленные последствия несоблюдения стандартов. Таким образом, определение реальных требований кибербезопасности – меньший приоритет, чем соответствие нормам. Еще одно последствие такой позиции – создание иллюзий.

Компании склонны верить, что соответствие стандартам защитит их от всех неприятностей, и пренебрегают другими профилактическими мероприятиями.

Мотивация сотрудников

Сотрудники мотивированы выполнять свою работу, причем выполнять хорошо. Стремление получить повышение, премию или пару добрых слов от руководителя, а также желание чувствовать себя полезным членом команды — факторы, подогревающие мотивацию. И они же — проблема.

Часто мотивация сотрудников не имеет ничего общего с соблюдением требований кибербезопасности (если, конечно, не рассматривать компании, работающие в этой отрасли). В большинстве своем люди не верят, что способны разобраться в ее тонкостях. Конечно, они не хотят, чтобы их бизнес страдал от утечек информации, и не собираются этому способствовать. Но при определенных обстоятельствах, связанных с системой вознаграждения, любой сотрудник вполне может поставить кибербезопасность своей фирмы под угрозу.

Сделать свою работу

Пример такого рода можно найти в практике одной известной автомобилестроительной компании из Азии. Она потеряла $1 млрд в результате утечки данных о новейших

исследованиях и разработках из корпоративной сети. Компания предпочла не сообщать об этом.

Впоследствии топ-менеджеры поручили специалистам по кибербезопасности усовершенствовать защиту информации о разработках. Специалисты предложили создать еще одну сеть для хранения таких данных — внутри корпоративной интрасети. Аргументация «за» сводилась к тому, что хакерам придется взламывать две сети вместо одной, чтобы добраться до конфиденциальной информации. Это чем-то напоминает систему обороны средневекового замка, в которой имелись вал и ров.

К сожалению, специалисты не учли один подводный камень: конструкторы автомобилей работали в тесном контакте с внешними партнерами, которые тоже нуждались в доступе к данным. Изоляция корпоративной сети обернулась тем, что эти два звена больше не могли обмениваться информацией. Как результат, конструкторы лишились возможности продуктивно работать. И что же они предприняли? Создали фейковые аккаунты для своих партнеров, чтобы те могли пользоваться корпоративной интрасетью. И никому не сообщили об этом.

Впоследствии мы спросили, понимают ли конструкторы, что их действия повысили риск утечки конфиденциальной информации. Они понимали, но нисколько не раскаивались. Поскольку их работа заключается в проектировании автомобилей, они без колебаний устранили препятствие, мешавшее двигаться вперед. Все, что их интересовало, — необходимость срочно закончить работу и очевидность возможных последствий (срыв дедлайна).

Ну а *возросшие киберриски* — это что-то неопределенное. Внешние партнеры могут злоупотреблять, а могут и не злоупотреблять доступом к данным. И даже если они это сделают, последствия скажутся когда-нибудь потом, завтра, в следующем месяце или даже году. А может, никто об этом и не узнает.

Дестимуляторы кибербезопасности

Финансовые стимулы могут усилить потенциальный конфликт между человеком, нацеленным выполнить свою работу, и компанией, стремящейся защитить себя. Эти стимулы обычно привязаны либо к реализации индивидуальных целей сотрудников, например повышению личной эффективности, либо к реализации целей подразделения (к примеру, выполнение или перевыполнение квартального плана).

Возьмем в качестве примера выпуск нового продукта или поглощение другой компании. В обоих случаях перед командой кибербезопасности ставится ряд задач: в первом нужно *определить, протестировать и внедрить* целый ряд мер киберзащиты, а во втором — проанализировать ее состояние в поглощаемой компании, чтобы правильно определить стоимость. Но качественное выполнение этих действий сдвигает сроки подписания документов и завершения сделки. Понятно, безопасность опять на втором плане. Сотрудники и топ-менеджеры получают бонусы за соблюдение дедлайнов; когда что-то затягивается, они

не получают ничего. И неважно, насколько уважительна причина – необходимость залатать бреши в системе безопасности. А ведь эти бреши способны подорвать финансовое положение компании куда сильнее, чем перенос сроков запуска нового продукта на несколько недель или даже месяцев.

Живая иллюстрация – история со смартфоном Samsung Galaxy Note 7. Его склонность к самопроизвольным возгораниям, о которой много писали средства массовой информации, не была результатом какой-либо киберуязвимости. Она стала возможной благодаря некоторым особенностям корпоративной культуры и системы стимулирования, поставившей быстроту запуска проекта выше безопасности. Надеясь затмить и обогнать непосредственного конкурента – Apple, компания Samsung максимально сократила сроки освоения своих продуктов, буквально вытолкнув на рынок навороченный смартфон со скрытыми конструкторскими и производственными дефектами[23]. В итоге Samsung потеряла почти $9,5 млрд выручки от реализации и $5 млрд прибыли – вместо ожидаемого конкурентного преимущества[24].

---

[23] Yoolim Lee and Min Jeong Lee, "Rush to Take Advantage of a Dull iPhone Started Samsung's Battery Crisis," Bloomberg, September 18, 2016, https://www.bloomberg.com/news/articles/2016-09-18/samsung-crisis-began-in-rush-to-capitalize-on-uninspiring-iphone.

[24] Jethro Mullen and Mark Thompson, "Samsung Takes $10 Billion Hit to End Galaxy Note 7 Fiasco," CNN, October 11, 2016, http://money.cnn.com/2016/10/11/technology/samsung-galaxy-note-7-what-next/index.html.

Экономика кибератак

Знание врага в лицо – отличительная особенность хороших руководителей; то же справедливо и в цифровом мире, особенно если речь о государственных учреждениях. Технические возможности хакеров – один из ключевых факторов выстраивания адекватной киберзащиты.

Сочетание рыночных механизмов и мощных инноваций заставляет пересмотреть некоторые прежде незыблемые тезисы в этой области. Например, вопрос «Кто нас атакует?» несколько теряет актуальность. Эти изменения непосредственно влияют на распределение инвестиций в кибербезопасность и на общие подходы к ее оценке.

Возможности государства

Существует убежденность, что у Северной Кореи, России, Китая и США есть все ресурсы для разработки наиболее продвинутых и мощных хакерских программ. Это предположение служит, с одной стороны, оправданием увеличения «вливаний» в кибербезопасность, а с другой – прекрасным объяснением на случай, если меры защиты подводят. Но хакерская программа – все же не авианосец: чтобы создать ее, стране не обязательно располагать запредельным техническим и финансовым потенциалом.

Например, два исследователя в области кибербезопасности, Брайан Мейкселл и Дилон Бересфорд, вооруженные лишь ноутбуками MacBook Pro, продемонстрировали,

как «...проникать даже в наиболее защищенные мировые сети без поддержки какого-либо государства»[25]. Они сделали это, найдя уязвимость в программно-логическом контроллере (ПЛК) от ведущего производителя этой отрасли. У них не было никаких ресурсов, только время.

ПЛК – рабочие лошадки промышленной автоматизации. Они контролируют все, от роботов в цехах до оборудования нефтеперерабатывающих заводов и центрифуг на атомных электростанциях. Как и многие технологии и продукты, они разрабатывались без учета требований кибербезопасности, а в результате обмен данными между ПЛК не всегда ведется в зашифрованной форме. Эта уязвимость позволила Мейкселлу и Бересфорду отправить ПЛК специальные сообщения и перехватить над ним контроль. Они могли заставить его работать с ошибками или вообще остановиться. Далее они могли использовать ПЛК с уязвимостью как исходный пункт и перехватить контроль над всеми остальными в данной промышленной среде.

История Кремниевой долины полна рассказов о суперуспешных компаниях, начинавших очень скромно. Например, Apple и Hewlett-Packard родились в буквальном смысле в гаражах своих основателей. Вероятно, что-то подобное можно было бы рассказать о наиболее продвинутых кибератаках. Они проводились отнюдь не из подвалов секретных правительственных организаций, а скорее

[25] Robert McMillan, "Siemens SCADA Hacking Talk Pulled Over Security Concerns," *PC World*, May 19, 2011, https://www.pcworld.idg.com.au/article/387095/siemens_scada_hacking_talk_pulled_over_security_concerns/.

из городских кафе, и стояли за ними люди вроде Мейкселла и Бересфорда, работающие со своих ноутбуков.

«Никто, кроме нас» — отныне неактуально

Даже если государство разрабатывает мощный хакерский арсенал, не обязательно, что потом оно за ним уследит. Годовой бюджет Агентства национальной безопасности США (АНБ) превышает $10 млрд, и значительная его часть всегда инвестировалась в развитие эксклюзивных хакерских инструментов[26]. Но благодаря ряду утечек и взломов эти программы сейчас может купить почти любой желающий. Ошеломительно, правда?

Атака сетевого червя-вымогателя WannaCry — одного из самых разрушительных вирусов в истории — прекрасный пример того, что ни одно государство не может бесконечно «стеречь» свои разработки. Правительства сохраняют монополию на определенные ресурсы, например вооруженные силы, но хакерские программы больше не входят в категорию НКН («Никто, кроме нас»). До них часто добираются посторонние личности и организации, в том числе криминальные структуры.

Всего за четыре дня — с 12 по 15 мая 2017 года — червь WannaCry инфицировал более 200 000 компьютеров

[26] "The Black Budget: Top Secret U.S. Intelligence Funding," *Washington Post*, accessed May 7, 2018, http://www.washingtonpost.com/wp-srv/special/national/black-budget/.

в 150 странах мира[27]. Червь – вредоносная программа, которая шифрует данные на зараженном компьютере. Если жертва платит отступные, хакер предоставляет ключ для дешифровки, после чего можно восстановить доступ к данным.

АНБ (группа по оперативному проникновению в компьютерные сети противника) разработало программу под названием EternalBlue, сделавшую возникновение WannaCry возможным. Это была часть огромного арсенала кибероружия, похищенного хакерской группировкой Shadow Brokers. Те намеревались продавать коварные программы правительствам, компаниям и физическим лицам. Первоначально выставив EternalBlue на аукцион, Shadow Brokers в апреле 2017 года разместила ее в бесплатном доступе[28].

Менее чем через месяц тысячи компаний обнаружили, что их сети инфицированы червем WannaCry, для некоторых последствия оказались катастрофическими[29]. На много дней была парализована Государственная служба здравоохранения Великобритании; некоторым ее подразделениям пришлось перенаправлять машины скорой

---

[27] Brian Fung, "How To Protect Yourself from the Global Ransomware Attack," *Washington Post*, May 15, 2017, https://www.washingtonpost.com/news/the-switch/wp/2017/05/15/how-to-protect-yourself-from-the-global-ransomware-attack.

[28] Internet Archive, "Equation Group-Cyber Weapons Auction," accessed May 7, 2018, https://web.archive.org/web/20160816004542/http://pastebin.com/NDTU5kJQ.

[29] The Shadow Brokers, "Don't Forget Your Base," Medium, April 8, 2017, https://medium.com/@shadowbrokerss/dont-forget-your-base-867d304a94b1.

помощи и отказывать в вызове в некритических случаях[30]. Автоконцерны Honda, Nissan и Renault вынуждены были остановить производство[31].

Эффективные рынки хакерских программ

Хакерский рынок быстро развивается. Сейчас здесь можно купить самые продвинутые программы и услуги, причем они доступны не только правительствам, но и любому покупателю, способному за них заплатить. Во многих случаях цена вполне приемлема и даже скромна.

Например, режимы с относительно небольшим бюджетом (как Демократическая Республика Конго, Объединенные Арабские Эмираты и Зимбабве) позволили себе приобрести программу SkyLock от компании Verint Systems, дающую возможность «засекать, отслеживать [и] манипулировать 70% мобильных телефонов, находящихся в любой точке мира»[32]. Целевой рынок широк и глоба-

[30] Alex Hern, "NHS Could Have Avoided WannaCry Hack with 'Basic IT Security', Says Report," *Guardian*, October 26, 2017, https://www.theguardian.com/technology/2017/oct/27/nhs-could-have-avoided-wannacry-hack-basic-it-securitynational-audit-office.

[31] "Honda Halts Japan Car Plant After WannaCry Virus Hits Computer Network," Reuters, June 21, 2017, https://www.reuters.com/article/us-hondacyberattack/honda-halts-japan-car-plant-after-wannacry-virus-hits-computernetwork-idUSKBN19C0EI.

[32] "SkyLock Product Description 2013 (brochure)," *Washington Post*, accessed May 6, 2018, http://apps.washingtonpost.com/g/page/business/skylock-product-description-2013/1276/.

лен. Verint Systems, скромно начинавшая с программы записи звонков для колл-центров, перешла на разработку кибероружия и средств наблюдения и обзавелась клиентурой в более чем 180 странах мира[33].

Продажа кибероружия – растущий бизнес. Глобальный розничный рынок демонстрирует двузначные темпы прироста, расширившись почти с нуля в 2001 году до $20 млрд в 2016 году[34]. Более того, сформировался обширный черный рынок сложных технических решений. Он удовлетворяет спрос на продукты, которые официальные поставщики не хотят или не могут продавать[35]. Работая и в даркнете, и у всех на виду, эти кустарные производители – как физические лица, так и фирмы – предлагают свои продукты и услуги на глобальном рынке.

Это конкурентная и практически бесконфликтная экономика, где действуют клиентоориентированные бизнес-модели и стратегии, перенятые у продвинутых ритейлеров и отделов продаж, располагающих практически неограниченным бюджетом. Игроки рынка стараются выделиться такими дополнительными опциями, как техническая поддержка 24/7, гарантийные обязательства и оперативность. Они используют многие прогрессивные инструменты,

[33] Verint, "Our Company," accessed May 7, 2018, https://www.verint.com/our-company/index.html.

[34] Jennifer Valentino-DeVries, Julia Angwin, and Steve Stecklow, "Document Trove Exposes Surveillance Methods," *Wall Street Journal*, November 19, 2011, https://www.wsj.com/articles/SB10001424052970203611404577044192607407780.

[35] "Cyber Warfare Market Size & Share, Global Industry Report, 2018–2025," Grand View Research, February 2018, https://www.grandviewresearch.com/industry-analysis/cyber-warfare-market.

в том числе формат подписки, скидки за объем закупок, дифференцированное ценообразование и объемистые каталоги хакерских услуг и инструментария для кибератак.

Повторяя успешную политику таких компаний, как Spotify, Netflix и Amazon Prime, некоторые предприимчивые хакеры внедряют формат подписки для продвижения продуктов. В 2017 году уже упомянутая группа Shadow Brokers предложила услугу под названием «Ни дня без взлома». За скромную ежемесячную плату можно было получать доступ к свежеворованной информации, включая как стандартный ассортимент вроде уязвимостей нулевого дня в операционных системах, смартфонах и финансовых сетях, так и более специфичные данные, например о военных ядерных программах России, Китая, Ирана и Северной Кореи[36].

Желающим рынок хакерских услуг готов предоставить полный цикл разработки кибератаки, начиная от исследований и подготовки, заканчивая реализацией. Все это можно и передать на аутсорсинг. Хороший пример — уже не функционирующий сайт WebStresser.org, представители которого за минимальную плату могли организовать вам DDoS-атаку на любую компанию или организацию. Вместе с рекламой отличного обслуживания и технической поддержки 24/7 WebStresser.org предлагал гибкую

[36] Уязвимость нулевого дня — это уязвимость, для корректировки которой не существует программного обеспечения зачастую потому, что его разработчики просто не знают о ней. The Shadow Brokers, "OH LORDY! Comey Wanna Cry Edition," Steemit (blog), May 8, 2018, https://steemit.com/shadowbrokers/@theshadowbrokers/oh-lordy-comey-wanna-cry-edition.

модель ежемесячной подписки, стоимость которой колебалась от $18,99 за «бронзовую» лицензию до $49,99 за «платиновую»[37].

Это динамичный, мощный и конкурентный рынок; криминальные структуры активно используют его для поиска необходимых технических средств и специалистов. Он демократизирует сферы деятельности, которые раньше считались прерогативой государственных организаций и крупных преступных синдикатов, а также делает хакерские программы и услуги доступными любому, у кого есть деньги и желание. Никакой технической подготовки не требуется.

С учетом всего этого компаниям пора сосредоточиться на ценности своей информации и бизнес-процессов не только для них самих, но и для кого-то другого. Какую сумму конкуренты или враги готовы потратить, чтобы навредить вам? Неважно, организуют ли они хакерскую атаку своими силами или кого-то наймут. Рынок позаботится о том, чтобы у них все получилось.

Асимметричность атак и защиты

Еще со времен щитов и копий в военных действиях существовала прямая зависимость между силой атаки и необходимой прочностью обороны. Именно она определяет, например, соотношение мощности бетонобойной бомбы

[37] Интернет-архив сайта WebStresser. Доступ от 18 января 2018 года, https://web.archive.org/web/20180118144032/https://webstresser.org/.

и глубины бункера, который бомба призвана разрушить. В цифровом мире такой зависимости нет. Защита от изощренной хакерской атаки обычно требует простых, незатратных, а иногда и банальных мер.

WannaCry

Упомянутый нами червь WannaCry был изощренным, опасным противником. Давайте посмотрим, что же следовало сделать компаниям (многие это и делали), чтобы вирусу не удалось добраться до их сетей.

1. Не игнорировать обновления ОС Windows. Все мы время от времени видим на экранах телефонов и компьютеров просьбу установить обновления, предназначенные в том числе для устранения уязвимостей в системе безопасности. Microsoft выпустила обновление, предназначенное для нейтрализации WannaCry, примерно за 20 дней до того, как он попал в интернет. Установка обновлений – процесс простой и доступный, а для стационарных компьютеров и ноутбуков может проводиться в автоматическом режиме[38].

[38] Установка обновлений на сервер в корпоративной среде требует больше времени и проведения дополнительных тестов, подтверждающих, что важные бизнес-приложения продолжают функционировать. Установка обновлений для промышленной системы контроля возможна не во всех случаях. Однако и здесь решение проблемы не отличается сложностью.

2. Регулярно и своевременно делать резервные копии операционных систем и данных. Если компания об этом не забывает, даже в случае проникновения WannaCry на ее компьютеры останется возможность восстановить предыдущую, чистую версию операционной системы и данных. А значит, можно будет вернуться к работе.

Из истории с WannaCry мы извлекли пару интересных уроков, касающихся не только создания червя и мер борьбы против него. Во-первых, неспособность компаний защититься от WannaCry — чисто управленческая, а не техническая проблема. Соблюдение «техники кибербезопасности» — рутина, которой люди часто пренебрегают себе во вред. Во-вторых, хотя сам по себе WannaCry был хитрым вирусом, представителям компаний требовалось узнать о нем не так много, чтобы избежать неприятностей. По сути, все необходимое уместилось в этой главе.

Quantum Insert

Quantum Insert — еще один пример вредоносной программы, с немалыми затратами разработанной в Агентстве национальной безопасности[39]. Хотя трудно точно оценить, сколько денег «влили» в этот вирус, есть интересный факт:

[39] Kim Zetter, "How to Detect Sneaky NSA 'Quantum Insert' Attacks," Wired, April 22, 2015, https://www.wired.com/2015/04/researchers-uncover-method-detect-nsa-quantum-insert-hacks/.

в 2013 году бюджет АНБ увеличили на $32 млн в связи с разработкой «нестандартных решений»[40].

Программа позволяла не только отслеживать посещение тех или иных сайтов, но и использовать эту информацию для установки вредоносных программ на компьютеры. Quantum Insert запускается, когда пользователь заходит на определенную веб-страницу. Сайт еще не успевает отреагировать на запрос, а Quantum Insert уже внедряет туда вредоносную программу. И пока браузер ожидает загрузки страницы, программа беспрепятственно проникает на компьютер.

Такие программы стали настолько популярными, что компании разрабатывали их коммерческие версии для стран с более скромными финансовыми ресурсами. Например, Gamma International GmbH продала аналогичную программу, разработанную компанией Dreamlab Technologies AG, правительству Туркменистана за 875 000 швейцарских франков (примерно $858 000)[41]. Чтобы не уступать конкурентам, Китай разработал аналогичную программу под названием Great Cannon[42].

Однако Quantum Insert и ее имитации имеют серьезный недостаток: от них нетрудно защититься. Эти программы

---

[40] Jacob Appelbaum et al., "NSA Preps America for Future Battle," Spiegel Online, January 17, 2015, https://www.spiegel.de/international/world/new-snowden-docs-indicate-scope-of-nsa-preparations-for-cyber-battle-a-1013409.html.

[41] WikiLeaks, "Quotation: Infection Proxy Project 1". Доступ 3 мая 2019 года, https://www.wikileaks.org/spyfiles/docs/DREAMLAB-2010-TMQuotInfe-en.pdf.

[42] Bill Marczak et al., "China's Great Cannon," The Citizen Lab, April 10, 2015, https://citizenlab.ca/2015/04/chinas-great-cannon/.

не работают, если на компьютере имеется зашифрованный алгоритм посещения сайтов. В этом случае они не находят подробностей, необходимых для фабрикации откликов веб-страниц. Сайты все чаще используют шифрование для защиты, и это касается не только банков или интернет-магазинов. Даже сайт с коллекцией эмодзи – https://emojipedia.org – применяет шифрование.

Определить, применяется ли шифрование на сайте, можно, посмотрев на первые пять букв в его адресе. Если это «https», шифрование производится и ваш компьютер неуязвим для атаки. Эта защита предоставляется бесплатно и не требует от вас никаких действий. Если вы хотите подстраховаться дополнительно, можно использовать виртуальную частную сеть (virtual private network – VPN), которая шифрует все ваши интернет-коммуникации. VPN предоставляется бесплатно или за небольшую плату.

Осознание несоответствия между серьезностью атаки и прочностью защиты поможет вам разобраться с двумя аспектами вашей персональной кибербезопасности. Во-первых, это касается инвестиций: вы научитесь скептически оценивать любые требования дополнительных расходов, подкрепленные исключительно заявлениями о растущей сложности кибератак. Во-вторых, вы поймете, что изощренность атаки – недостаточное оправдание неспособности вашей компании защитить себя.

Глава 3

Распространенные заблуждения

СМИ, реклама и в некоторой степени массовая культура влияют на наши представления о киберугрозах, их опасности и методах устранения. Поскольку кибербезопасность – относительно новая тема, вам, возможно, сложно интерпретировать связанные с ней новостные заголовки, оценивать их актуальность для вашей компании и фильтровать дополнительную информацию. Растущий интерес к сфере постепенно облегчает эти задачи, и все же, читая новости, стоит учитывать цели и интересы их источников.

На эту тему чаще высказываются члены правительств и поставщики IT-решений по кибербезопасности, а рупором служат СМИ. Далее мы рассмотрим нюансы, влияющие на то, какая информация и где освещается, а какая – нет.

Правительство

Главный долг любого правительства – заботиться о народе. Испокон веков это подразумевало обеспечение национальной безопасности, исполнение законов и укрепление

экономики. Каждое правительство пытается достичь этих целей по-своему, но никто не спорит с тем, что они приоритетны.

Мы живем в цифровую эпоху; это отражается на всех сферах жизни. Правительства вынуждены пересматривать многие аспекты деятельности и искать наилучшие способы справляться со своей ролью.

Долг предупреждать

Правительства зачастую предупреждают о надвигающихся или ожидаемых бедствиях: воздушных налетах на Лондон во время Второй мировой войны, ураганах на юго-востоке США, цунами в Индийском океане. Людям даются простые, понятные рекомендации: прятаться в бомбоубежище, уезжать или подниматься как можно выше. Остается только им следовать.

К несчастью, с предупреждениями о киберугрозах все сложнее. Возможно, вы помните, как весной 2018 года США и Великобритания заявили о российских атаках против своих правительств, компаний и частных лиц[43]. В сообщениях

[43] David D. Kirkpatrick and Ron Nixon, "U.S.-U.K. Warning on Cyberattacks Includes Private Homes," *New York Times*, April 16, 2018, https://www.nytimes.com/2018/04/16/world/europe/us-uk-russia-cybersecurity-threat.html?emc=edit_nn_20180417&nl=morning-briefing&nlid=50794232201804l7&te=1; информационный бюллетень Национального центра кибербезопасности Великобритании, https://www.ncsc.gov.uk/alerts/russian-state-sponsored-cyber-actors-targeting-network-infrastructure-devices.

подчеркивалось, что под угрозой оказались в первую очередь сетевые маршрутизаторы, серверы интернет-провайдеров, а также устройства, подключенные к интернету (например, термостаты и камеры). Утверждалось, что пока неясно, насколько успешны действия хакеров и каковы их намерения. В заключении приводились рекомендации: как узнать, не взломана ли ваша домашняя сеть, и как укрепить ее защиту.

Однако эти рекомендации были непонятны людям, чьи устройства и сети оказались под угрозой. Ну а некоторые пункты, например изменить условия договора с провайдером, выглядели сложными или просто невыполнимыми.

Примерно в то же время МИД Нидерландов выпустил спецпредупреждение для своих граждан, путешествующих по Турции, Китаю, России и Ирану или проживающих там. Речь шла о киберугрозах для их электронных устройств[44]. МИД рекомендовал стандартные меры безопасности, например использование «чистых» ноутбуков и смартфонов с минимумом необходимых данных. Проблема таких советов в том, что они не учитывают объем информации и технологий, необходимых для деловых поездок; не соответствуют реалиям жизни и работы в зарубежных странах.

Подобные рекомендации могут быть продиктованы как реальными угрозами, так и очевидными геополитическими соображениями. Так или иначе, они бесполезны для защиты компаний или частных лиц и лишь повышают нашу тревожность.

---

[44] "Turkey Poses Cyber Security Threat, Holland Warns Travellers," Ahval, April 9, 2018, https://ahvalnews.com/cybersecurity/turkey-poses-cyber-security-threat-holland-warns-travellers.

Принять ли помощь от государства?

Вал успешных кибератак на бизнес, зачастую приписываемых «внешним врагам», породил множество дискуссий об ответственности правительства. Должно ли государство защищать частные компании? Это важный момент. Традиционно под национальной безопасностью понимали защиту границ, разведку/контрразведку и готовность к любому нападению. Но на цифровой войне все не так просто.

Первая сложность — идентифицировать врага. Если к вашим границам подошла танковая колонна, все достаточно очевидно, а вот кибератаку можно осуществить откуда угодно. Например, бостонская компания, атакованная якобы из Северной Кореи, точно так же могла подвергнуться угрозе из Нью-Йорка, но не напрямую, а по замысловатому маршруту через Францию и Сингапур. Все «улики» (источник хакерских программ, особенности написания кода, адреса атакующих компьютеров) легко подделать. Кроме того, собрать их и проанализировать можно только после начала атаки. Мы не можем заранее узнать, есть ли у нее «иностранный след», и обсудить с военными уместность ответных действий.

Когда правительство предлагает помощь в организации киберзащиты, руководству компании важно понять, какие риски это устранит, какие нет и не создаст ли новых проблем. Подобная помощь, как правило, включает мониторинг всех сетевых коммуникаций компании, входящих и исходящих. Это нивелирует риск атак с использованием вредоносных программ, но не защищает от угроз,

устранение которых требует понимания специфики бизнес-процессов компании. Мониторинг не предотвратил миллиардные убытки автоконцерна из Азии (о чем мы говорили в главе 2) и вряд ли выявит финансовые махинации в отделе закупок или хищение интеллектуальной собственности кем-то из партнеров.

Да, мониторинг сетевых коммуникаций частично защищает от кибератак. Однако последствия того, что ваша сокровищница конфиденциальной информации окажется в распоряжении правительства (или даже нескольких правительств, если речь о транснациональной корпорации), непредсказуемы. Ведь глобальные интересы государств и транснациональных корпораций не совпадают, и есть риск, что информации, собираемой в ходе противодействия кибератакам, найдут и другое применение.

Именно поэтому глава службы безопасности транснациональной горнодобывающей компании отклонил предложенную правительственным агентством США помощь с мониторингом сетей[45]. Несколько лет спустя аналогичное предложение поступило его преемнику. В присланном соглашении мелким шрифтом был прописан пункт, согласно которому агентство получало право использовать любую собранную информацию для расследования уголовных дел. Предложение вновь отклонили. Даже если эту информацию никогда не используют для других нужд, риски существуют. Чужие руки — это чужие руки. К тому же правительственные агентства, включая АНБ (хотя в его

[45] На правах пересказа частной беседы, состоявшейся 16 апреля 2019 года.

названии и фигурирует слово «безопасность»), вряд ли могут похвастаться безоговорочным умением защищать себя и свои данные от кибератак[46].

Вышесказанное — не критика той помощи, которую правительства предоставляют частным компаниям и лицам для повышения кибербезопасности. Но мы хотим подчеркнуть, что характер предлагаемых решений напрямую зависит от типа угроз, с которыми государство привыкло бороться, — например, военная агрессия. Бизнес же сталкивается с более широким спектром рисков и, защищаясь от них, должен руководствоваться своими внутренними приоритетами.

Поставщики IT-решений по кибербезопасности

Рынок кибербезопасности растет стремительнее многих других областей экономики, но конкуренция здесь острейшая. По одной из оценок, в 2018 году 2300 игроков этого рынка предлагали около дюжины разных типов продуктов[47], и количество игроков будет только расти. Поставщикам услуг в этой сфере непросто отстроиться от своих прямых конкурентов и выгодно позиционировать свои продукты на фоне тех, которые настроены на другие киберриски.

---

[46] Scott Shane, Nicole Perlroth, and David E. Sanger, "Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core," *New York Times*, November 12, 2017, https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html.

[47] https://www.crunchbase.com/search/organization.companies/70fb49fd65d4beea2d65330825fd1023eed764a7.

Опросы и отчеты

Продемонстрировать уникальность на переполненном рынке всегда сложно. Чтобы добиться этого, поставщики IT-решений по кибербезопасности иногда используют опросы и отчеты, подчеркивающие их весомость и масштаб возможностей.

Игроки рынка, особенно не успевшие занять свою нишу, стремятся привлечь внимание, публикуя устрашающие прогнозы расходов на борьбу с киберпреступностью. Например, в отчете Cybersecurity Ventures за 2016 год говорилось о грядущем «хакеркалипсисе». Согласно прогнозам этой организации, в 2021 году мировой ущерб от киберпреступлений достигнет $6 трлн[48]. Для сравнения: это больше ВВП любой страны, кроме США и Китая.

Другой пример — компания CrowdStrike. Она расширила свой ежегодный отчет о глобальных угрозах, включив туда не только открытые данные о кибератаках в 2018 году, но и сведения о 90 млрд ежедневных инцидентов, которые зафиксировала платформа Falcon[49]. Мониторинг сетей, который выполняет Falcon, похож на вариант, предложенный правительством США (предыдущий раздел), и имеет те же ограничения и риски. Все 90 млрд

[48] Steve Morgan, "Hackerpocalypse: A Cybercrime Revelation," Cybersecurity Ventures, August 26, 2016, https://cybersecurityventures.com/annual-cybercrime-report-2016/.

[49] "2018 CrowdStrike Global Threat Report: Blurring the Lines Between Statecraft and Tradecraft," CrowdStrike, 2018, https://www.crowdstrike.com/resources/reports/2018-crowdstrike-global-threat-report-blurring-the-lines-between-statecraft-and-tradecraft/.

событий он атрибутирует одинаково — как атаки вредоносных программ — и не учитывает внутренние киберриски, например отключение недовольным IT-специалистом критически важной системы контроля воздушного пространства.

Поставщики услуг в сфере кибербезопасности привлекают внимание к своим коммерческим предложениям, сознательно искажая данные об угрозах. У этого подхода давняя история. Так, 19 марта 2009 года бывший старший вице-президент и глава службы безопасности компании AT&T Эдвард Аморозо сообщил Комитету по торговле, науке и транспорту Сената США следующее: «В прошлом году ФБР объявило, что доходы от киберпреступлений впервые превысили оборот наркоторговцев, всегда считавшийся наиболее прибыльным криминальным бизнесом и приносивший ежегодно более $1 трлн»[50]. Никаких ссылок на источник он не привел. Названный им доход киберпреступников был в 80 раз больше прибыли AT&T, а также превышал ВВП любой страны в мире, кроме первой дюжины[51]. Далее Аморозо предложил изменить приоритеты федеральных закупок так, чтобы стимулировать

[50] Слушания по усилению кибербезопасности в Комитете по торговле, науке и транспорту Сената США. Свидетельские показания старшего вице-президента и главы службы безопасности компании AT&T Эдварда Аморозо (19 марта 2009 года), https://www.commerce.senate.gov/services/files/e8d018c6-bf5f-4ea6-9ecc-a990c4b954c4.

[51] Чистая прибыль компании AT&T за тот год, когда Аморозо давал показания перед сенаторами, составила $12,5 млн (данные годового отчета за 2009 год: https://www.att.com/Common/about_us/annual_report/pdfs/ATT2009_Financials.pdf).

гражданские организации использовать решения AT&T по борьбе с DDoS-атаками[52].

Нерыночное регулирование спроса

Регулирование спроса с помощью госорганов, как в случае с Аморозо, — еще один хитрый ход, который поставщики услуг в сфере кибербезопасности используют, чтобы закрепиться на рынке и увеличить свои доходы.

В 2017 году израильская компания Cellebrite (подрядчик правительства США, производящий устройства для мобильной криминалистики) лоббировала принятие в штате Нью-Йорк закона, обязывающего использовать ее продукт Textalyzer для судебно-криминалистического анализа смартфонов всех водителей после ДТП. Textalyzer устанавливает факт отправки и получения водителем сообщений перед аварией[53]. В США 49 штатов уже приняли законы, запрещающие переписываться за рулем. Несмотря на это почти 18000 представителей правоохранительных органов каждый год сообщают о 6,3 млн автокатастроф,

---

[52] В 2009 году доходы киберпреступников составили $1 трлн, что уступает лишь ВВП 13 крупнейших стран мира. Международный валютный фонд, доклад о перспективах развития мировой экономики. Апрель 2012 года, http://www.imf.org/external/pubs/ft/weo/2012/01/weodata/index.aspx.

[53] "NYS Legislature Hosts Distracted Driving Lobby Day Event," YouTube video, 46:05, posted by NYSenate, April 24, 2017, https://www.youtube.com/watch?v=r3N0TL_WEtE.

вызванных в том числе нарушениями этого запрета[54]. Если учесть потенциальный объем рынка, неудивительно, что Cellebrite лоббирует принятие аналогичного закона в других штатах и на национальном уровне[55].

Компании манипулируют цифрами, чтобы привлечь внимание к конкретным киберрискам и решениям, способным их устранить[56]. Хотя многие отчеты, подготовленные представителями отрасли, содержат полезную информацию, необходимо оценивать актуальность конкретных рисков для вашей компании и критически воспринимать информацию о возможном ущербе.

---

[54] Законопроект Сената США S6325A, Sess. of 2015–2016 (NY2016), https://www.nysenate.gov/legislation/bills/2015/s6325/amendment/a; данные Страхового института безопасности дорожного движения (Insurance Institute for Highway Safety), "Cellphone Use Laws by State," дата обращения: January 13, 2021, https://www.iihs.org/topics/distracted-driving/cellphone-use-laws; отчет полиции о ДТП за 2015 г.: информация о дорожных авариях Национального центра статистики и анализа данных Министерства транспорта США, "Quick Facts 2016," https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812451.

[55] Данные управления программ правосудия Министерства юстиции США, "Census of State and Local Law Enforcement Agencies, 2008," July 2011, https://www.bjs.gov/content/pub/pdf/csllea08.pdf; "Distracted Operators Risk Casualties (DORCs): New York State Legislature and DORCs Announce Unique Efforts to Combat Distracted Driving," PR Newswire, April 5, 2016, https://www.prnewswire.com/news-releases/new-york-state-legislature-and-dorcs-announce-unique-efforts-to-combat-distracted-driving-300246450.html.

[56] В частности, лоббировались такие законы, как «Вопросы уголовного судопроизводства, национальной безопасности и цифровых улик, полученных в результате проведения судебной экспертизы», US Senate Lobbying Disclosure Act Database, "LD-2 Disclosure Form," accessed March 9, 2018, https://soprweb.senate.gov/index.cfm?event=getFilingDetails&filingID=1DE19BE9-5152-4AB3-8037-D7194268FD0B&filingTypeID=51.

Средства массовой информации

Как правило, мы узнаём то, что хотят донести до нас представители правительств и игроки рынка кибербезопасности, через новостные СМИ. Они же влияют на наше мнение о киберугрозах и борьбе с ними, на общее видение проблемы и степени ее приоритетности. Новостную повестку, связанную с кибербезопасностью, формируют два ключевых фактора.

Ничего секретного

СМИ могут говорить лишь о тех атаках или утечках данных, о которых им известно, которые уже в той или иной степени стали достоянием гласности. Такая информация распространяется несколькими путями.

— Иногда последствия утечки данных очевидны и их трудно скрыть, как в случае взлома энергосети Украины в 2015 году[57].
— Часто хакеры сами хвастаются превосходством над службами безопасности и обнародуют свои «трофеи». Вспомним взлом сайта знакомств Ashley Madison.

[57] E-ISAC and SANS ICS report, "Analysis of the Cyber Attack on the Ukrainian Power Grid," March 18, 2016, p. 4. Доступно по ссылке: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

Тогда хакеры опубликовали персональные данные 32 млн пользователей этого ресурса[58].

— Эксперты по кибербезопасности, которым удается обнаружить или проанализировать утечку, обычно также обнародуют результаты изысканий. Например, в мае 2018 года был опубликован отчет о серии хакерских атак, затронувших более 300 сайтов, в том числе сайты зоопарка Сан-Диего и правительства штата Чиуауа (Мексика)[59].

— Компании обязаны включать такие сведения в свои ежегодные отчеты (это требования регулятора). Пример – утечка персональных данных и конфиденциальной финансовой информации чуть ли не половины жителей США из Equifax, одного из трех крупнейших кредитных агентств в стране[60].

В то же время СМИ не вправе сообщать о засекреченных утечках данных или кибератаках, поэтому многие инциденты, включая хищения информации, составляющей коммерческую тайну, финансовые махинации и вымогательства, часто остаются неизвестными широкой публике.

---

[58] Kim Zetter, "Hackers Finally Post Stolen Ashley Madison Data," *Wired*, August 18, 2015, https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/.

[59] Troy Mursch, "Large Cryptojacking Campaign Targeting Vulnerable Drupal Websites," Bad Packets Report, May 5, 2018, https://badpackets.net/large-cryptojacking-campaign-targeting-vulnerable-drupal-websites/.

[60] Brian Fung, "Equifax's Massive 2017 Data Breach Keeps Getting Worse," Washington Post, March 1, 2018, https://www.washingtonpost.com/news/theswitch/wp/2018/03/01/equifax.

Запрос аудитории

Мы зависим от прессы, но и пресса зависит от нас. СМИ публикуют то, что хотят видеть их читатели. Принцип «плохая новость — это хорошая новость» справедлив и для цифрового мира, особенно если речь о кибератаках «коварного внешнего врага» — сложно организованных, никогда ранее не встречавшихся, грозящих катастрофой национального или глобального масштаба. А если наш коварный внешний враг еще и не использует в письменных коммуникациях латиницу? Сенсация!

Такая «страшилка» всегда даст сто очков вперед истории о заурядном маркетологе, без хакерских навыков похитившем корпоративные «бриллианты короны», которые плохо лежали. Хотя угрозы со стороны конкурентов, партнеров, клиентов, поставщиков и сотрудников куда распространеннее и наносят бизнесу куда больший ущерб, читателям подобные новости почти не интересны.

Итак, на деятельность правительств, СМИ и поставщиков услуг в сфере кибербезопасности влияют их функции, цели и стимулы. Анализируя это влияние, вы сможете критически переосмыслить кричащие газетные заголовки и понять, что действительно важно для вас и вашей компании. Теперь, когда мы обрисовали ситуацию в отрасли, можно посвятить остальную часть книги новому подходу к кибербезопасности, который позволит эффективно защищать компанию, ее акционеров и более широкий круг стейкхолдеров.

Часть II

Принципы

Эффективная стратегия кибербезопасности включает в себя понимание рисков, управление ими и возможность их устранить. Чтобы помочь компании справиться со всеми этими задачами, вам понадобятся лишь ваши обширные знания о бизнес-процессах и их специфике. Не обязательно разрабатывать стратегию с нуля или радикально трансформировать систему контроля. Но важно помочь компании вывести представления о кибербезопасности за пределы технических аспектов, а решения принимать исходя из интересов бизнеса и существующих рисков.

Чтобы помочь в этом, мы разработали четыре принципа цифрового управления. Эти принципы не требуют подготовки в области компьютерных технологий и могут быть немедленно применены на практике. Конечно, сколько бы советов по кибербезопасности вы ни изучили (включая те, что приведены в этой книге), вам вряд ли удастся подготовиться ко всему на свете. Но эти принципы, возможно, пригодятся вам в непредвиденной ситуации или новых обстоятельствах.

Наши четыре принципа можно использовать как лакмусовую бумажку: они помогут оценить эффективность управления киберрисками в вашей компании. Следует она им или нет? Как у вас организованы процессы, обеспечивающие защиту от киберугроз? К тому же с помощью

этих принципов вы наладите внутренний контроль над системой кибербезопасности. В их основе – понимание различий между вашими обязанностями и обязанностями других сотрудников вашей компании, особенно тех, кто отвечает за киберзащиту.

Благодаря этим принципам вы разберетесь в ситуациях и событиях, зачастую находящихся вне контроля специалистов по кибербезопасности, но при этом критически важных для их деятельности.

Глава 4

Если вы не понимаете, значит, вам плохо объяснили

Руководство и сотрудники вашего отдела кибербезопасности обязаны предоставлять вам материалы, отчеты и рекомендации в форме, доступной пониманию неспециалистов.

Текущая ситуация

Брифинги по кибербезопасности способны вогнать в ступор многих. Некоторые руководители говорили, что были бы рады уделять проблеме киберугроз больше времени на заседаниях совета директоров и профильных комитетов, но рекомендации, которые дают ответственные за этот вопрос коллеги, часто либо бесполезны, либо непонятны. Презентации полны «воды», будто готовившие их эксперты стремились просто заполнить отведенное для выступления время. А те самые эксперты в свою очередь

обижаются, ведь руководство не демонстрирует никакого стремления разобраться хотя бы в простейших, но очень важных терминах!

Если учесть разницу в образовании, опыте работы и функционале, обе стороны можно понять.

Последствия

Без актуальной, понятной информации о состоянии ваших бизнес-процессов нельзя оценить и способность компании выдержать кибератаки. Запутанные презентации не расскажут, насколько эффективны текущие или будущие инвестиции в безопасность. Не вникая в ситуацию глубоко, вы окажетесь ее заложником: вам останется либо одобрить финансирование без четкого представления о том, как это защитит ваш бизнес, либо урезать расходы и повысить риски. А потом что-нибудь случится – и придется посыпать голову пеплом. Получается какая-то информационная асимметрия.

В итоге контроль над системами кибербезопасности часто делегируют IT-отделу. Так вы полностью перекладываете ответственность на этих людей, но не до конца понимаете их цели и задачи. А ведь, не понимая, чем занимаются специалисты по кибербезопасности, вы не сможете ни контролировать их действия, ни подвергать сомнению решения, ни оценивать расходы.

Возможное решение

Настаивайте на том, чтобы специалисты по кибербезопасности формулировали выводы и рекомендации четко и понятно — а именно в контексте вашей компании и ее бизнес-процессов. Сама по себе информация о мощности системы контроля бесполезна, если вы не понимаете ее значения для защиты бизнеса. В следующей главе мы попробуем решить эту проблему, проследив взаимосвязи между бизнес-рисками, типами атак и средствами их предотвращения или смягчения последствий.

Без четкого представления о связи бизнес-рисков и кибератак рекомендации по безопасности будут лишь сбивать с толку — как репортажи о крикете, если вы бесконечно далеки от этого вида спорта. Термины «бэтсмен» или «боулер» так и останутся непонятными, не говоря уже о правилах игры, или, точнее, матча.

Глава 5

На кону всегда бизнес

Все вопросы кибербезопасности начинаются и заканчиваются проблемами бизнеса и рисками, связанными с его процессами и стратегией, а не с компьютерами и их уязвимостями.

Текущая ситуация

Стандарты, продукты и услуги, доступные специалистам по информационной безопасности, отнюдь не облегчают их работу. По сути, все эти вещи, скорее, подкрепляют тезис, что кибербезопасность — это защита компьютеров, а не бизнеса.

Признанные во всем мире стандарты, например Концепция кибербезопасности NIST и международные стандарты ISO 27000, описывают средства контроля, необходимые для защиты компьютеров и хранящейся на них информации. Там не говорится о том, как эти средства могут помочь в защите ключевых бизнес-процессов от кибератак. Как мы упоминали ранее, это не вина разработчиков, а скорее следствие внутренних ограничений самих

стандартов, разработанных для слишком широкого круга организаций.

Продукты и услуги кибербезопасности имеют одни и те же ограничения. Например, антивирусы защищают от вредоносного программного обеспечения, брандмауэры – от взлома через интернет, а шифрование данных необходимо на случай их утечки или кражи. Эти решения полезны для конкретных проблем, но каждое из них само по себе не годится для более глобальной задачи. Коммерческие соображения побуждают поставщиков ПО сосредоточиться на защите именно техники, а не бизнеса в целом. Целевой рынок универсальных, ориентированных на защиту компьютеров услуг намного обширнее, а затраты на их разработку намного ниже, чем у программ, предназначенных для устранения конкретных рисков в конкретных компаниях.

Последствия

Внешние факторы отнюдь не побуждают специалистов выходить за рамки технического подхода. На первый взгляд это даже кажется здравым – сосредоточиться на защите компьютерных систем, поскольку такая деятельность (например, установка обновлений) очень важна. Но проблема в том, что очень легко потратить все деньги и время на обслуживание компьютеров. А фундаментальная проблема защиты вашей компании в целом так и останется нерешенной.

Если люди, ответственные за кибербезопасность, не слишком разбираются в том, как функционирует ваш бизнес, возможны два варианта.

В первом случае их вмешательство приведет к нарушению отлаженных рабочих процессов. Так было, например, с автомобилестроительной компанией, чьи внешние партнеры потеряли доступ к необходимой информации, когда ее в целях безопасности переместили в корпоративную интрасеть. «Безопасность мешает вести бизнес» — стереотипное определение такого сценария, но мы отдаем предпочтение другой формулировке: «Неправильно выстроенная система безопасности мешает вести бизнес». Иными словами, чтобы грамотно защитить каждый конкретный бизнес, необходимо понимать, как он работает.

Во втором случае фокус на безопасности компьютеров приведет к тому, что ваша компания в целом будет недостаточно защищена. Если команда экспертов по кибербезопасности не разбирается в тонкостях ведения вашего бизнеса, то не сможет обеспечить его надежную защиту.

Возможное решение

Итак, внешних факторов и рыночных драйверов, которые стимулировали бы разработчиков создавать индивидуализированные (завязанные на конкретных бизнес-процессах) системы кибербезопасности, пока нет. Значит, придется найти альтернативу. Поскольку вы руководите компанией и держите все рычаги контроля, именно вам

придется побеспокоиться о ее поиске. Памятка «Управление киберрисками» содержит вопросы, которые помогут удостовериться, что ваша компания уделяет достаточно внимания этому аспекту.

Первое, что вам важно сделать, — признать, что устранение киберрисков подразумевает не только защиту компьютеров. На втором этапе нужно будет применить этот подход на практике, причем потребуется совместная работа и коллективная ответственность. Недостаточно поручить специалистам из IT-отдела обеспечить безопасность компании. Не менее важно, чтобы менеджеры среднего звена предоставили этим экспертам достаточно информации о своих рабочих процессах. Тогда киберзащита будет способствовать, а не препятствовать ведению бизнеса.

В своей предыдущей книге Digital Defense Томас Паренти отметил: «Любые меры по обеспечению кибербезопасности компании, не основанные на понимании того, чем она занимается, по определению неполны. Они могут защитить лишь против универсальных атак на ее компьютеры»[61].

Хотите узнать, не попала ли и ваша компания в эту распространенную ловушку? Задайте себе два вопроса:

1. Какими именно средствами ваша компания защищает свою ценную информацию и каждый автоматизированный бизнес-процесс?

[61] Thomas Parenty, Digital Defense: What You Should Know About Protecting Your Company's Assets (Boston: Harvard Business School Press, 2003), xvii.

2. Какую именно информацию и какие бизнес-процессы защищает каждая конкретная технология кибербезопасности, используемая вашей компанией?

Если вы не можете ответить на первый вопрос, нет оснований считать, что вы защищены. Если вы не можете ответить на второй, задумайтесь, точно ли ваш бюджет на кибербезопасность расходуется разумно?[62]

[62] Ibid. P. 23.

Глава 6

Кибербезопасность должна быть у всех на слуху

Рабочие процессы компании, ее жизнедеятельность и структура – все должно быть неотрывным от заботы о кибербезопасности. Выводите ее из тени, она – не просто часть чьего-то функционала.

Текущая ситуация

В большинстве компаний сотрудники согласны с тем, что кибербезопасность важна. Однако обычно они разделяют распространенное мнение, что за этот вопрос отвечают преимущественно их коллеги из IT-отдела. Такой показатель, как доля затрат на кибербезопасность в общем бюджете IT-отдела, укрепляет их в этом убеждении.

Рядовые сотрудники не сомневаются, что их ответственность в этой области ограничивается выбором достаточно

сложного пароля от учетной записи и отсутствием на мониторе стикера с ним. Иными словами, они не рассматривают заботу о кибербезопасности как часть своих обязанностей. В основе такого подхода лежит идея, что кибербезопасность – проблема космически сложная и дилетанты тут ничего полезного не сделают. Лучше оставить все профессионалам.

Последствия

Полное делегирование задач по обеспечению кибербезопасности кому-то одному (например, IT-отделу) приводит к тем же негативным последствиям, что и фокус на защите компьютеров вместо защиты бизнес-процессов. Автоконцерн из Азии, упомянутый в главе 2, – прекрасный пример. Решение IT-специалистов создать внутри корпоративной сети еще одну сеть для хранения данных, а также решение сотрудников компании создать фейковые аккаунты для внешних партнеров принимались без согласования между отделами R&D и IT. Между ними не было никаких организационных или операционных связей.

Первоначальная утечка информации, приведшая к миллиардным убыткам, не была результатом действий продвинутых киберпреступников, или иностранных хакеров, или даже злого гения-одиночки. За ней стоял кто-то из отдела маркетинга. Этот человек не обладал никакими хакерскими навыками, зато у него было кое-что весьма ценное – санкционированный доступ к технической

информации, которым он и воспользовался, чтобы скопировать файлы и вынести за пределы компании. На тот момент имелось множество антихакерских продуктов, которые могли бы предотвратить утечку информации и сопутствующие финансовые потери. Однако, как и разработчики, маркетологи работали в отрыве от IT-отдела. Более того, сотрудники отдела информационной безопасности, расположенного в Калифорнии, и сотрудники отдела маркетинга, находившегося в Азии, говорили буквально на разных языках.

Организационная и операционная обособленность функций кибербезопасности в компании ведет к брешам в защите. Другие подразделения зачастую даже не сомневаются, что IT-отдел позаботится обо всех киберрисках, возникающих в результате их деятельности; следовательно, это не их зона ответственности. Ну а в результате такого отношения IT-специалисты почти не контактируют с другими коллегами.

Возможное решение

Хорошая команда кибербезопасности — большая ценность. Мудрому руководителю важно стремиться к ее созданию: это поможет избежать многих бед. Отлично, если ваши эксперты по кибербезопасности вникнут в суть бизнеса и его цели, а затем используют эти знания, чтобы грамотно выстроить свою работу. В противном случае их действия будут столь же незаметны, как падение пресловутого

дерева в пустом лесу: никто не слышит — так, может, звука и нет?

Существует несколько способов убедиться в том, что специалисты по кибербезопасности пользуются влиянием в вашей компании и руководство их слышит. Один из этих способов касается организации рабочих процессов.

- Поместите группу специалистов по кибербезопасности в состав линейного подразделения, желательно сталкивающегося с высоким уровнем рабочих киберрисков. Этот подход противоположен тому, чтобы рассматривать ее как функциональную единицу (например, IT-отдел).
- Включите специалистов по кибербезопасности в штат структурных подразделений.
- Формируйте внутреннюю компетенцию в сфере кибербезопасности, особенно в подразделениях с наивысшим киберриском.

Иногда перевод специалистов по кибербезопасности в структурные подразделения в ближайшем будущем невозможен. В таком случае вам пригодятся формальные процедуры анализа и оценки киберрисков, предусмотренные — и выполняемые — в критически важных бизнес-процессах. Ключевой момент этого анализа (методика описана в главе 9) — отслеживание изменений, чреватых новыми киберрисками. Такие потенциально рискованные изменения включают:

— разработку новых видов продуктов или услуг;
— реорганизацию в процессе поглощения компании или слияния с ней, а также создание совместного предприятия;
— инновационные нововведения (например, освоение облачных технологий).

Глава 7

Не забывайте о мотивации

Знайте, чего хотят ваши сотрудники. Правильно мотивируйте их. Пусть они тоже будут заинтересованы в заботе о кибербезопасности.

Текущая ситуация

Мотивация сотрудников, зачастую с помощью материальных стимулов, — практика общепринятая, но редко рассматриваемая в контексте киберугроз. А ведь эффективность мер защиты снижается из-за того, что компании забывают поощрять правильное к ним отношение. Хуже того, внедрение некоторых неоднозначных стимулов (например, бонусов за соблюдение сроков доставки) иногда ставит крест на кибербезопасности в принципе.

Если компании мотивируют сотрудников укладываться в жесткие дедлайны, это может идти системе кибербезопасности во вред. Стивен Керр, бывший глава отдела обучения и лидерства в General Electric и Goldman Sachs, подробно раскрыл этот вопрос в статье On the Folly

of Rewarding A, While Hoping for B[63]. Тенденция характерна для многих компаний; касается как сотрудников, непосредственно отвечающих за кибербезопасность, так и их коллег, для которых подобные задачи – лишь небольшая часть должностных обязанностей.

Еще одна проблема – вопрос, какую именно модель поведения топ-менеджерам следует поощрять. Одно дело – мотивирование сотрудников, цели которых конкретны и очевидны (например, выполнение плана продаж). Мотивировать людей на хорошие результаты в области кибербезопасности (например, успешное отражение атак) гораздо сложнее: трудно учесть все действия и решения, которые, возможно, имели место раньше, в дежурство другого сотрудника, но повлияли на исход событий. А будете ли вы вознаграждать сотрудников за внедрение прогрессивных практик в сфере кибербезопасности или решите, что это лишь часть их работы? Например, доктора не получают бонусов за то, что их пациентам удалось выжить, а пилотам не выплачивают премии за благополучное приземление самолета.

Последствия

Одна глобальная финансовая компания со штаб-квартирой в США – яркий пример того, как персональная мотивация и интересы отдельных сотрудников отдела

[63] Steven Kerr, "On the Folly of Rewarding A, While Hoping for B", *Academy of Management Executive* 9, no. 1 (February 1995), accessed December 15, 2018, https://www.ou.edu/russell/UGcomp/Kerr.pdf.

кибербезопасности свели на нет работу корпоративных брандмауэров. Брандмауэры нужны, чтобы контролировать доступ в интернет. Они блокируют те сетевые подключения, которые могли бы использовать хакеры; защищают компьютеры от атак, но при этом должны допускать обычные, необходимые рабочие коммуникации — например, с бизнес-приложением для самообслуживания клиентов. Сотрудники IT-службы регулируют все эти механизмы, прописывая правила работы брандмауэра, то есть определяют перечень разрешенных и запрещенных контактов. Поскольку бизнес-приложения время от времени меняются, правила приходится обновлять и пересматривать. Когда мы спросили одного из сотрудников компании, специализирующейся на финансовых услугах, как часто они это делают, он ответил: «Никогда». В дальнейшей беседе удалось выяснить причину. Если компания подвергнется кибератаке (возможно, из-за неверно прописанных правил для брандмауэра), никто не обвинит в этом конкретно сотрудников IT-службы, особенно если есть возможность заподозрить иностранное государство. Если же сотрудники IT-службы, обновляя правила для брандмауэра, случайно заблокируют доступ к каким-либо бизнес-приложениям, то последствия наступят незамедлительно и придется спешно решать проблему.

А вот пример транснациональной страховой компании из Азии наглядно демонстрирует, как *большие аппетиты* могут вступить в противоречие с целями кибербезопасности. Эта компания постоянно наращивала расходы, реализуя стратегию агрессивного роста на основе поглощения конкурентов. Одновременно совет директоров инициировал

аудит киберрисков. Интересен факт, что аудит затрагивал лишь основную деятельность компании и не касался ни процессов, связанных с ее развитием, ни угроз, которыми чреваты слияния и поглощения. Расширение бизнеса имело наивысший приоритет, поэтому руководство не хотело рисковать задержкой или отменой подобных сделок. А ведь это грозило появлением новых рисков для основной деятельности и дополнительными расходами в результате выявления в поглощаемых компаниях проблем с кибербезопасностью.

Возможное решение

Нетрудно догадаться, что каждый конкретный сотрудник может поставить личные и сиюминутные интересы выше интересов компании в сфере кибербезопасности. IT-специалисты, пренебрегшие обновлением правил для брандмауэров, и инженеры-автомобилестроители, создавшие небезопасную бизнес-среду, чтобы помочь внешним партнерам получить доступ к корпоративной сети, лишь подтверждают этот тезис. Но обвинять этих людей в наплевательстве и эгоизме нет смысла. Не стоит забывать: именно руководство компании несет ответственность за то, чтобы подчиненные правильно определяли приоритеты.

Ключ к повышению кибербезопасности — понимание повседневных интересов и мотивации сотрудников. Если компания учтет их, принимая решения, то ее защита будет куда надежнее, чем если просто установить последнюю версию антихакерской программы.

Часть III

Задачи

Все, описанное в следующих трех главах, – основа основ, без которой эффективный надзор в цифровой среде невозможен. Работая в этом направлении, вы укажете компании ключевые процедуры, обязательные к исполнению; процессы, требующие особого внимания; результаты, которых хотите достичь. И никто не справится здесь лучше, чем вы.

Вот спектр ключевых целей вашей компании в сфере кибербезопасности:

- *идентификация киберрисков в контексте приоритетов бизнеса и его ценности;*
- *полная интеграция мер кибербезопасности в деятельность компании;*
- *лидерство и эффективное реагирование в случае чрезвычайных ситуаций в сфере кибербезопасности.*

Цифровое управление включает и такие обязанности, как привлечение стейкхолдеров, изучение нормативных материалов и всестороннее развитие сотрудников. И основу для этого создаете именно вы.

Глава 8

Управление киберрисками

Главная цель вашей компании в сфере кибербезопасности – управление рисками, с которыми ей приходится сталкиваться. Значит, долг руководства – обеспечить выявление, изучение, контроль и мониторинг киберрисков в соответствии с бизнес-приоритетами. Для начала ответьте на ряд взаимосвязанных вопросов, в том числе:

- С какими киберрисками нам приходится сталкиваться?
- Как кибератака может повлиять на наш бизнес?
- Принимают ли топ-менеджеры участие в оценке таких рисков?
- Разумны ли наши инвестиции в защиту от кибератак?
- Насколько эффективна наша киберзащита?

Последующие практические шаги помогут вам получить ответы на эти и многие другие вопросы. А сейчас мы рекомендуем освежить в памяти концепцию трех элементов управления киберрисками.

1. *Понятность киберриска.* Рассматривайте каждую киберугрозу в контексте тех бизнес-рисков, которые она может вызвать.
2. *Обоснованность мер кибербезопасности.* Оценивайте их с точки зрения тех бизнес-процессов, которые они защищают, а не просто с точки зрения предотвращения атак.
3. *Многообразие факторов эффективности.* Обращайте внимание не только на мощность сервисов кибербезопасности, но и на нетехнические факторы, определяющие успех.

Выявление киберрисков

Чтобы надзор за выявлением киберрисков был эффективным, убедитесь, что ваша компания:

— идентифицирует киберугрозы в контексте ключевых бизнес-процессов и угрожающих им рисков;
— вовлекает топ-менеджеров в процесс идентификации киберрисков и оценки их влияния на бизнес.

Связь между киберрисками и бизнес-рисками

CEO компании CLP (третьей по величине энергетической корпорации в Азии) Ричард Ланкастер смотрит на киберриски так: «Первоначально мы воспринимали киберугро-

зы как проблему, находящуюся в компетенции IT-службы. Но со временем мы поняли, что наши мощности по производству и передаче электроэнергии также могут оказаться под угрозой. Теперь мы знаем, что киберриск – это действительно бизнес-риск, а моя работа в должности CEO состоит именно в управлении бизнес-рисками»[64]. Топ-менеджеры и эксперты разделяют взгляды Ланкастера.

Проблема в том, как найти связь между кибер- и бизнес-рисками, а также как вовлечь в эту работу совет директоров и топ-менеджеров, обеспечив эффективную нейтрализацию киберриска.

Где же начинать поиск связей?

Самый очевидный путь – начать с конкретной киберугрозы, например внедрения вредоносных программ или взлома пароля, а затем представить, как это может отразиться на бизнесе. Сейчас многие игроки рынка средств кибербезопасности поступают именно так. Разработчики создают продукты для обнаружения коварного ПО и повышения безопасности авторизации; в стандартах описываются общие принципы устранения таких угроз. Увы, этого недостаточно, чтобы установить связь между киберрисками в целом и бизнес-рисками, характерными для вашей компании. Простое осознание факта, что вредоносные программы опасны, не помогает понять, чем именно они могут испортить жизнь вам.

Более практичный подход состоит в том, чтобы сначала идентифицировать ключевые виды деятельности

[64] Частная беседа 20 мая 2019 года.

вашей компании и связанные с ними риски. Исходя из этого специалисты по безопасности могли бы установить, каким образом кибератака может повлечь за собой ущерб.

Представьте: вы заседаете в совете директоров промышленной компании. Вы уже осознали важность ее производственных линий и риски, порождаемые тропическими штормами, отключением электроэнергии или неисправностью оборудования. Теперь задайте себе вопрос: каким образом вам может повредить кибератака? Вспомните о робототехнике. Важное преимущество автоматизации — простота переналадки сборочной линии на производство другого продукта: достаточно загрузить новую программу в управляющие роботами компьютеры. Но эта же гибкость делает вашу компанию уязвимой. Чтобы нарушить работу линии, хакерам всего-то нужно изменить программу, контролирующую роботов. В результате они будут функционировать неправильно или вообще остановятся.

Как видите, подход, при котором исходной точкой является анализ деятельности компании, дает экспертам по кибербезопасности четкое представление о дальнейших шагах по предотвращению вмешательства в ПО компьютеров, а значит, по нейтрализации бизнес-рисков.

Такая смена угла зрения может показаться незначительной, однако на самом деле она глобальна. Начав с ключевых видов деятельности компании, а также присущих им рисков и роли в них компьютерных систем, вы с остальными руководителями сможете отследить все связи между бизнес-рисками и киберрисками, а затем использовать эту информацию для выстраивания киберзащиты.

Разработка сценариев киберугроз

Рассмотрев киберугрозы в контексте рисков, характерных для вашего бизнеса, можно переходить к формированию общей базы данных для последующих дискуссий и решений.

Определение приоритетности рисков и мер по их нейтрализации — социальный процесс, а не техническая задача. Каждый, от руководства компании и специалистов по кибербезопасности до рядовых сотрудников IT-службы, может иметь собственное мнение по этому вопросу. Но вам необходимо привести их к общему знаменателю, чтобы двигаться дальше, имея согласованные представления о цели и направлении движения.

Рассказать историю — типичный способ собрать и структурировать информацию, а затем распространить ее среди самой широкой аудитории. Мы разработали сценарий киберугрозы, включающий четыре основных пункта (таблица 2). Для таких «историй» представители разных звеньев компании собирают и анализируют информацию коллегиально. Кроме топ-менеджеров и членов их управленческих команд к процессу могут привлекаться:

— сотрудники, вовлеченные в ключевую деятельность компании, например конструкторы автомобилей, клерки, выписывающие счета за рентгенологическое исследование, сотрудники отдела маркетинга (*операционная деятельность*);

Таблица 2. Четыре компонента сценария киберугроз

Компонент	Цель
Ключевые виды деятельности и риски	Выявить ключевые бизнес-процессы компании и сопряженные с ними риски
Вспомогательные системы	Понять, как компьютерные системы обеспечивают ключевые рабочие процессы компании
Кибератаки и их последствия	Выяснить, какие кибератаки угрожают ключевым бизнес-процессам и каковы возможные последствия
Киберпротивники	Предположить, кто может атаковать компанию

— сотрудники, ответственные за администрирование компьютерных систем, необходимых компании (*системы*);
— специалисты по техническим аспектам киберзащиты (*кибербезопасность*);
— персонал с компетенцией в разных областях — пра́ва, связей с общественностью, HR-ресурсов и физической защищенности (*эксперты*).

Далее рассмотрим каждый из пунктов подробно.

Ключевые виды деятельности и риски

Первый компонент сценария — анализ критически важных видов деятельности, описание их результатов (для компании) и связанных с ними рисков. Например, в химической компании, о которой мы уже упоминали, ключевой

вид деятельности — производство ароматических и полиэфирных смол.

Понятие критически важных видов деятельности варьируется в зависимости от особенностей компании и отрасли. Например, клиентская поддержка, как правило, отличается низкими рисками. Но если вы управляете казино, отдел работы с клиентами — критически важное подразделение. Казино в бывшей португальской колонии Макао[65] зависят от небольшой группы VIP-клиентов, или, как их тут называют, «китов», которые приносят около 54% валовой выручки[66]. Привлечение и удержание «китов» требует значительных инвестиций (например, предоставления им частных самолетов и роскошных апартаментов, а также эксклюзивного обслуживания в отелях и мишленовских ресторанах). Для казино риски, касающиеся отношений с клиентами, чреваты серьезной потерей прибыли.

Итак, вы определили ключевые виды деятельности вашей компании. Теперь нужно оценить присущие им риски.

---

[65] Сейчас Макао — специальный административный район в составе КНР (наряду с Гонконгом); функционирует как особая экономическая зона и имеет отдельную систему управления, отличную от остальной, социалистической, принятой в КНР (принцип «одна страна, две системы»). В этом городе площадью 32,9 км^2 проживает 650 000 человек (2020), и он считается одним из самых густонаселенных регионов в мире. Как португальская колония Макао просуществовал чуть больше четырех веков, с 1557 до 1999 года, когда район был передан Китаю. *Прим. ред.*

[66] Бюро по вопросам инспекции и координации игорного бизнеса Специального административного района Макао, доступ 17 января 2019 года, http://www.dicj.gov.mo/web/en/information/DadosEstat/index.html.

Есть два вида рисков, требующих особого внимания. Во-первых, это риски, не позволяющие компании извлечь максимум выгоды. В случае с химической компанией перебои в процессах (риск) приведут к срыву производства смол (следствие), а в результате снизится выручка от реализации (будет потеряно преимущество). Существуют также сопутствующие риски, которые могут повредить потребителям и остальным стейкхолдерам. Для химической компании это, например, выбросы вредных веществ. Чаще всего же встречается такой сопутствующий риск, как утечка конфиденциальной информации о клиентах – например, паролей и данных о кредитных картах.

Иногда разные риски переплетаются. Казино ориентируются на VIP-клиентов, приносящих максимум прибыли, и о них же собирают разного рода данные, включая среднее время, проводимое за игрой, средний размер ставки, среднее количество игроков в час и уровень мастерства. Эта информация помогает казино оптимизировать игровой опыт крупных игроков, а заодно и собственные прибыли. Финансовая информация о VIP-клиентах также очень ценна и охватывает не просто данные о кредитных картах игроков. В частности, сведения об их счетах в офшорах и недвижимости в разных уголках мира помогают решать вопросы о предоставлении дополнительного кредита и его погашении. Конкуренция за привлечение VIP-игроков очень жесткая, поскольку один такой клиент может увеличить прибыль казино на несколько миллионов долларов. Если такие сведения достанутся конкуренту, то помогут ему переманить ваших «китов». А попав в руки

налоговых органов или криминальных структур, они угрожают подорвать финансовое положение VIP-клиента в целом.

Однако, анализируя риски компании, не следует считать любой потенциальный риск того или иного вида деятельности серьезной угрозой. В 2006 году мы встречались с независимым членом совета директоров компании по производству жестких дисков, входящей в Fortune 500. Ее штаб-квартира располагалась в Кремниевой долине, а весь зал заседаний был увешан копиями патентов в золотых рамках – свидетельствами богатой инновациями истории. Глядя на эту выставку, вы наверняка бы решили, что риск хищения интеллектуальной собственности для компании во главе угла. Но, как оказалось, о нем здесь беспокоились меньше всего. Компания заключила соглашения о кросс-лицензировании со всеми основными конкурентами и переместила производственные мощности в Малайзию, которая вместе с соседями – Сингапуром и Таиландом – сосредоточила у себя 80% общего объема производства жестких дисков в мире[67]. Таким образом, преимущество компании состоит в производстве большого объема жестких дисков с низкой себестоимостью при сохранении высокого качества и надежности. И все благодаря инновациям – например, уникальной планировке производственных цехов, управлению цепочками поставок, контролю качества и грамотной HR-работе.

[67] A. Shameen, "Think Southeast Asia Is Taking a Backseat? Think Again: Singapore, Malaysia and the rest are booming by exporting to China," Chief Executive. Apr 1, 2006. P. 44–47.

То, что представляет существенный риск для одного бизнеса, не обязательно является таковым для другого. Хотя перебои в производстве смол наносят большой ущерб одной компании, торгующей бытовой химией, совсем не обязательно, что другая пострадает от них в той же мере. Возможно, ее химикаты не пользуются таким спросом, или не играют такой роли в общей прибыли, или у компании имеются легкодоступные альтернативные мощности.

Вам же на этом этапе необходимо удостовериться в том, что:

- вы идентифицировали ключевые бизнес-процессы, проанализировали их преимущества и оценили сопряженные с ними серьезные риски.

Рекомендации для этого шага приведены в главе 11 (таблица 4).

Новые бизнес-риски, порожденные информационными технологиями

Мощь кибератак приводит к появлению новых бизнес-рисков, которые в прошлом привлекали гораздо меньше внимания. Хороший пример — проблема конфиденциальности медицинской информации. Спрос на такую информацию на черном рынке резко растет, стоимость медицинской карты одного пациента со всеми данными

уже превысила $1000[68]. Больницы и контролирующие инстанции обратили внимание на этот факт. В 2017 году сеть больниц Advocate Health Care выплатила штраф в $5,5 млн департаменту здравоохранения и социальных услуг США за три последовательные утечки персональных данных 4 млн человек в 2013 году. Безусловно, любая больница должна учитывать риск утечки сведений о пациентах, но еще более серьезен риск не просто утечки, а изменения этих сведений.

Представьте ожесточенную конкуренцию между двумя сетями больниц. Ставки высоки, победа гарантирует большую прибыль. Как переманить пациентов? Ответ прост: взломать компьютеры конкурента и внести изменения в прописанные пациентам лекарства, их дозировку, диагнозы и назначения для оперативного вмешательства. Неправильное лечение или ошибочные назначения препаратов могут нанести вред пациенту или даже убить его. Замена слова «правая» на «левая» в направлении на операцию по удалению почки может обернуться смертным приговором пациенту, а возможно, и больнице. И дело не только в судебном преследовании за врачебную ошибку. Такие хакерские атаки приводят к утрате доверия. Кто ляжет в больницу, где его могут с одинаковой вероятностью как вылечить, так и убить?

---

[68] Brigid Sweeney, "The Frightening New Frontier for Hackers: Medical Records," Modern Healthcare, April 10, 2017, https://www.modernhealthcare.com/article/20170410/NEWS/170419987.

Сообщества военных и разведчиков уже долгое время обеспокоены проблемой обеспечения безопасности информации; первая работа по этому вопросу была опубликована еще в 1975 году[69]. В условиях постоянно возрастающего уровня автоматизации бизнес-процессов коммерческие компании также должны побеспокоиться об этом.

Вспомогательные системы

Целью кибератаки, как правило, являются компьютерные системы, обеспечивающие рабочие процессы. Таким образом, чтобы укрепить защиту, вашей компании нужно понять, какие компьютерные системы и сервисы находятся под угрозой, а также оценить их функциональность.

Здесь важно сразу привлечь операционный персонал: именно эти сотрудники ближе всего знакомы с используемыми компьютерными системами и приложениями, а также с последствиями их сбоев и остановок. Системные администраторы, обслуживающие эти ресурсы и лучше других представляющие их роль в работе компании (включая функции, о которых может не знать операционный персонал), также должны помочь. В целом можно сказать, что сотрудники IT-служб определяют задачи и функции

[69] K.J. Biba, "Integrity Considerations for Secure Computer Systems," MITRE technical report, June 30, 1975, http://seclab.cs.ucdavis.edu/projects/history/papers/biba75.pdf.

компьютерных систем общего назначения, а инженеры делают то же самое для автоматизированных систем управления производственными процессами.

Учитывая сложную структуру компьютерных систем и сетей, следует периодически проверять все жизненно важные для компании технологии. Проверка включает установление их физического местонахождения: сотрудники команды кибербезопасности должны знать, куда идти, чтобы принять контрмеры в случае атаки.

Ваша задача на этом этапе — удостовериться, что:

- компания заблаговременно проводит проверки компьютерных систем, поддерживающих ключевые виды деятельности, и данные актуальны.

Рекомендации для этого шага приведены в главе 11 (таблица 5).

Атаки и их последствия

Кибератаки

Следующий компонент сценария киберугрозы включает выявление и оценку разных видов атак, способных навредить вашему бизнесу. Для этого разберем предпосылки и критерии успешной атаки.

Говоря простыми словами, кибератака представляет собой ряд действий (так называемых векторов угрозы),

нацеленных на использование брешей компьютерной системы. Находящиеся в авангарде обороны сотрудники отдела кибербезопасности должны установить процедуры, применяемые в ходе атаки, и выявить те уязвимости, на которые они нацелены. Например, оружием червя WannaCry была хакерская программа, использовавшая программные ошибки в системах безопасности приложений Microsoft. Внутренняя уязвимость состояла в запуске таких приложений.

Кибератаки не обязательно бывают хитрыми или технически сложными. Например, для большинства компьютеров характерна такая уязвимость, как почти тотальный контроль администратора за приложениями и информацией. Такие полномочия необходимы для правильного функционирования и эксплуатации систем, однако допускают злоупотребления. В этом случае атака – не что иное, как злоупотребление администратора своими полномочиями.

Чтобы вызвать перебои в функционировании производственных мощностей, хакеры, как правило, используют два способа фальсификации программных инструкций. Один основан на внутренних особенностях автоматизированной линии, позволяющих перехватить контроль над загрузкой инструкций. В зависимости от конструкции роботизированного оборудования для этого может потребоваться или не потребоваться пароль или специальное разрешение. Второй способ – внедрение программы, использующей уязвимость в компьютерной системе и обходящей ограничения на загрузку внешних инструкций.

В обоих случаях хакеру необходимо подключиться к автоматизированной линии через сеть или при помощи флешки / другого приспособления.

Масштабы

Хакеры не ограничены географией. Они могут атаковать из любой точки земного шара и быстро парализовать всю компанию через компьютерную сеть. Например, кража данных о 94 млн кредитных карт из транснационального ритейлера TJX, имеющего 2000 торговых точек в Северной Америке и Европе, началась с парковки торгового центра в пригороде Майами: хакер подключился к Wi-Fi двух магазинов модной одежды Marshalls прямо из своего автомобиля[70]. Понятно, какую головную боль может создать такая кибератака. Ее последствия испытали на себе не только штаб-квартира компании Framingham в штате Массачусетс и сеть магазинов Marshalls, но и все сети связанных с ней брендов. Покупатели крупнейшей одноименной сети TJ Maxx также пострадали.

Кибератака иногда бьет по бизнесу значительно сильнее любых других преступных действий. В случае с хищением интеллектуальной собственности ценность информации, которую злоумышленники способны скачать с компьютеров компании, намного превышает ценность имущества, которое они могут вынести через дверь.

[70] United States of America v. Albert Gonzalez et al., 08 CR10.2.2.3 PBS (US District Court of Massachusetts, 2008).

Сейчас цифровой контроль критически важной инфраструктуры стараются усилить, и эта тенденция лишь подчеркивает уровень потенциальной угрозы. Например, в декабре 2015 года слаженные атаки на три украинские энергетические компании обесточили около 230 000 домохозяйств Ивано-Франковска на шесть часов[71]. Последующий анализ программы, использовавшейся хакерами, показал, что последствия могли быть куда серьезнее[72]. Кибератаки куда опаснее многих других преступлений именно потому, что за ними стоят серьезные противники.

Причины успеха

У кибератак нет универсального сценария. Далеко не все они одинаково просты в исполнении. Как научиться распознавать те их виды, которых стоит опасаться? В первую очередь вам следует понять, что требуется противнику для успешной кибератаки. У нее три ключевые предпосылки:

1. *Знания* (что должен знать ваш противник). Они варьируются от умения создавать хакерские программы

[71] E-ISAC and SANS ICS report, "Analysis of the Cyber Attack on the Ukrainian Power Grid," March 18, 2016, p. 4, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf; Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," Wired, March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid.

[72] Joe Slowik, "Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE," Dragos white paper, accessed December 3, 2018, https://dragos.com/whitepapers/CrashOverride2018.html.

до навыков управления системами, контролирующими работу гидроэлектростанции.

2. *Инструменты и оборудование* включают не только сами хакерские программы, но и, например, ноутбуки или радиопередатчики.
3. *Дислокация* – как в географическом (точка на карте), так и в организационном смысле (например, сотрудник или контрагент компании).

Расследуя мошенничество с дебетовыми картами банка из Юго-Восточной Азии, мы выяснили, что необходимые знания включали формат кодов авторизации Visa и Mastercard и умение настроить терминалы, принимающие карты. Инструментами стали, собственно, терминалы и база данных с номерами счетов дебетовых карт. Хакерам требовалось находиться поблизости, чтобы координировать свои действия с сообщниками, но не обязательно было работать в банке или хотя бы присутствовать в его стенах.

Оценив осуществимость разных видов атак, подумайте еще и о том, какие более простые, не связанные с киберпреступностью угрозы могут повредить вашему бизнесу. Например, страховая компания из Азии сначала беспокоилась, что ее агенты будут выписывать полисы, по которым сами же предъявят мошеннические требования, а поможет им в этом использование потенциальных уязвимостей мобильного приложения. Но потом компания поняла, что для таких афер агенту гораздо проще привлечь друга или родственника, то есть первоначальные опасения отпали в силу малой реалистичности.

Последствия

Хотя за разработку подобных сценариев отвечает корпоративный отдел кибербезопасности, операционный персонал и системные администраторы должны объяснить его сотрудникам возможные последствия атаки. Серия вопросов «Что, если?» может стать связующим звеном между этими подразделениями. Например, как будет обстоять дело с оказанием медицинской помощи, если данные о пациентах заблокирует программа-вымогатель? Национальной службе здравоохранения Великобритании после нашествия сетевого червя WannaCry пришлось «отменить тысячи назначенных приемов и операций»[73].

Некоторые последствия кибератак выходят далеко за пределы финансовых убытков. Например, в 2017 году вирус NotPetya нарушил деятельность многих крупных компаний по всему миру, включая AP Moller-Maersk, понесшую убытки в размере от $200 до $300 млн, и FedEx, чьи убытки составили $400 млн[74]. Фармацевтический гигант Merck оценил убытки от NotPetya в $670 млн как из-за прямых

[73] Owen Hughes, "WannaCry Impact on NHS Considerably Larger Than Previously Suggested," Digital Health, October 27, 2017, https://www.digitalhealth.net/2017/10/wannacry-impact-on-nhs-considerably-larger-than-previously-suggested/.

[74] Richard Milne, "Moller-Maersk Puts Cost of Cyber Attack at Up to $300m," Financial Times, August 16, 2017, https://www.ft.com/content/a44ede7c-825f-11e7-a4ce-15b2513cb3ff; Kim S. Nash, Sara Castellanos, and Adam Janofsky, "One Year After NotPetya Cyberattack, Firms Wrestle with Recovery Costs," Wall Street Journal, June 27, 2018, https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906.

потерь, так и из-за упущенной выгоды[75]. Но последствия для клиентов Merck могли оказаться куда серьезнее. Атака NotPetya парализовала многие мощности Merck, включая производство противораковой вакцины для детей от 11–12 лет[76]. К счастью, компании удалось получить вакцину из запасов Центров по контролю и профилактике заболеваний США и полностью удовлетворить спрос. Не случись этого, последствия кибератаки не ограничились бы финансовыми потерями: повысился бы риск развития рака у подростков.

Руководство компании и ее топ-менеджеры имеют достаточно возможностей выявить ключевые риски и определить меры предотвращения. Коллеги из других департаментов, в том числе специалисты по внутреннему аудиту, правам и финансам, могли бы помочь с анализом сопутствующих рисков. Встречи по этим вопросам важны, но совсем не обязательно должны отнимать много времени. Хорошо продуманные беседы и дискуссии — эффективный способ получить и обобщить информацию.

Ваша задача на этом этапе разработки сценария киберугрозы — удостовериться, что ваша компания идентифицировала:

---

[75] Там же.

[76] Bill Berkrot, "Merck Keytruda Sales Soar, But European Application Pulled," Reuters, October 27, 2017, https://www.reuters.com/article/us-merckco-results/merck-keytruda-sales-soar-but-european-application-pulledidUSKBN1CW1EF; Centers for Disease Control and Prevention, accessed February 3, 2019, https://www.cdc.gov/hpv/parents/questions-answers.html.

- виды кибератак, способные привести к наиболее серьезным рискам для ключевых видов деятельности;
- масштабы потенциального вреда от кибератаки (для компании и стейкхолдеров).

Рекомендации для этого шага приведены в главе 11 (таблица 6).

Киберпротивники

Кибератаки – не стихийные бедствия: они не происходят ни с того ни с сего, за ними всегда кто-то стоит. Вопрос в следующем: «Кто хочет вам навредить?» Возможны разные ответы: другие государства, преступные организации, конкуренты, недовольные сотрудники, террористы или общественные движения. Ланкастер из CLP отмечает: «Ситуация все время меняется. Критически важные объекты инфраструктуры, особенно энергетические компании, все чаще становятся объектом кибератак. Из числа противников нас в первую очередь беспокоят хорошо финансируемые организованные преступники и иностранные государства».

Идентификация потенциальных врагов, их мотивов и возможностей поможет вашей компании оценить вероятность кибератаки и определить меры, которые помогут ее отразить. Как уже говорилось в главе 2, современные хакерские программы легкодоступны. Это повышает

важность контроля таких аспектов, как финансирование, персонал и логистика.

Подумайте, что у вашей компании есть ценного для кого-либо еще. Например, конкурент, возможно, будет охотиться за результатами ваших исследований и разработок или коммерческими тайнами, а криминальная структура постарается украсть финансовую информацию о клиентах, чтобы продать ее на черном рынке.

Даже клиенты могут вас предать. AMSC (в прошлом American Superconductor) — некогда прибыльная компания, разрабатывавшая программное обеспечение для ветровых турбин, со штаб-квартирой в Девенсе (штат Массачусетс). В 2011 году один из ее крупнейших клиентов, Sinovel, внезапно прекращает платежи и отказывается вносить предоплату по заключенным контрактам, всего на сумму около $800 млн. Расследование показало, что Sinovel подкупила одного из европейских разработчиков AMSC, чтобы просто украсть ПО, а затем установить его более чем на тысяче турбин в Китае. В июле 2018 года, то есть через семь лет после кражи, американский суд взыскал в пользу AMSC $59 млн. Часть суммы была выплачена, но это и близко не возместило снижение акционерного капитала компании более чем на $1 млрд, не говоря уже о сокращении семисот рабочих мест — более половины общей численности ее персонала[77]. В результате

[77] Nate Raymond, "China's Sinovel Convicted in U.S. of Trade-Secret Theft," Reuters, January 24, 2018, https://www.reuters.com/article/us-sinovel-wind-gro-usacourt/chinas-sinovel-convicted-in-u-s-of-trade-secret-theft-idUSKBN1FD2XL.

хищения интеллектуальной собственности в 2010-м финансовом году AMSC сообщила об убытках на сумму $186 млн. Компании так и не удалось вернуться к прибыльности[78].

Может случиться так, что бизнес вашего противника превосходит по масштабам ваш собственный, да и ситуация на рынке складывается не в вашу пользу. Во время нашей встречи управляющие казино района Котай в Макао рассказывали о системе взаимодействия с клиентами, созданной, чтобы пополнять и анализировать базу данных о VIP-игроках. Сведения поступали из многих точек в Макао и через местную телекоммуникационную сеть передавались в единый операционный центр. Данные не шифровались — управляющие не видели в этом необходимости. Тогда мы задали вопрос: «Кому принадлежит телекоммуникационная сеть?» Казалось, в тот момент из комнаты выкачали весь воздух. Управляющие казино внезапно осознали, что телекоммуникационная фирма, имевшая неограниченный доступ к их ценнейшей информации, принадлежит концерну, куда входит их крупнейший конкурент.

Иногда сама отрасль или то, как ведется бизнес, тоже провоцирует кибератаки. Например, общества по охране окружающей среды иногда следят за компаниями с особенно большими выбросами вредных веществ, а бывший сотрудник АНБ Эдвард Сноуден похитил у работодателя информацию, доказывающую существование программ

[78] Годовые отчеты AMSC. Доступ 2 декабря 2018 года, https://ir.amsc.com/financial-information/annual-reports.

слежения, что АНБ публично отрицало[79]. В другом случае группа «Анонимус» организовала атаки против пяти нефтедобывающих компаний: Shell, BP, Exxon, «Газпрома» и «Роснефти», поскольку считала их ответственными за нанесение ущерба экологии Арктики[80]. Такие действия компаний, как массовые сокращения или закрытие предприятий, тоже могут подтолкнуть сотрудников к мести.

Также имеет смысл выйти за пределы компании и шире взглянуть на политическую и деловую среду, в которой она живет. Например, если справедливы подозрения, что за кибератаками на энергетические компании в Ивано-Франковске стояла Россия, то мотивы этих атак не имеют ничего общего с самими компаниями. Скорее всего, по ним был нанесен удар просто потому, что они находятся в Украине – стране, с которой у России сейчас более чем сложные отношения.

Топ-менеджеры располагают хорошими возможностями выявить потенциальных киберврагов компании. Но и тут возможны неожиданности. Атака WannaCry испортила жизнь множеству компаний по всему миру, а ведь между ними не было ничего общего за исключением того, что они не потрудились обновить операционные системы.

---

[79] Barton Gellman and Jerry Markon, "Edward Snowden Says Motive Behind Leaks Was to Expose 'Surveillance State,'" Washington Post, June 10, 2013, https://www.washingtonpost.com/politics/edward-snowden-says-motive-behind-leaks-was-to-expose-surveillance-state/2013/06/09/aa3f0804-d13b-11e2-a73e-826d299ff459_story.html.

[80] Kim Zetter, "Oil Companies Spring a Leak, Courtesy of Anonymous," Wired, July 16, 2012, https://www.wired.com/2012/07/oil-companies-hacked.

И, разумеется, не стоит забывать о лицах, имеющих свои счеты с компанией или просто стремящихся красивой атакой укрепить свою хакерскую репутацию.

Ваша цель – удостовериться в том, что ваша компания:

- анализирует спектр потенциальных киберпротивников, оценивает их возможности и мотивы, а также понимает, что делает ее желанной целью.

Рекомендации для этого шага приведены в главе 11 (таблица 7).

Когда хедж-фонды атакуют

В 2016 году специалисты по кибербезопасности из MedSec — фирмы, специализировавшейся на проблемах учреждений здравоохранения, — опубликовали доклад об уязвимостях электронных стимуляторов сердца и дефибрилляторов, производимых St. Jude Medical. Это транснациональная компания, изготавливающая широкий спектр медицинского оборудования и позже поглощенная Abbott Laboratories. Предварительно MedSec потратила полтора года на исследование оборудования от разных поставщиков. По словам CEO MedSec Жюстин Боне, «...St. Jude выделяется среди других компаний невнимательным отношением к проблемам безопасности»[81].

[81] Bloomberg, "MedSec's CEO: St. Jude Has History of Sweeping Things Under Table," YouTube, August 25, 2016, https://www.youtube.com/watch?v=curdJoTysF8.

Среди наиболее серьезных уязвимостей кардиостимуляторов этой компании была, к примеру, модификация программных команд имплантированного устройства с расстояния более 15 метров, что могло привести к прекращению подачи разряда или истощению батареи. Боне утверждает, что другие эксперты в сфере безопасности на основе исследования, проведенного в 2013 году, пришли к тем же выводам, но компания так ничего и не сделала.

Считая, что и в этот раз St. Jude не последует рекомендациям, MedSec решила пойти другим путем, чтобы привлечь внимание к выявленным уязвимостям и заставить компанию действовать. MedSec обратилась в инвестиционную фирму Muddy Waters, имевшую большой опыт в игре против акций тех или иных компаний. Если бы цена акций St. Jude упала, Muddy Waters получила бы прибыль. Предположительно MedSec координировала выход доклада об уязвимостях с игрой компании Muddy Waters на понижение акций St. Jude в соответствии с соглашением о разделе полученной прибыли. Общественность была настроена против MedSec и Muddy Waters, а St. Jude яростно отрицала наличие уязвимостей и подала в суд, обвинив компании в клевете[82].

В результате Министерство национальной безопасности США и Управление по контролю за качеством

[82] Tom Spring, "Researchers: MedSec, Muddy Waters Set Bad Precedent with St. Jude Medical Short," Threatpost, August 31, 2016, https://threatpost.com/researchers-medsec-muddy-waters-set-bad-precedent-with-st-jude-medicalshort/120266/.

пищевых продуктов и медикаментов провели расследование[83]. Управление выпустило предупреждение о том, что 460 000 кардиостимуляторов имеют уязвимости и их программное обеспечение следует обновить.

Если софт компьютеров в корпоративной сети можно обновить в один момент и удаленно, здесь возникла серьезная проблема: 460 000 пациентов должны были посетить своих лечащих врачей, чтобы обновить прошивку имплантированных кардиостимуляторов! К несчастью, в небольшом количестве случаев это приводило к «полной утрате функциональности»[84].

Этот случай позволяет сделать несколько интересных наблюдений. Во-первых, ущерб нанесла не кибератака. Доказательство того, что она могла бы достичь цели, разрушило репутацию St. Jude и инициировало расследование на федеральном уровне. Во-вторых, спорный способ выявления этого риска ради того, чтобы обрушить курс акций компании и обогатить биржевых спекулянтов, причинил ущерб всем акционерам, а не только St. Jude. В результате беспокоящиеся лишь о прибыли хедж-фонды и фирмы, исследующие вопросы кибербезопасности,

---

[83] Reuters, "Medical Supplier St. Jude Is Suing Short Seller Muddy Waters," Fortune.com, September 7, 2016, http://fortune.com/2016/09/07/st-jude-sues-muddy-waters/.

[84] Управление по санитарному надзору за качеством пищевых продуктов и медикаментов США. "Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication," August 29, 2017, https://www.fda.gov/medical-devices/safety-communications/firmware-update-address-cybersecurity-vulnerabilities-identified-abbotts-formerly-st-jude-medicals.

также попали в список потенциальных противников. Можно подумать, раньше их было недостаточно. И все же именно очевидное нежелание St. Jude ликвидировать потенциальную уязвимость дополнительно мотивировало его киберпротивников действовать так грубо.

Сценарии киберугроз в действии: графство Маручи

Приведем пример кризиса, развивавшегося точно по стандартному сценарию киберугрозы. Этот инцидент лишний раз свидетельствует о том, что рассказать историю — самый удобный способ понятно объяснить технические аспекты кибератаки и защиты от нее. Первый принцип цифрового контроля — «если вы этого не понимаете, вам плохо объяснили» — вполне реализуем на практике.

Графство Маручи — пасторальное комьюнити и место паломничества туристов примерно в сотне километров к северу от Брисбена (Австралия), в Саншайн-Коаст (Квинсленд). Тихий океан, вода теплая круглый год, а типичный прогноз погоды звучит примерно так: «Прекрасная погода сегодня, и еще лучше завтра». Отличная экология. Невероятные красоты: протяженные пляжи с белым песком, потрясающие озера, субтропические дождевые леса, глубокие ущелья, прозрачные ручьи и шумные водопады. Здесь живут коалы и многие редкие птицы, например буроголовый траурный какаду и земляной попугай.

Компания Maroochy Water Services управляет водоснабжением графства: ее деятельность включает забор, очистку и распределение воды, а также сбор и обработку около 35 млн литров сточных вод в день[85]. Это предприятие критически важно для Маручи. Поскольку разные территории графства находятся на разной высоте над уровнем моря, система канализации включает 142 насосные станции, расположенные в стратегических точках 880-километровой сети Maroochy Water Services. Сточные воды закачиваются на достаточную высоту, а оттуда самотеком под действием силы тяжести поступают на очистные сооружения.

Maroochy Water Services имеет централизованную систему управления: из одной точки операторы могут включать и выключать отдельные станции, а также регулировать мощность насосов. Станциями можно управлять и на месте, а размещенные на них приборы способны передавать команды, чтобы контролировать работу других станций.

В конце января 2000 года система управления операциями начала вести себя странно: терялась связь с насосными станциями, нарушался контроль их работы, а иногда подавались ложные сигналы тревоги[86]. Несколькими неделями позже обслуживающая компания поняла, что причина в хакерской атаке, но было поздно. Ко времени, когда

[85] Joseph Weiss, Protecting Industrial Control Systems from Electronic Threats (New York: Momentum Press, 2010), 109.

[86] Nabil Sayfayn and Stuart Madnick, "Cybersafety Analysis of the Maroochy Shire Sewage Spill," working paper, MIT Sloan School of Management, May 2017, http://web.mit.edu/smadnick/www/wp/2017-09.pdf.

проблему диагностировали, сточные воды переполнили резервуары и потекли по графству ручьями. Они затопили соседние районы, приливно-отливную сеть и даже поле для гольфа, где проводился чемпионат PGA Австралии – при пятизвездочном отеле Hyatt Regency Coolum Resort[87]. В близлежащем городке Пасифик Парадайз «до миллиона литров неочищенных сточных вод попали в ливневую канализацию»[88]. В местных парках и русле реки «...все живое погибло, вода в ручьях стала черной, а жители страдали от ужасной вони»[89]. И все это последствия кибератаки.

Все закончилось вечером 23 апреля, после того как полиция обнаружила подозрительную машину возле насосной станции в городке с говорящим названием Десепшен-Бей (*Залив Обмана. – Прим. пер.*). В салоне были найдены украденные приборы для контроля насосов, компьютеры, сетевые кабели и радиооборудование – полный арсенал для кибератаки. Примерно три месяца машина злоумышленника служила ему мобильным центром управления; за это время он организовал более сорока атак и затопил канализационными стоками чистейший уголок природы!

Злоумышленником оказался бывший сотрудник компании, поставлявшей контрольные приборы на насосные станции. С работодателями он регулярно конфликтовал.

---

[87] Cornelia Dean, "Indulged on Australia's Sunshine Coast," New York Times, April 4, 1993, https://www.nytimes.com/1993/04/04/travel/indulged-on-australia-s-sunshine-coast.html.

[88] Glenis Green, "Hacker Caused Sewage Overflows, Court Told," Courier-Mail, October 17, 2001, https://www.mail-archive.com/cybercrime-alerts@topica.com/msg00577.html.

[89] Там же.

Дважды этот человек пытался устроиться в Maroochy Water Services, но безуспешно; в итоге, рассерженный и обиженный на весь свет, он решил отомстить обеим компаниям[90]. Зная устройство системы операционного контроля, он смог установить радиосвязь с приборами отдельных насосных станций, что и привело к их странному поведению. В кибератаке использовалось то же оборудование, которое обеспечивало управление насосами, но теперь оно стало мощным оружием.

Атака велась в два этапа: подключение к системе контроля одной насосной станции, а затем манипулирование ею с целью нарушить работу и парализовать центральную систему управления. Для успеха обиженному хакеру хватило двух уязвимостей в системе кибербезопасности: первая состояла в том, что для доступа к оборудованию не запрашивался пароль, а вторая – в том, что радиочастоту, на которой осуществлялась связь с системой контроля, легко было узнать из технической документации. Для проведения кибератаки требовалось находиться в зоне устойчивой радиосвязи, но совсем не обязательно – на самой насосной станции.

Успеху диверсии немало способствовало то, что злоумышленник располагал инсайдерской информацией. Тем не менее и без этого организовать ее не так уж сложно, поскольку информация, ранее известная только сотрудникам и подрядчикам компании, теперь доступна всем, у кого есть интернет. Потратив некоторое время на веб-поиск,

[90] Glenis Green, "Hacker Jailed for Sewage Sabotage". The Brisbane Courier-Mail, Brisbane, Australia, November 1, 2001.

можно загрузить протоколы коммуникации, документацию по продукту, инструкции по программированию и ПО для оборудования, аналогичного используемому на насосных станциях. На форумах специалисты с удовольствием ответят на ваши вопросы и посоветуют, как правильно эксплуатировать оборудование такого типа, а достать его помогут интернет-магазины известных брендов и онлайн-аукционы. Поэтому хакеры могут планировать и тестировать атаки, с комфортом расположившись дома или в офисе в любой точке земного шара.

Последствия этого нападения могли оказаться куда серьезнее. Если бы вышли из строя все насосные станции, графство утонуло бы в сточных водах, что привело бы к экологической катастрофе. Страшное преступление, а для злоумышленника куда менее затратное, чем, например, взрыв одной из насосных станций.

Из ситуации с Maroochy Water Services можно сделать несколько выводов (см. таблицу 3). Один из них таков: важно понимать, как хакер может использовать уязвимости вашей системы. Другой говорит о необходимости выбрать адекватные инструменты для отражения атаки.

В данном случае требовались всего две предосторожности: установка пароля для доступа к системе контроля насосных станций и шифровка радиосообщений. При этом, поскольку злоумышленник не использовал вредоносные программы, такие типичные контрмеры, как покупка антивируса и обучение сотрудников антифишингу, оказались бы бесполезными.

Таблица 3. Четыре компонента сценария киберугрозы в графстве Маручи

Компонент	Ситуация в графстве Маручи
Ключевые виды деятельности и сопряженные с ними риски	Вид деятельности: переработка сточных вод. Риск: сбой в функционировании насосных станций
Вспомогательные системы	Централизованная система управления операциями. Приборы системы контроля на насосной станции
Кибератаки и их последствия	Эксплуатация незащищенной сети коммуникаций, недостатки в системе авторизации при входе в систему управления насосными станциями. Масштабный сброс неочищенных сточных вод
Киберпротивник	Обиженный бывший сотрудник

Как видите, объяснение технических аспектов и средств противодействия этой атаке вполне понятно неспециалисту. Именно такие примеры гипотетических киберрисков компания обязана довести до всех сотрудников.

По мере того как вы идентифицируете риски, становится очевидным еще один вывод: важно постоянно анализировать систему кибербезопасности на предмет недоработок и ошибок. Незащищенный доступ к системе контроля и отсутствие шифрования сообщений как раз и были такими недоработками. Ключевые ошибки в случае мошенничества с дебетовыми картами, о котором мы писали ранее, – технические баги в протоколах одобрения онлайн-платежей, изъяны при разработке процедур соблюдения времени оплаты и решения спорных вопросов. Компания

может выявить эти уязвимости, только если будет анализировать киберриски в контексте своей бизнес-деятельности.

Сценарии киберугроз — в центре внимания компании!

Использование сценариев киберугроз для выявления наиболее важных киберрисков вашей компании — весьма полезный и эффективный метод цифрового надзора по ряду причин. Перечислим их.

Смена угла зрения. Идентификация и оценка приоритетности киберрисков переводит их обсуждение из технической плоскости в плоскость защиты ключевых направлений бизнеса. Руководство компании может участвовать в этом процессе, а вы (вместе с остальными членами совета директоров) должны его возглавить.

Технические аспекты в контексте предпринимательской деятельности. Сбор, анализ и систематизация технической информации, имеющей отношение к кибератакам, уязвимостям компьютеров и информационной инфраструктуры, важны. Они помогут сформировать базу знаний, необходимую для эффективной защиты ключевых направлений вашего бизнеса.

Практический подход. Необходимо определить, как именно вы будете собирать информацию, анализировать ее и принимать решения, а также выделить те категории персонала, которые лучше других смогут вам

помочь. Возможно, ваша компания и так уже решает многие из этих задач, поэтому без особого труда разработает сценарии киберугроз на основе координирования уже ведущейся работы и собранных сведений.

Содействие сотрудничеству и умение находить общий язык. Разработка сценария киберугроз может стать основой для мобилизации усилий и взаимодействия самых разных бизнес-единиц — от топ-менеджеров и специалистов по кибербезопасности до рядового персонала, а также сотрудников, управляющих вспомогательными компьютерными системами. Это поможет достичь консенсуса относительно приоритетности киберрисков, а также возможных методов их устранения.

Унификация информации, связанной с киберрисками и бизнес-рисками. Сценарий киберугрозы содержит набор сведений, помогающих связать атаки, потенциальные бизнес-риски и ключевые виды деятельности. Команды и отдельные сотрудники вашей компании будут использовать разные фрагменты этого набора в соответствии со своим функционалом, но «красная нить», проходящая через этот документ, поможет объединить усилия в идентификации, определении приоритетов и управлении наиболее важными киберрисками.

Создание прочной базы для цифрового управления. Систематизация и презентация киберрисков в контексте бизнес-рисков создает основу для реализации других

функций, связанных с кибербезопасностью. Сюда относятся управление киберрисками, о котором мы поговорим далее в этой главе, а также обеспечение устойчивости компании перед лицом инициированных киберугрозами кризисов, о чем пойдет речь в следующей главе. Рассмотрение киберрисков в контексте бизнес-рисков влияет также на решение проблем организационной структуры и корпоративной культуры, от которых во многом зависит информационная безопасность компании.

Вовлеченность руководства и осуществление надзора. Ваша роль в разработке сценариев киберугроз понятна. Не менее очевидно, что сотрудники должны детально отчитываться вам о проведении всех мероприятий и проработке всех вопросов, связанных с киберрисками.

Отражение кибератак

Ваша ответственность в области нейтрализации киберрисков — надзор. Вам необходимо удостовериться, что ваша компания:

- анализирует приоритетность киберрисков, прогнозируя, как та или иная атака повлияет на ключевые виды деятельности;
- выбирает меры контроля с учетом приоритетности рисков;
- анализирует эффективность применяемых мер;

— разрабатывает планы нейтрализации киберрисков, непосредственно увязывая меры контроля с видами деятельности, которые они призваны защищать.

Определение приоритетности кибератак

С практической точки зрения киберриски — не что иное, как кибератаки, вызывающие бизнес-риски. Определение приоритетности киберрисков неразрывно связано с определением приоритетности кибератак. Очень удобно, когда всю необходимую информацию компания может найти в сценариях киберугроз.

Базовый критерий приоритетности кибератаки — ее способность причинить вред компании. Таким образом, логично начать с первого этапа сценария киберугрозы, где выявляются ключевые виды деятельности и присущие им внутренние риски. Это напоминает о втором принципе цифрового управления: «На кону всегда бизнес. Все вопросы кибербезопасности начинаются и заканчиваются проблемами бизнеса и рисками, связанными с его процессами и стратегией, а не с компьютерами и их уязвимостями».

Идентифицировав ключевые виды деятельности и сопряженные с ними риски, можно переходить к следующему этапу — выявлению рисков, которые приводят к самым мощным и опасным кибератакам. Оставшиеся этапы

помогут оценить их вероятность и разрушительный потенциал.

Проанализировав вспомогательные системы (на втором этапе), можно переходить к идентификации атак, способных воздействовать на ключевые виды вашей деятельности. Далее определите критерии успешных кибератак, а также глубину и масштаб их воздействия. Необходимо выявить те атаки, последствия которых будут наиболее серьезными, и те, которые проще осуществить. Наконец, следует оценить мотивацию и возможности потенциальных противников.

Оценка приоритетности киберрисков – не только фундамент для выбора мер безопасности, но и основа обучения занятого в этой сфере персонала. Координируя этот процесс, вы удостоверитесь, что средства, выделяемые компанией на кибербезопасность, оптимальны для нивелирования наиболее серьезных бизнес- и киберрисков.

Степень приоритетности кибератак должна оцениваться на основе:

- их способности подорвать ключевые виды вашей деятельности;
- спектра возможных последствий;
- ресурсов, необходимых для успешной атаки;
- мотивации и потенциала вероятных киберпротивников.

Рекомендации для этого шага приведены в главе 11 (таблица 8).

Выбор мер контроля

Определив приоритетность возможных кибератак, переходите к следующему шагу – выбору подходящих средств защиты. Взаимосвязи между способами кибератак и уязвимостями вспомогательных бизнес-систем – хорошая основа для поиска адекватных мер контроля.

Стандарты, например ISO/IEC27002 «Информационные технологии. Технологии безопасности. Практические рекомендации по информационной безопасности», могут помочь в этом вопросе, поскольку там рассматривается потенциал разных мер контроля с точки зрения типичных проблем кибербезопасности[91].

Когда компания выбирает способы защиты от кибератаки, может оказаться, что в совокупности они эффективнее, чем по отдельности. Раньше, когда кибербезопасность сводилась к контролю корпоративных сетей, предпочтительным техническим решением были брандмауэры. В наши дни они дополняются системами, выявляющими и предотвращающими проникновение, анализом журналов безопасности и прочими мерами. В случае с киберзащитой целое определенно сильнее суммы частей: совокупность мер защиты компенсирует ограниченность любой отдельно взятой меры.

[91] "Information technology – Security techniques – Code of practice for information security controls / Technologies de l'information – Techniques de securite – Code de bonne pratique pour le management de la securite de l'information," ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission), Geneva, Switzerland, 2013.

Меры могут быть не только технические, но и физические и процедурные. Применяя их в совокупности, нейтрализовать киберриски получится более эффективно и менее затратно. В 1980-х годах мы сертифицировали систему безопасности компьютеров в пусковых шахтах ядерных ракет. Существовало опасение, что некоторые требования безопасности, приведенные в стандарте Министерства обороны 5200.28, помешают расчету на боевом дежурстве выполнить президентский приказ. Мы учитывали это опасение и ориентированность мер контроля на нейтрализацию рисков. Мы также понимали, что физический контроль более эффективно решает проблему авторизации и учета посещений, чем компьютерные системы безопасности где-то глубоко в ракетной шахте. Благодаря включению физических мер контроля в общий набор мы добились более высокого уровня безопасности с меньшими затратами.

Выбирая способы контроля, важно проверить, как они будут работать на практике, в ходе повседневной деятельности. Иначе можно выбрать меры, на первый взгляд вполне приемлемые, но либо не способные обеспечить надежную защиту бизнеса, либо даже усиливающие риски.

Глобальная финансовая организация, чей годовой бюджет на нужды кибербезопасности измеряется сотнями миллионов долларов, — яркий пример того, почему важно учитывать специфику бизнеса. Ее сотрудникам необходимо пересылать конфиденциальную информацию внешним партнерам — как крупным институциональным организациям, так и мелким подрядчикам. Риск, что эти

имейлы кто-то перехватит, серьезен. Чтобы нейтрализовать его, организация внедрила собственную систему шифрования электронной почты, обезопасившись от перехвата имейлов, а дополнительно задействовала так называемую технологию предотвращения потери данных (data loss prevention – DLP), позволяющую определить, есть ли в имейле конфиденциальная информация. Для этого DLP использует ряд процедур – от сопоставления с шаблоном до сложного эвристического анализа. Эта технология применяется, чтобы не допустить утечки данных.

Финансовая организация использовала DLP, чтобы удостовериться, что вся исходящая информация зашифрована. Но DLP проверяла *только* содержание незашифрованных писем! Это означало, что, если третьей стороне отправлялся зашифрованный имейл, в нем могла содержаться любая конфиденциальная информация, и никто бы об этом не узнал. Не проанализировав способ организации бизнес-коммуникаций, отдел кибербезопасности по иронии судьбы сам же создал канал, которым любой инсайдер мог воспользоваться для безопасной и скрытой пересылки любых «бриллиантов короны».

Ваша задача – удостовериться, что компания:

- выбирает меры контроля исходя из их соответствия задаче нейтрализации приоритетных кибератак.

Рекомендации для этого шага приведены в главе 11 (таблица 9).

Проверка эффективности мер контроля

Если ваша компания выбрала контрмеры для нейтрализации наиболее значимых киберрисков, нужно оценить их эффективность. Пока эти меры не внедрены, не получится проверить их, зато вам может пригодиться анализ «человеческого фактора». Рассмотрим два аспекта: 1) управление системой контроля специалистами по кибербезопасности; 2) поведение людей, сталкивающихся с системой контроля.

Управление системой контроля

Во внешней среде действует множество факторов. Иногда они мешают качественному управлению системой кибербезопасности и снижают ее эффективность. В главе 7 мы рассказывали, как слишком динамичная среда одной финансовой компании мешала сотрудникам IT-службы в правильном конфигурировании брандмауэров. Если бы они выполняли свои обязанности надлежащим образом, то вызывали бы на себя огонь критики со стороны коллег и столкнулись бы с немалым давлением.

Еще один важный фактор — растущая сложность технических средств кибербезопасности, а значит, и их настройки, управления и использования. Например, защита внутренней корпоративной сети, вспомогательных систем и информации объединяет множество мер: от брандмауэров и средств, предотвращающих незаконные проникновения, до мониторинга сетевых коммуникаций. Каждое устройство, задействованное в защите сети, так же как

подключенные к ней компьютеры, фиксирует события со своего участка. Индивидуальные журналы регистрации «запоминают», например, неудавшуюся смену пароля или отключение антивирусной программы.

Эти журналы – не слишком ценная мера кибербезопасности, если рассматривать их по отдельности. Но если объединить их и проанализировать, вы получите достаточно эффективное средство выявления и предотвращения кибератак. Рынок, в свою очередь, предлагает множество журналов регистрации и аналитических программ. Их способность собирать и анализировать миллионы записей – палка о двух концах, поскольку трудно понять, какие события наиболее важны и в каких случаях следует проводить расследование. Чтобы устранить этот нюанс, поставщики предлагают шаблонные решения конкретных проблем, например «подгонку» под стандарты безопасности для платежных карт[92]. Но эти решения имеют тот же недостаток, что и любые стандарты: не учитывают индивидуальные особенности бизнеса конкретной компании и потому не могут отсортировать записи в регистрационных журналах по важности. В результате специалисты по кибербезопасности сомневаются в эффективности анализа журналов для нейтрализации киберрисков.

[92] Mary K. Pratt, "What Is SIEM Software? How It Works and How to Choose the Right Tool," CSO.com, November 28, 2017, https://www.csoonline.com/article/2124604/network-security/what-is-siem-software-how-it-works-andhow-to-choose-the-right-tool.html.

Работа со сценариями киберугроз решает проблему эффективнее. Это хороший способ идентифицировать процедуры, связанные с наиболее опасными атаками на критичные для бизнеса компьютерные системы. Без этих ориентиров специалисты по кибербезопасности чувствуют себя примерно как радиоастрономы программы SETI, тщетно пытающиеся услышать сигналы инопланетян во Вселенной.

До утечки информации в 2013 году крупный ритейлер Target в США вложил большие средства в покупку продвинутых программ, выявляющих и регистрирующих кибератаки. Благодаря этому компания получила множество предупреждений, что системы подвергались атаке непосредственно перед утечкой, но не приняла должных мер[93]. По собственному признанию, Target просто завалило «огромным количеством технической информации в регистрационных журналах»[94]. Если бы Target приобрела программы анализа журналов и приложила больше усилий для выявления признаков наиболее актуальных кибератак, то, возможно, не упустила бы важные тревожные сигналы. Компания могла не допустить утечки данных примерно 70 млн клиентов.

---

[93] Michael Riley, Ben Elgin, Dune Lawrence, and Carol Matlack, "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It," Bloomberg Businessweek, March 17, 2014, https://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data.

[94] Elizabeth A. Harris and Nicole Perlroth, "Target Missed Signs of a Data Breach," New York Times, March 13, 2014, https://www.nytimes.com/2014/03/14/business/target-missed-signs-of-a-data-breach.html.

Поведение людей

Вышеупомянутые средства анализа регистрационных журналов – пример контрмеры, очевидной для всех сотрудников, кроме специалистов по кибербезопасности. Многие другие способы контроля не только очевидны сотрудникам, но и непосредственно затрагивают их интересы. И то, как люди поведут себя, столкнувшись с такими вещами, может серьезно снизить эффективность мер безопасности и создать новые киберриски. В главе 2 мы обсуждали, как перенос сведений о разработках автоконцерна в интранет, осуществленный с благими намерениями, побудил сотрудников создать фейковые аккаунты для внешних партнеров. Конструкторы умышленно предприняли действия, подрывавшие систему кибербезопасности, поскольку она мешала им нормально работать.

Неумение прогнозировать вполне предсказуемое поведение людей может свести на нет весь контроль и повысить риски ущерба, которые предполагалось нейтрализовать. Такая мера, как ежедневное мытье рук, наглядно иллюстрирует эту мысль.

Благодаря уникальной анатомии больших пальцев наши руки идеально управляются с любыми предметами, в том числе покрытыми бактериями и вирусами. Выделяющийся на ладонях кожный жир связывает всю эту заразу и служит главным каналом ее попадания в наш организм. Дело может кончиться инфекцией. Мытье рук с мылом давно доказало свою эффективность в профилактике многих заболеваний. Мыло химически разлагает содержащий патогенные микроорганизмы жировой слой, позволяя

воде смывать их. Древняя история мыла как основного средства для чистоты рук была поставлена под сомнение в 1972 году: в его состав начали добавлять антибиотики[95]. На первый взгляд, антибактериальное мыло — хорошая идея. Но с тех пор люди стали тратить на мытье рук гораздо меньше времени, и антибиотики оказались практически бесполезными: они должны оставаться на коже не менее двух минут, чтобы подействовать. Большинству из нас не хватает терпения, чтобы мыть руки так долго. Многочисленные научные исследования подтвердили эту очевидную истину: в среднем на мытье рук человек тратит шесть секунд[96]. Антибактериальное мыло также отрицательно влияет на окружающую среду, нарушая процесс фотосинтеза и стимулируя появление бактерий, устойчивых к антибиотикам.

Нечто подобное есть и в сфере кибербезопасности. Касается это внедрения процедур авторизации — пожалуй, наиболее явных и обременительных мер контроля. Многие компании требуют от сотрудников регулярно менять пароли: раз в месяц или в квартал. Смысл в том, чтобы нейтрализовать риск взлома путем анализа личной информации сотрудника или методом автоподбора. Частая смена пароля заставит хакера каждый раз начинать взлом

---

[95] Во время раскопок Древнего Вавилона были найдены цилиндры с описанием процесса мыловарения, относящегося к XXIX веку до н. э.

[96] Carl P. Borchgrevink, Jae-Min Cha, Seung-Hyun Kim, "Hand Washing Practices in a College Town Environment," Journal of Environmental Health 75, no. 8 (2013): 18–24.

сначала. Это выглядит здраво. Но лишь пока мы не вспомним о том, как люди забывчивы и ленивы.

Мы исследовали похожую ситуацию в корпорации, предоставляющей финансовые услуги, со штаб-квартирой в Азии. Политика использования паролей требовала менять их ежемесячно; повторно применять старые запрещалось. Неудивительно, что при анализе образцов паролей выяснилось, что сотрудники изобрели множество творческих способов обойти неудобные требования. Например, кое-кто блеснул следующей серией паролей:

— password201801 (в январе);
— password201802 (в феврале);
— password201803 (в марте);
— и так далее.

Конечно, сотрудник легко запоминал эти пароли, но и хакеру было бы нетрудно расшифровать их логику. Такая практика подрывает основы безопасности: в ответ на обременительные меры раздраженные пользователи стараются придумать пароли попроще[97].

Настойчивые требования регулярной смены паролей не только не учитывают человеческий фактор, но и отвлекают от поиска альтернативных, цифровых мер контроля.

[97] Michelle L. Mazurek et al., "Measuring Password Guessability for an Entire University," working paper, Carnegie Mellon Cylab, October 22, 2013, https://www.cylab.cmu.edu/_files/pdfs/tech_reports/CMUCyLab13013.pdf.

Благодаря менеджерам паролей, появившимся в середине 1990-х, теперь легко подобрать длинный, уникальный произвольный пароль для каждого сайта, приложения или службы, которыми вы пользуетесь; при этом совсем не обязательно их запоминать. Все, что вам нужно помнить, — пароль к самому менеджеру паролей. Например, даже при наличии программного обеспечения, способного перебрать 100 трлн возможных паролей в секунду, хакеру потребуется более 600 миллиардов триллионов столетий, чтобы взломать произвольный пароль из 30 символов, а это существенно превышает оставшийся срок существования нашей Вселенной. Такой надежный пароль нет необходимости менять вообще (только если вы подозреваете, что его могли раскрыть при кибератаке на ваш компьютер). Но даже если такое случится, вам достаточно сделать один клик, чтобы подобрать другой столь же надежный пароль.

Итак, ваша задача — удостовериться, что компания:

- выявила и учла нетехнические факторы риска, например поведение сотрудников. Это важно для качественного управления мерами кибербезопасности и анализа их эффективности на практике.

Рекомендации для этого шага приведены в главе 11 (таблица 10).

Разработка плана нейтрализации киберрисков

Итак, вы определили приоритетность киберрисков, выбрали способы контроля и оценили их эффективность. Пора разрабатывать план по нейтрализации киберугроз. Помимо таких индивидуальных особенностей, как график внедрения выбранных мер, здесь важны ответы на ряд вопросов. Первый: почему компания проводит эти мероприятия по укреплению кибербезопасности? Ответ зависит от того, как взаимосвязаны ключевые виды деятельности вашей компании, уязвимости вспомогательных систем, кибератаки, которые могли бы их использовать, и, наконец, итоговое воздействие на компанию в целом. Эту информацию можно найти в сценариях киберугроз.

Также план по нейтрализации киберрисков должен отвечать на вопросы: как понять, что предпринято уже достаточно усилий? И в каком случае можно считать, что риски снижены до приемлемого уровня? Никто не спорит, что меры по нейтрализации необходимы и могут потребовать существенных инвестиций; тем не менее бюджет команды кибербезопасности нужно держать в пределах разумного.

Выявление и оценка приоритетности киберрисков неотрывны от аналогичных процессов в отношении бизнес-рисков, поэтому вам стоит проанализировать взаимосвязь между способностью кибератаки нарушить или прервать ключевые рабочие процессы и надежностью мер защиты, направленных на минимизацию возможного ущерба. Анализ основан на вкладе команды кибербезопасности

в обеспечение эффективного контроля, а топ-менеджеров – в нивелирование уровня бизнес-рисков.

Итак, ваш план по нейтрализации киберрисков сводится к перечню мероприятий и инвестиций, необходимых, чтобы максимально снизить угрозу. Внедряя разумные способы контроля, используя связанные с ними возможности и делая это регулярно, вы обеспечите надлежащий уровень защиты. На этом этапе вам предстоит удостовериться, что компания:

- разрабатывает наглядный план нейтрализации киберрисков, из которого ясно, как и когда внедрение определенных мер защиты снижает наиболее актуальные риски до приемлемого уровня.

Рекомендации для этого шага приведены в главе 11 (таблица 11).

Глава 9

Защита компании

Внедрив концепцию рассмотрения киберрисков в контексте бизнес-рисков, на следующем этапе вы должны удостовериться, что компания всегда готова к их нейтрализации. Это требует вдумчивого отношения к организационной структуре, рабочим процессам и корпоративной культуре. Не забывайте об открытости и необходимости постоянного диалога с коллегами.

Первое, что вам следует знать, — где искать и откуда ждать новые кибериски. Хорошая новость: далеко ходить не придется. Некоторые риски связаны с внешними факторами, например с приобретением уязвимого программного обеспечения. Но подавляющее большинство возникает из-за изменений, происходящих внутри компании под влиянием разных условий. Эти риски важно не пропустить, а каждое изменение, связанное с управлением или бизнес-процессами, необходимо анализировать. Только так вы разработаете эффективный план оценки и нейтрализации новых киберугроз.

Сотрудники должны регулярно информировать вас о том, как все обстоит с выявлением киберрисков применительно к конкретным видам деятельности. В этой главе предложена двухэтапная оценка текущего положения дел. В ее основе лежит как тестирование эффективности мер

контроля, так и анализ прогресса в плане нейтрализации корпоративных киберрисков.

Помимо выявления и отслеживания рисков, важную роль также играет отношение к команде кибербезопасности внутри компании. Непременно удостоверьтесь, что ее положение в организационной структуре компании выбрано здраво, с учетом миссии и интересов бизнеса. В конце главы мы как раз обсудим некоторые общепринятые нормы корпоративного поведения, ведущие к тому, что руководство и топ-менеджеры подолгу остаются в неведении относительно состояния кибербезопасности компании.

Разработка прогноза по киберрискам

Для надзора за менеджментом киберрисков вам необходимо удостовериться, что ваша компания:

— знает, на что обращать внимание, чтобы не пропустить новые киберриски;
— разрабатывает процедуры выявления новых киберрисков (с четко определенными контрольными точками) и составляет планы по их нейтрализации, конкретно обозначая критерии оценки и обязанности сотрудников.

Прогнозирование киберрисков

Первые попытки прогнозировать землетрясения относятся по меньшей мере к IV веку до н. э. Аристотель в своем труде «Метеорологика» заявил, что лучший способ делать это — наблюдать за «лунным затмением» или за появлением «тонкого и вытянутого в длину облачка, подобного тщательно проведенной длинной прямой черте»[98]. За следующее тысячелетие сейсмологи почти не добились прогресса в выявлении более надежных предвестников

[98] В трактате «Метеорологика» Аристотель предположил, что источник и предпосылка землетрясений — ветра, ищущие выхода из земных недр, куда они предварительно проникли из атмосферы. «Колебания земли вызываются не водой и не землей, а пневмой, когда внешние испарения почему-либо устремляются вглубь [земли] <...>. Так же объясняется появление порой обычных предвестий землетрясения: в ясном небе днем или вскоре после заката показывается тонкое и вытянутое в длину облачко, подобное тщательно проведенной длинной прямой черте, ведь в это время [поток] пневмы, изменивший свое направление, ослабевает <...>. И при лунном затмении иногда случается землетрясение. Ведь когда приближается [время] затемнения, а свет и солнечное тепло еще не полностью исчезли из воздуха, но уже ослабевают, наступает безветрие, потому что пневма перемещается в землю. Это и вызывает землетрясение перед затмением. И ветры часто поднимаются перед затмениями: перед полуночными — в самом начале ночи и в полночь — перед утренними затмениями. Это происходит потому, что тепло от Луны слабеет, когда на своем пути [она] уже приближается к месту затмения. Когда исчезает то, что удерживало воздух в неподвижности, он снова приходит в движение и начинает дуть (gignetai pneuma), но не раньше, чем произойдет затмение» (Аристотель. Метеорологика. Книга 2. Глава 8). Цит. по: Аристотель. Собрание сочинений в 4 томах / Пер. Н. В. Брагинской. М., 1981. Т. 3. *Прим. ред.*

землетрясений. Колебания атмосферного давления, химический состав грунтовых вод, электромагнитное излучение, поведение змей, собак и кошек — каких только гипотез не было. Все это тщательно исследовалось, но научного подтверждения не нашло.

Предсказать кибератаку не многим более реально. Среди направлений кибербезопасности, конечно, есть прогнозирование угроз — такой киберэквивалент сейсмологии. Эта научная дисциплина пытается рассчитать плановые атаки и предугадать надвигающиеся. Она фокусируется на выявлении потенциальных противников, их намерений и ресурсов. Это напоминает работу разведки. Однако практикуемое многими компаниями прогнозирование угроз редко заканчивается конкретными действиями, например корректировкой системы киберзащиты.

Прогнозирование киберугроз — невероятно увлекательное дело, отчасти из-за потока необработанных данных: от поставщиков, из источников угроз, из даркнета, СМИ, от правительств и разведывательных структур, обменивающихся информацией и разведданными. Все это необходимо разобрать, проанализировать и интерпретировать.

Хотя многие киберугрозы приходят из глубин интернета, а возможности прогнозирования ограничены, компании могут в чем-то действовать на опережение. Эра киберсейсмологии уже наступила. Надо только сменить угол зрения, чтобы увидеть это.

Куда не стоит смотреть

Каждый раз, внося изменения в компьютерные системы, компания подвергает себя риску кибератаки. А ведь она всего лишь обновляет параметры конфигурации или устанавливает новое программное обеспечение.

Отследить и проанализировать технические изменения в компьютерной инфраструктуре всей компании просто нереально из-за огромного объема данных. К тому же это не имеет особого смысла, поскольку вне бизнес-контекста, раскрываемого в сценарии киберугроз, можно провести лишь базовый анализ.

Известные технологии кибератаки — сфера, где часто пытаются найти новые риски. С тактической точки зрения специалисты по кибербезопасности должны знать о новейших инструментах и способах эксплуатации уязвимостей системы. Однако стратегически в этом нет особой пользы, поскольку, как уже отмечалось в главе 1, кибератаки будущего — потомки тех, которые появились в 1960-х и 1970-х годах.

Еще один источник изменений, часто изучаемый на предмет новых потенциальных киберрисков, — глобальные технологические инновации, например интернет вещей, big data, искусственный интеллект, блокчейн и облачные вычисления. Все области знаний, связанные с компьютерными технологиями, включая классические (базы данных, компьютерная графика), имеют собственные специфические бреши, о которых должен знать отдел информационной безопасности. Однако лишь в процессе планирования

и внедрения новых технологий компания может получить сведения, помогающие понять, как генерируются новые киберриски (для ее ключевых видов деятельности). Если уж на то пошло, технологические прорывы напоминают нам о необходимости быть начеку, ведь бизнес постоянно внедряет инновации.

Изменения в бизнесе имеют значение

Меняется что-то в вашем бизнесе — меняются и потенциальные угрозы. Этот факт обеспечивает контекст для анализа и определения приоритетов, а также подсказывает направление поиска новых киберрисков, которые необходимо принять к сведению. Вы можете рассматривать каждое изменение и каждую трансформацию в разных ракурсах. Далее мы объясним, как это поможет выявить новые киберриски.

Новые направления деятельности и модернизация старых процессов

Меняя способы ведения бизнеса, а с ними часть компьютерных систем, мы вполне можем столкнуться с неизвестными прежде уязвимостями. Новые направления деятельности, например разработка продуктов или услуг, нередко влекут за собой новые виды рисков. Они могут быть связаны как с самими продуктами и услугами, так и с возможностями для кибератак.

Изменения внутренних процессов также чреваты новыми киберрисками. Эти изменения различны по характеру:

от новой процедуры авторизации для совершения покупки на сайте до передачи на «облачный» аутсорсинг финансовых функций или управления персоналом. Неправильно разработанная процедура авторизации и разные погрешности контроля создают новые киберриски при оплате онлайн-заказа. Компания и ее клиенты вполне могут стать жертвой мошенников.

Изменения в структуре бизнеса

Масштабные изменения в структуре бизнеса — тоже источник новых киберрисков. К таким изменениям относится, например, открытие филиалов в новых регионах или за границей.

Большинство СМИ, говоря о кибератаках при поддержке государства, подчеркивают их техническую сложность; якобы наиболее изощренно атакуются цели, расположенные в другой стране. Но атака при господдержке может быть еще опаснее, если ее цель не за рубежом, а внутри. Например, в 2012 году мы привлекли внимание СМИ к тому, что отдельные полицейские управления Китая заставляли иностранные компании, находившиеся на их территории, устанавливать сетевые устройства, которые позволяли полиции перехватывать все входящие и исходящие сообщения в их офисах на территории КНР[99]. Это оказалось частной ини-

[99] Kevin Voigt, "International Firms Caught in China's Security Web," CNN, August 24, 2012, https://www.cnn.com/2012/08/24/business/china-foreign-companies-internet/index.html; Jonathan Ansfield, "Chinese Authorities Putting Pressure on Businesses to Help Censor the Web," New York Times, November 13, 2012, https://www.nytimes.com/2012/11/14/world/asia/china-pressures-businesses-to-help-censor-web.html.

циативой, а не результатом общенациональной политики. Однако в целом власти могут получить доступ к находящейся на их территории телекоммуникационной инфраструктуре, даже не прибегая к кибератакам или установке спецоборудования. Им достаточно просто попросить об этом. А ситуация с казино в Макао подтверждает, что даже конкурент может поживиться вашей информацией, если она передается по его телекоммуникационным сетям.

Мы не отговариваем вас от выхода на рынки, где вы, возможно, столкнетесь с новыми киберрисками. Но важно учесть их, принимая решение о расширении деятельности.

Слияния и поглощения также генерируют широкий спектр новых киберрисков, ведь, приобретая какую-нибудь компанию, вы неминуемо приобретаете и все ее киберриски. Ее экономическая ценность может резко измениться, если впоследствии обнаружатся существенные проблемы вроде утечек информации. Постарайтесь заранее учесть затраты на нейтрализацию этих угроз, чтобы точнее определить цену и прочие финансовые условия сделки. Вдобавок вирусы, заразившие сети поглощенной компании, могут проникнуть далеко за пределы ее стен и повредить всему вашему бизнесу.

Изменения во внешней деловой среде

Предприятия, с которыми ваша компания поддерживает стратегические деловые отношения (например, партнеры и контрагенты в цепочке поставок), также являются источниками потенциальных киберрисков, причем значение их постоянно растет. Для эффективного сотрудничества

бизнесу все чаще требуется технологическая интеграция и операционная совместимость, но многие компании не слишком интересуются тем, насколько вдумчиво их партнеры нейтрализуют киберриски. Например, атака на Target началась через вполне легальное соединение поставщика услуг по отоплению, вентиляции и кондиционированию воздуха с основной корпоративной сетью компании.

Киберриски, с которыми компания сталкивается, контактируя с партнерами по цепочке поставок, изощреннее, чем предоставление простого удобного канала для атаки. Уязвимости продуктов и услуг, получаемых от поставщиков, могут нанести ущерб компьютерной сети, в которую они интегрированы. Возможно, пострадают именно те системы, без которых работа компании окажется парализована. Продукты, казалось бы, совершенно разные, — полицейский нагрудный видеорегистратор, цифровая фоторамка и музыкальные компакт-диски — с одинаковой вероятностью могут таить в себе вредоносные программы[100]. Нейтрализация таких киберрисков требует комбинированного подхода, включающего жесткие требования к разработке продуктов и строгую систему контроля качества.

---

[100] Catalin Cimpanu, "Police Body Cameras Shipped with Pre-Installed Conficker Virus," Softpedia News, November 15, 2015, https://news.softpedia.com/news/police-body-cameras-shipped-with-pre-installed-confickervirus-496177.shtml; Gregg Keizer, "Best Buy Sold Infected Digital Picture Frames," Computerworld, January 23, 2008, https://www.computerworld.com/article/2538961/best-buy-sold-infected-digital-picture-frames.html; Bruce Schneier, "Real Story of the Rogue Rootkit," Wired, November 5, 2017, https://www.wired.com/2005/11/real-story-of-the-rogue-rootkit/.

Все рассмотренные выше источники киберрисков связаны со стратегическими и тактическими изменениями в компании: с выходом на новые рынки, оптимизацией бизнес-процессов, снижением затрат или разработкой и релизом новых продуктов. Для большинства из них готовятся формальные планы, критерии оценки выполнения и согласования с руководством. Если, исходя из обновленного сценария киберугроз для компании, какие-либо изменения приобретают статус критичных, вам следует об этом знать.

Изменения текущей деятельности компании

В текущей деятельности компании также могут возникать уязвимости ключевых бизнес-систем. Иногда они лишь следствие изменений, о которых мы писали ранее. Предоставление основному поставщику прямого доступа к приложениям компании — одномоментное решение, влекущее за собой долгосрочные изменения. Но для сотрудников поставщика управление счетами покупателей — текущая деятельность, способная генерировать киберриск (например, в результате ошибочного предоставления менеджерам более широких полномочий). Перенос коммерческой информации в облачное хранилище — тоже прекрасный пример единовременного изменения, в результате которого возникает множество потенциальных киберрисков. Ошибки конфигурации облачных файловых хранилищ Amazon Web Services привели к утечке конфиденциальной информации огромного количества организаций. АНБ лишилось важных сведений тактической разведки (и в частности,

данных разведки на поле боя), а Accenture потеряла пароли и ключи шифрования, использовавшиеся для защиты информации о клиентах[101].

Уязвимости могут содержаться не только в ПО, полученном от внешних поставщиков, но и в том, которое компания разрабатывает собственными силами. Специалисты редко пишут программы с нуля, отдавая предпочтение «сборке» из готовых, причем некоторые образцы берутся из внешних источников. Например, в 2017 году правительство Эстонии аннулировало действие около 750 000 «умных» ID-карт, поскольку в системе шифрования поступившего от третьей стороны ПО, встроенного в чипы, обнаружилась уязвимость. Студент выпускного курса из Германии, написавший вредоносную программу, не собирался заниматься хакерством; он просто решил продемонстрировать трудности, встречающиеся при разработке сложных программ.

Также существует понятие «теневое IT»: некоторые сотрудники используют сторонние технологии без ведома и одобрения коллег из IT-служб. Установка беспроводных подключений к корпоративной сети — лишь один пример. Такая практика распространяется пугающе быстро и уже включает широкое пользование облачными сервисами и интернетом вещей. Обычно люди прибегают к этим

[101] "Classified Pentagon Data Leaked on the Public Cloud," BBC News, November 29, 2017, https://www.bbc.com/news/technology-42166004; Zack Whittaker, "Accenture Left a Huge Trove of Highly Sensitive Data on Exposed Servers," ZDNet, October 10, 2017, https://www.zdnet.com/article/accenture-left-a-huge-trove-of-client-passwords-on-exposed-servers.

уловкам, чтобы улучшить свою результативность или просто ради удобства. Считая, что сотрудники IT-служб слишком заняты, чтобы по просьбе коллег установить желаемую программу, или вообще опасаясь нарваться на отказ, многие предпочитают действовать самостоятельно.

Хотя ни одно из этих изменений, казалось бы, не стоит повышенного внимания, все равно постарайтесь удостовериться, что сотрудники отслеживают даже пока незаметные источники новых киберрисков. Для таких угроз тоже необходимы адекватные способы нейтрализации. Осознавая, сколь многое влечет за собой новые угрозы, вы с коллегами всегда будете начеку в случае изменений в деятельности, структуре или внешней среде вашей компании. Пока вы не приступили к планированию конкретных мероприятий, любая дискуссия о киберрисках носит гипотетический характер, но вам следует выяснить как можно больше об их последствиях для бизнеса — например, перед созданием совместного предприятия или внедрением таких инноваций, как интернет вещей. То есть о ваших надзорных функциях важнее всего вспомнить, когда ваша компания готовится что-либо предпринять. Но не обязательно вечно пытаться предсказать будущее.

Систематизированное описание изменений в бизнесе

Чтобы управлять возникновением киберрисков в режиме реального времени, вашей компании следует внедрить процесс интеграции бизнес-изменений в операционную деятельность. Аналогично следует выработать типовую

методику анализа рисков и выбора адекватных мер их нейтрализации.

Для начала изучите ключевые элементы существующей процедуры управления изменениями. Возможно, туда удастся включить аспекты, связанные с киберрисками. В оптимизации процедуры важны два этапа: во-первых, следует расширить сферу ее действия так, чтобы охватить все бизнес-изменения, генерирующие киберриски, а во-вторых — удостовериться, что она включает их анализ. Многие компании и так включают анализ киберрисков в процедуру рассмотрения проектов, предложенных IT-службой. Но если инициатором проекта выступает другой отдел, об этом часто забывают.

По нашему опыту, сотрудники зачастую полагают, что проблемой киберрисков занимается кто-то другой, хотя и не имеют никаких тому подтверждений. Этому способствуют вера в IT-специалистов и экспертов по кибербезопасности, а также убежденность, что проблема слишком очевидна и важна, чтобы о ней просто забыли. А если каждый участник очередной реорганизации уверен, что о кибербезопасности позаботится кто-то другой, обычно оказывается, что о ней не позаботился никто.

Процедуры идентификации киберрисков, их оценки и приоритизации, а также разработки контрмер, описанные в предыдущей главе, применимы и к выявлению новых угроз. Кроме того, методику анализа и значительную часть результатов, полученных при изучении существующих бизнес-рисков (например, виды атак, способных причинить наибольший ущерб, и меры их

нейтрализации), можно позаимствовать непосредственно из сценариев киберугроз. Также ваша компания может воспользоваться этим опытом, чтобы классифицировать новые риски и определить их приоритетность. Важную роль здесь играют специалисты по кибербезопасности, профессионалы в смежных областях, например юриспруденции, и сотрудники, занимающиеся текущими бизнес-процессами, а также администрированием компьютерных систем.

Определить ключевые моменты относительно несложно. Проблема в том, чтобы понять, в каком направлении искать и насколько глубоко; обычно масштабы реорганизации достаточно велики и невозможно проанализировать все ее направления одинаково тщательно. В предыдущей главе мы предложили вам оценить приоритетность тех или иных видов деятельности компании. Жизненно важные рабочие процессы – удобная отправная точка, если у вас нет достаточных ресурсов, а главное, времени для всестороннего анализа.

Процессы и виды деятельности, обеспечивающие прогнозирование киберрисков, должны протекать внутри компании. Ваши сотрудники куда лучше, чем привлеченные консультанты, ориентируются в ситуации и способны выявить надвигающуюся опасность прежде, чем она превратится в реальную проблему. Ваша же задача – удостовериться, что компания:

- выявляет те бизнес-изменения, которые способны генерировать новые киберриски;

- проводит регулярный анализ этих изменений, чтобы разработать адекватные способы нейтрализации киберрисков.

Рекомендации для этого шага приведены в главе 12 (таблица 12).

Оценка текущей ситуации в вашей компании

Чтобы мониторинг текущей ситуации с киберрисками был успешным, вам следует удостовериться, что компания:

— регулярно тестирует эффективность мер нейтрализации киберрисков;
— контролирует выполнение планов по нейтрализации рисков.

Чтобы оценить готовность вашей компании к борьбе с киберрисками, надо понять следующее:

— какова ситуация с киберрисками;
— о чем следует беспокоиться;
— что не вызывает тревоги.

К сожалению, получить проверенные факты и убедительные ответы на основе глубокого анализа не так просто. И что в результате? Вы слышите что-то вроде «тут все в порядке» и «здесь надо еще поработать» или обобщенные оценки отдельных мер кибербезопасности.

Это неправильно: аналитические данные должны быть не только обоснованными, но и актуальными. А процесс анализа не нужно усложнять настолько, чтобы результаты ко времени получения уже устаревали.

Чтобы обеспечить и релевантность, и обоснованность, и приемлемые сроки получения данных, мы предложили подход, включающий две перманентно действующие процедуры: тестирование эффективности мер контроля и контроль процесса нейтрализации киберрисков.

Тестирование эффективности мер контроля

Эта процедура очень важна для оценки текущего остаточного риска: как уже несколько раз говорилось, наличие тех или иных мер контроля еще не гарантирует безоговорочных преимуществ. Тестирование действенности контроля показывает, насколько та или иная мера эффективна для нейтрализации киберрисков.

В главе 2 мы упоминали, что резервное копирование данных могло бы защитить компании от червя WannaCry. Даже если WannaCry уничтожит важную информацию, организация сможет получить к ней доступ, восстановив резервные копии файлов. Резервное копирование — давно и широко используемая мера не только от киберрисков, но и от разнообразных технических сбоев и ошибок персонала. Чтобы протестировать эффективность этой меры контроля, недостаточно убедиться, что кто-то регулярно делает резервные

копии. Надо сделать шаг вперед и удостовериться, что резервные копии могут быть успешно восстановлены.

Хотя независимое тестирование и анализ полезны при выборе отдельных продуктов кибербезопасности, способы нейтрализации рисков лучше тестировать самостоятельно. Различия между испытательной платформой независимой организации и деловой средой самой компании слишком велики и могут исказить результаты. Кроме того, нельзя оценить эффективность мер контроля исключительно с помощью них самих. Например, антивирусное программное обеспечение не справится с вирусами, которые оно не в состоянии обнаружить. Римский поэт Ювенал, живший в I веке н. э., прогнозировал возникновение такой ситуации, задав вопрос: «Кто устережет самих сторожей?»[102] Этот принцип распространяется не только на технологии, но и на специалистов по кибербезопасности: анализировать ее архитектуру и технические решения должен сотрудник, не принимавший участия в принятии технических решений. Яркий пример – перенос конструкторской информации по новым автомобилям в корпоративный интранет.

Ваша задача – удостовериться, что компания:

- ☐ постоянно тестирует эффективность мер по нейтрализации киберрисков.

Рекомендации для этого шага приведены в главе 12 (таблица 13).

[102] Википедия. Доступ 28 апреля 2020 года, https://ru.wikipedia.org/w/index.php?title=Quis_custodiet_ipsos_custodes%3F&stable=1.

Контроль выполнения планов по нейтрализации киберрисков

В предыдущей главе мы обсудили план нейтрализации киберрисков, который представляет собой перечень продуманных действий, достаточных, чтобы защитить жизненно важные виды деятельности. Если компания следует плану и внедряет постоянно действующую киберзащиту, остаточный риск снижается до приемлемого уровня.

Для этого и нужен контроль выполнения плана: благодаря ему регулярно идентифицируются области, где уровень риска очень высок. Пока компания не внедрит меры для нейтрализации киберрисков, ее деятельность останется крайне уязвимой для атак. Объединив информацию о текущем состоянии с результатами тестирования мер контроля, вы получите ясную картину остаточного киберриска для каждого вида деятельности. Здесь вам необходимо удостовериться, что компания:

- регулярно обновляет информацию о выполнении плана нейтрализации киберрисков;
- отчитывается о положении дел с киберрисками в ключевых видах предпринимательской деятельности.

Рекомендации для этого шага приведены в главе 12 (таблица 14).

Оптимизация организационной эффективности

Оценивая организационную эффективность, удостоверьтесь, что компания:

- принимает во внимание внутреннюю динамику, мотивы и стимулы, определяя роль команды кибербезопасности в организационной структуре;
- поощряет обмен информацией в сфере кибербезопасности и открытое обсуждение вопросов, связанных с киберрисками.

Команда кибербезопасности в корпоративной иерархии

Формирование преданной своему делу команды кибербезопасности под руководством компетентного директора по кибербезопасности (Chief Information Security Officer – CISO) – важный шаг. От него во многом зависит ваша стратегия в области информационной безопасности, а также надежность защиты от киберугроз. Положение этой службы в организационной структуре компании – критерий, определяющий эффективность ее работы. Следует обратить внимание на согласование задач, целей и интересов директора по кибербезопасности и его команды с задачами и целями высшего руководства, а также избегать расхождений между ними.

Традиционно за кибербезопасность отвечал в первую очередь IT-отдел, поэтому соответствующие команды создавались в его структуре. При этом редко учитывались различия в миссии и мотивации IT-директора (CIO) и директора по кибербезопасности (CISO).

Вообще говоря, руководство обычно поощряет IT-директора за внедрение новых систем и приложений, обновление компьютерной и сетевой инфраструктуры, особенно если этого удалось достичь в более короткие сроки и с меньшими затратами, чем в предыдущем году. Что же касается директора по кибербезопасности, он отвечает за стратегию кибербезопасности и все меры в этой сфере. В процессе решения задач директор по кибербезопасности нередко расходится с IT-директором, что негативно влияет на уровень заработной платы последних, если, к примеру, срываются сроки внедрения тех или иных технологий. Помимо финансовой заинтересованности есть другой камень преткновения — вопрос достаточного финансирования. Поскольку бюджет, которым распоряжается директор по кибербезопасности, входит в бюджет IT-отдела, именно IT-директор принимает окончательное решение о выделении денег — например, на закупку технических средств контроля, переподготовку сотрудников и профилактику некоторых видов кибератак.

Мы ни в чем не обвиняем IT-директора. Мы сотрудничали со многими из них и видели, что нужды кибербезопасности они ставят выше своей финансовой выгоды. Однако эффективное корпоративное управление не может опираться на сотрудников, вынужденных действовать

вопреки собственным интересам, равно как и зависеть от характера и суждений человека, оказавшегося в кресле IT-директора. Если ваш директор по кибербезопасности подотчетен IT-директору, следует определить меры, сглаживающие конфликт интересов и облегчающие поиск консенсуса.

Принимая решение о подотчетности команды кибербезопасности, необходимо учитывать и другие факторы, например уровень топ-менеджера, которому подчиняется директор по кибербезопасности. Хотя каждая компания имеет уникальные организационные особенности, мы рекомендуем обратить внимание на непосредственных подчиненных CEO. Подотчетность CISO кому-то из них имеет несколько очевидных преимуществ. Успешная реализация задач директора по кибербезопасности и его команды требует кросс-функционального взаимодействия сотрудников в масштабах всей компании, в том числе тех, которые ему не подчиняются. Его способность добиваться такого взаимодействия резко возрастет, если он будет подотчетен кому-либо из топ-менеджеров, находящихся в прямом подчинении у CEO. Далее, столь высокое положение директора по кибербезопасности и команды кибербезопасности в организационной иерархии подчеркнет приоритетность его задач лучше любых слов. А также обеспечит качественную интеграцию связанных с кибербезопасностью решений и мер в рамках ключевых видов деятельности, поскольку директор по кибербезопасности станет непременным участником дискуссий обо всех изменениях, генерирующих киберриски.

В принципе, на вопрос, кто из топ-менеджеров должен курировать команду кибербезопасности, нет неправильных ответов. Но следует принять во внимание некоторые соображения. Например, если учесть широкий спектр киберугроз для промышленных систем контроля и автоматизированных процессов в целом, выбор на эту роль директора по производству (COO) выглядит логичным для любой промышленной компании, особенно для тех, кто занимается критически важными объектами инфраструктуры.

Когда компания CLP решила нанять директора по кибербезопасности, одной из проблем стало его положение в корпоративной иерархии. Вопрос сводился к тому, кто будет нести ответственность за риски. Директор по производству CLP Дерек Паркин заметил: «Я несу ответственность за операционную деятельность, а значит, и за ее физическую охрану и защиту. Однако у меня нет прямого доступа к управлению наиболее разрушительным потенциальным риском – риском кибератак»[103]. Сейчас проблема решена: директор по кибербезопасности подчинен непосредственно директору по производству, а рабочие места специалистов по кибербезопасности расположены в шаговой доступности от его кабинета. Паркин использует дополнительные преимущества этого решения: организует тесное взаимодействие между командой кибербезопасности и традиционной службой безопасности, а также распространяет принципы культуры безопасности на цифровую сферу.

[103] Из частной беседы 17 мая 2019 года.

Еще одна удачная кандидатура на роль тимлида команды кибербезопасности — начальник юридического отдела. От природы или из-за особенностей профессии, но корпоративные юристы всегда стараются смотреть в будущее, своевременно прогнозировать потенциальные риски и принимать меры по их нейтрализации или предотвращению. Мы заметили любопытный момент: многие юристы понимают суть киберрисков и их последствий лучше, чем некоторые программисты, сфокусированные на разработке полезных приложений, а не на том, как кто-то может обернуть результаты их работы во вред (как компании-разработчику, так и пользователям и партнерам).

Финансовый директор — тоже неплохой выбор. Его участие в стратегическом планировании и привычка соблюдать налоговую дисциплину будут преимуществами. Наконец, на роль тимлида команды кибербезопасности можете подойти вы и другие члены совета директоров. Как мы уже говорили, для эффективного надзора вы и ваши коллеги нуждаетесь в точной и достоверной информации. Чем меньше у директора по кибербезопасности контактов с высшим руководством, тем выше риск искажения этой информации в процессе передачи. Вспомните игру «испорченный телефон», когда дети садятся в круг и один из них шепчет какое-нибудь слово соседу. Это повторяется до тех пор, пока передаваемое слово не возвращается к первому участнику. Обычно он слышит совсем не то, что произнес в начале игры.

Но существует топ-менеджер, которого мы не рекомендуем на роль тимлида команды кибербезопасности, — это

CEO. Хотя такое решение может выглядеть подтверждением высокого приоритета ее задач, на самом деле результат будет прямо противоположным. Такое решение изолирует команду кибербезопасности от текущей деятельности компании. Она оказывается запертой в своего рода бункере, просто расположенном выше по склону холма, чем другие бункеры.

Итак, ваша обязанность — удостовериться, что компания:

- выбрала команде кибербезопасности правильное положение в корпоративной иерархии, учла необходимость согласовывать работу ее участников с текущими процессами, обеспечила директору по кибербезопасности достаточную свободу действий и эффективную коммуникацию с советом директоров.

Рекомендации для этого шага приведены в главе 12 (таблица 15).

Компетенции совета директоров

Оптимизация организационной структуры компании в целях повышения кибербезопасности не затрагивает совет директоров как таковой. Советам директоров нет необходимости меняться: их самоорганизация, устройство и процедуры зависят только от них самих. Главное — помнить о важном принципе цифрового управления: «Кибербезопасность должна быть в приоритете».

Значение кибербезопасности постоянно растет. Членам совета директоров зачастую не хватает знаний в этой области, поэтому часто звучат предложения расширить его компетенции, назначив независимых внешних директоров (INED) с соответствующим опытом и подготовкой и создав комитеты по кибербезопасности. Однако, помимо удручающей нехватки кадров, существует целый ряд причин, по которым эта, казалось бы, хорошая идея оборачивается сомнительной затеей. Во-первых, естественное следствие такого решения – нежелание остальных членов совета директоров вникать в проблему. Зачем, если ею занимаются грамотные профессионалы? Во-вторых, в случае утечки какой-либо информации козлом отпущения рискует стать именно INED. В-третьих, наличие опыта в сфере кибербезопасности еще не означает, что человек станет эффективным членом совета директоров. Узкий взгляд на вещи и фокус на технологических аспектах нередко мешают этому. INED с обширным бэкграундом в технических аспектах кибербезопасности может плохо понимать разницу между управлением и надзором.

Комитеты по кибербезопасности в составе совета директоров также не обязательны. Как мы уже говорили, созданию эффективной киберзащиты препятствует в первую очередь оторванность соответствующей службы от ключевых видов деятельности компании. Непонимание текущих рабочих процессов приводит к неверным управленческим решениям, не учитывающим важные бизнес-факторы и совершенно нежизнеспособным. Вдобавок формируется иллюзия, будто комитет решает все проблемы,

поэтому беспокоиться не о чем. Таким образом, очередное кажущееся правильным решение на самом деле контрпродуктивно. То же касается введения экспертов по кибербезопасности в состав команды по технологиям, поскольку сотрудники укрепляются в мысли, что это чисто техническая проблема и неспециалистам можно забыть о ней.

Главный юрисконсульт и ответственный секретарь CLP Дэвид Симмондс работает в тесном контакте с советом директоров. «Кибербезопасность – вовсе не такая непознаваемая вещь, как принято считать, – говорит он. – Речь не только о высоких технологиях. Скорее, это вопрос общего администрирования, как и многое, чем приходится заниматься совету директоров. Нам вовсе не обязательно иметь специалистов по цифровым технологиям в составе совета; наоборот, они скорее помешают»[104]. Далее Симмондс продолжает: «Совет директоров считает управление киберрисками наивысшим приоритетом, а функцию надзора в сфере кибербезопасности – важнейшей своей обязанностью. На собраниях совета директоров все больше времени отводится обсуждению вопросов кибербезопасности, а участие аудиторского комитета в тренингах по информационным технологиям – пример приверженности компании данной идее».

Ваши обязанности по надзору за цифровым управлением можно упростить, а затрачиваемое на них время – сократить за счет организационных мероприятий. В памятке по киберрискам приведено множество запросов,

[104] Там же.

решающих эту задачу. Там же есть примеры данных, которые должны содержаться в ответах на запросы. Сбор некоторой информации (например, связанной с приоритетностью ключевых видов деятельности) требует вашего участия. Прочие сведения дадут общую картину и облегчат понимание того, с какими рисками предстоит столкнуться вашей компании.

Не забывайте требовать дополнительные свидетельства того, что предприняты все необходимые меры кибербезопасности и учтены все сопутствующие факторы и тенденции. Своевременная инвентаризация ключевых компьютерных систем – хороший пример: вы должны удостовериться, что компания ее провела, хотя в вашем личном участии нет необходимости. В таких вопросах вам эффективнее всего поможет отдел внутреннего аудита: 1) подобное инспектирование – часть его обязанностей, и 2) у него налажены коммуникации с советом директоров. Эта помощь, как правило, проходит в два этапа. Во-первых, необходимо подтвердить, что упомянутые свидетельства (например, документы по инвентаризации и сценарии киберугроз) действительно есть, – это неоценимо для проверки вашей системы кибербезопасности. Если в ответ на запрос не удается привести реальные доказательства, следует заняться этим плотнее. А во-вторых, внутренний аудит может в первоочередном порядке оценить качество представленных доказательств, равно как и процессов их сбора и обработки.

Содействие отдела внутреннего аудита существенно экономит ваше время и избавляет от тяжелых и нудных

аспектов надзора. Более того, компания получает дополнительные преимущества, фокусируясь на деятельности, наиболее значимой для совершенствования системы кибербезопасности.

Поощряйте прозрачность

Для эффективного управления руководство компании нуждается в точных и своевременных данных обо всех аспектах деятельности. Получение такой информации — всегда проблема, но в сфере кибербезопасности она особенно остра, хотя бы потому, что сторонний наблюдатель мало что может тут понять. Глядя на Великую Китайскую стену, нетрудно представить, от каких атак она может защитить. Этого не скажешь о брандмауэре, чей потенциал скрывается в устройстве, напоминающем деталь стереосистемы. Даже не будучи профессиональным маляром, вы наверняка сможете определить, как давно покрасили ту или иную поверхность и насколько хорошо. Но в сфере кибербезопасности все совсем иначе. Многие процессы, например конфигурирование системы обнаружения вторжений, окутаны туманом.

Недостаток прозрачности ведет к тому, что вам как руководителю приходится в большей мере полагаться на предоставляющих информацию профессионалов. Чтобы убедиться, что доверие оправдано, вы должны расширить свои надзорные обязанности еще одним пунктом. Включите туда проверку политики топ-менеджмента: работают ли эти люди над созданием открытой внутренней среды, где

каждый сотрудник может быстро и честно высказать мнение или поделиться информацией по поводу текущей ситуации с кибербезопасностью? Это особенно важно, если информация негативная.

Прежде чем обсудить факторы создания открытой среды, рассмотрим некоторые нюансы, повлиявшие на эффективность коммуникаций до и во время Сингапурского киберкризиса 2018 года.

SingHealth

Новости наконец-то пришли по электронной почте. Десятого июля 2018 года доктору Айви Ын, CEO компании SingHealth, сообщили, что неделю назад их электронная медицинская картотека (EMR) была взломана. EMR проработала почти десятилетие и была основой практически всех ключевых рабочих процессов SingHealth, начиная с лечения пациентов и заканчивая управлением счетами. CEO сразу поняла, что это «очень серьезное происшествие», и поручила IT-директору поставить в известность власти Сингапура[105].

Предчувствия ее не обманули: как выяснилось позже, это была «самая серьезная утечка персональных данных»

[105] Singapore Ministry of Communications and Information, "Public Report of the Committee of Inquiry (COI) into the Cyber-attack on Singapore Health Services Private Limited Patient Database," press release, accessed March 6, 2019, https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2019/1/public-report-of-the-coi.

в истории Сингапура[106]. Крупнейшая сеть больниц SingHealth утратила медицинские записи 25% жителей города, включая сведения о лекарствах, выписанных премьер-министру Ли Сяньлуну[107].

До назначения на пост Айви Ын была известным педиатром. На стенах ее офиса до сих пор висят фотографии детей, которым она не смогла помочь, — чтобы «...напоминать о том, что мы берем на себя заботу о пациентах, мы никогда не сможем сделать для них достаточно много»[108]. На должности CEO SingHealth эта забота о людях нашла свое выражение в медицинской и административной деятельности Айви Ын. В числе прочего она никогда не пренебрегала сохранностью персональных данных пациентов. Под ее контролем SingHealth инвестировала большую сумму в передовые технологии и процедуры, «...не отвергнув и не сократив ни одной бюджетной заявки, имеющей отношение к кибербезопасности»[109].

Годами проверки подтверждали качество киберзащиты ее компании; комитеты совета директоров по аудиту и рискам регулярно обсуждали вопросы инвестиций в кибербезопасность и принимаемые меры. SingHealth вела четкую политику, соответствовавшую новейшим международным

---

[106] Выступление ответственного за кибербезопасность министра С. Изварана в парламенте по вопросу о кибератаке на компьютерные системы компании SingHealth 6 августа 2018 года.

[107] Там же.

[108] "Why SingHealth CEO Keeps Photos of Dead Young Patients in Her Office," AsiaOne, accessed March 5, 2019, https://www.asiaone.com/health/why-singhealth-ceo-keeps-photos-dead-young-patients-her-office.

[109] Министерство коммуникаций и информации Сингапура. Публичный отчет комитета по расследованиям. С. 15.

стандартам и ориентированную на контроль над соблюдением всех требований регулятора. В компании имелся IT-директор, которому непосредственно подчинялся директор по кибербезопасности (CISO). IT-директор проводил «...обучение персонала борьбе с фишингом и рассылал огромное количество имейлов IT-специалистам, информируя их о политике безопасности, ответственности и уязвимостях в защите»[110].

Несмотря на все эти усилия, катастрофа назревала задолго до утечки. Совет директоров и топ-менеджеры не очень хорошо представляли себе важнейшие проблемы и решения, которые послужили предпосылкой для кибератаки, а также для реакции на нее компании. Топ-менеджеры SingHealth не уделяли должного внимания проблеме кибербезопасности. Ее делегировали техническим специалистам, которые вполне ожидаемо не имели достаточных знаний в области системы EMR и тех бизнес-функций, которые она поддерживала.

Несмотря на заявления Айви Ын о том, что «...такая ужасная катастрофа, как утечка данных наших пациентов, — совершенно неприемлемый риск», решения, принимавшиеся IT-службой, не отражали этих взглядов[111].

---

[110] Channel NewsAsia, "SingHealth COI Report: 16 Recommendations Put Forward in Dealing with IT Security Incidents," Gov.Sg, January 13, 2019, https://www.channelnewsasia.com/news/singapore/singhealth-coi-report-it-security-recommendations-11104458.

[111] Faris Mokhtar, "SingHealth Top Executive Hopes for New Solutions to Internet Separation, Which Has Caused 'Multiple Inconveniences,'" TODAY (Singapore), November 5, 2018, https://www.todayonline.com/singapore/singhealthtop-executive-hopes-new-solutions-internet-separation-which-has-caused-multiple.

За несколько лет до утечки, в 2014 году, один IT-специалист выявил уязвимость в системе безопасности EMR и сообщил об этом. В условиях отсутствия коммуникации между техническими и бизнес-отделами IT-менеджер среднего звена принял решение проигнорировать сообщение. Впоследствии хакер воспользовался именно этой уязвимостью.

В предыдущие годы многие решения в сфере безопасности принимались без глубокого понимания ключевых видов деятельности компании и приоритетности рисков. Не были внедрены меры контроля, способные нейтрализовать даже самую мощную кибератаку или эффективно отреагировать на нее.

В момент кибератаки рядовые сотрудники IT-службы, оказавшиеся на переднем крае обороны, защищались очень инициативно, пусть и не совсем грамотно. Однако бездействие руководителей на всех уровнях цифрового управления, вплоть до IT-директора и директора по кибербезопасности, свело на нет их усилия.

Доказательства успешной атаки обнаружил рядовой сотрудник команды кибербезопасности за несколько месяцев до ее официального признания. Руководитель группы оперативного реагирования положил его рапорт под сукно, поскольку «имел превратные представления о том, что такое "инцидент в сфере безопасности" и когда о нем следует сообщать». Далее он решил «...повременить с докладом, поскольку чувствовал, что давление на него и его команду резко возрастет, как только топ-менеджеры узнают о кибератаке». Кроме того, его беспокоило, что «...в компании

плохо посмотрят на всю эту историю, если впоследствии окажется, что тревога была ложной»[112]. Следующий в служебной иерархии директор по кибербезопасности «...не понял значимости представленной информации и не предпринял никаких действий, чтобы разобраться в ситуации», а затем ловко уклонился от принятия решения о том, доводить ли инцидент до всеобщего сведения[113]. Когда наконец о случившемся сообщили IT-директору, тот тоже повременил докладывать CEO и совету директоров, решив дополнительно изучить проблему и выработать необходимые решения: показать, что IT-служба приняла все надлежащие меры по нейтрализации и сдерживанию кибератаки. Таким образом, время было безнадежно упущено.

Утечка данных прогремела на весь Сингапур. После этого совет директоров SingHealth организовал независимое расследование, чтобы выявить функционал, ответственность и действия персонала. Заодно с некоторых сотрудников удержали премии и взыскали компенсации, чтобы «повысить чувство ответственности» в будущем[114]. Как обычно в случае таких масштабных утечек, компания отменила выплату бонусов, уволила сотрудников команды кибербезопасности и технических специалистов и сняла с должности директора по кибербезопасности.

---

[112] Министерство коммуникаций и информации Сингапура. Публичный отчет комитета по расследованиям. Резюме доклада.

[113] Там же.

[114] IHiS, "IHiS Committed to Improving Cyber Defence in Healthcare," January 14, 2019, https://www.ihis.com.sg/Latest_News/Media_Releases/Pages/Committed-to-Improving-Cyber-Defence-in-Healthcare.aspx.

В итоге пострадала репутация как отдельных сотрудников, так и компании в целом. На нее посыпались штрафы; топ-менеджеров вызывали на допросы и дачу показаний в суд. SingHealth подписала 500-страничное мировое соглашение, переполненное всевозможными техническими требованиями. Компании еще долго придется отмываться от всего этого.

Ответственность или осуждение

Как показала утечка информации в SingHealth, после подобных инцидентов начинаются взаимные обвинения и поиск козлов отпущения. Топ-менеджеров ждет множество неприятных последствий, начиная от объяснений перед обозленными акционерами и представителями властей, заканчивая взысканиями вроде лишения премии, понижения в должности и ухода из совета директоров. Все эти меры пускают в ход, надеясь привить руководителям более внимательное отношение к проблемам кибербезопасности, причем касается это не только пострадавшей компании, но и тех, которые пока лишь наблюдают ситуацию со стороны. Короче говоря, система загорается целью исключить риск утечек информации, а чтобы достигнуть этого, начинает все жестче давить на топ-менеджеров. Поскольку давление идет и извне, последние не могут пресечь это. Однако, как мы покажем в следующей главе, топ-менеджерам по силам спрогнозировать ситуацию и подготовить компанию и самих себя к киберкризису.

Руководству необходимо определиться, прежде всего, с подходом к проблеме. На чем строить корпоративную политику в сфере кибербезопасности: на ответственности или на суровых карательных мерах? Выбор достаточно прост, даже если на первый взгляд кажется противоречивым. Можно либо наказывать сотрудников за каждый просчет и каждый провал, либо добиваться высокого уровня защищенности компании от киберугроз. «Смешать и взболтать» невозможно, поскольку метод кнута гарантирует, что ни вы, ни ваши топ-менеджеры не получите информации, необходимой для создания надежной киберзащиты.

После инцидента с утечкой данных совет директоров SingHealth организовал независимое расследование с целью найти виновных, и на первый взгляд это было разумное, необходимое решение. Вполне вероятно, что руководители других компаний, столкнувшихся с подобными проблемами, поступили бы так же. Да и факт, что по итогам несколько сотрудников получили благодарности за успешные действия в сложной обстановке, казалось бы, подтверждает объективность и добросовестность дознавателей.

И все же давайте проанализируем последствия любых действий под девизом «найти и покарать» — прежде всего их влияние на поведение человека. Мы не раз сталкивались с ситуациями, когда страх «попасть под раздачу» заставлял подчиненных утаивать от руководства критически важную информацию о киберрисках и уязвимостях. Несколько лет назад мы встречались с управляющим директором одного европейского производителя в Китае, для которого ранее проводили оценку киберрисков. Он бурно

радовался тому, что мы не нашли никаких проблем. Мы опешили, ведь наше заключение вовсе не было безусловно положительным. Как выяснилось, директор завода, которому мы отослали отчет, подредактировал его, заменив все наши выводы на более позитивные, и только в таком приглаженном виде показал управляющему директору.

Даже беспочвенный страх обвинений иногда заставляет людей излишне «сглаживать углы» в своих отчетах. Рассмотрим интересный пример. Директор по кибербезопасности и IT-директор одной крупной транснациональной компании пригласили эксперта по кибербезопасности, чтобы тот проверил, легко ли проникнуть в их систему защиты. Тестирование должно было затронуть в том числе услуги по мониторингу систем безопасности, оказываемые внешним поставщиком. Для чистоты эксперимента директор по кибербезопасности и IT-директор не предупредили о проверке никого из сотрудников. Тестирование закончилось ошеломляющим успехом или полным провалом — в зависимости от точки зрения. Эксперт сумел проникнуть в святая святых информационных систем компании, и никто этого не заметил! Даже когда директор по кибербезопасности попросил гипотетического хакера действовать более грубо, чтобы облегчить его обнаружение при помощи компьютерного эквивалента звякающих банок и кастрюль, взлом засекли далеко не сразу.

По итогам эксперимента IT-директор и директор по кибербезопасности провели серию совещаний, выясняя причины такого сокрушительного провала, а затем разработали план по устранению проблем и приступили к его

реализации. Вплоть до этого момента IT-директор и директор по кибербезопасности действовали грамотно, будто по хорошему учебнику.

Однако, пока информация о результатах проверки доходила до совета директоров, она сильно изменилась. Не считая пары замечаний о необходимых усовершенствованиях там и тут, итоговый отчет в целом создавал впечатление, будто все попытки сетевых проникновений удалось выявить и пресечь. Когда мы рассказали председателю совета директоров правду, он весьма удивился по двум причинам. Понятно, в первую очередь его удивили такие серьезные расхождения между отчетом и действительностью, но еще больше — сам факт того, что сотрудники решились на подлог. С его точки зрения, информирование совета директоров о том, что компания протестировала систему киберзащиты, выявила бреши и уже приступила к их устранению, было бы вполне достойным ответом.

Страх стать козлом отпущения неотрывен от страха быть обвиненным и еще больше отбивает у людей охоту говорить правду. Когда мы расследовали мошенничество с дебетовыми картами в Юго-Восточной Азии (о нем говорилось в предыдущей главе), один из топ-менеджеров банка заявил, что «с удовольствием зальет полы кровью виновных», причем фразу он повторял часто и громко; многие коллеги ее слышали. Результат не заставил себя ждать: сотрудники IT-службы начали нам лгать. Даже с учетом неточностей перевода с индонезийского языка на английский было ясно: они существенно исказили то, что говорили в начале недели. В итоге они признались, что их

непосредственный руководитель порекомендовал утаивать информацию, опасаясь, что в результате пострадает именно он. Страхи оказались неоправданными: он сохранил работу. А вот кровожадного топ-менеджера уволили.

Не убивайте гонца

В вышедшем в 1972 году оскароносном фильме «Крестный отец» юрист главного героя Том Хаген выдвигает деловое предложение, но получает отказ. Он сразу находит себе оправдание и заявляет: «Мистер Корлеоне всегда настаивает на том, чтобы дурные новости сообщались ему немедленно». Но людей, подобных в этом отношении Дону Корлеоне, очень немного: мало кто любит плохие вести. Отсюда и истории, когда гонцов, приносивших дурную весть, убивали.

Более 2000 лет назад царь Армении Тигран ввязался в войну с Римской империей. Когда один из гонцов сообщил, что римский полководец Лукулл со своей армией стремительно наступает, Тигран, охваченный яростью, отсек ему голову[115]. В результате царь потерял связь

[115] *Плутарх.* Избранные жизнеописания: [Пер. с древнегреч.]/ Сост. и примеч. М. Томашевской; иллюстрации В. Медведева. — М.: Правда, 1987. Т. 2. 605 с. Раздел «Лукулл», с. 105. Несколько отличающийся вариант этой же истории (гонца повесили) приводился в книге Аппиана Александрийского «Римские войны», в главе «Митридатовы войны». *Аппиан Александрийский.* Римская история / Отв. ред. д-р ист. наук Е. С. Голубцова; ст. И. Л. Маяк; коммент. А. С. Балахванцева. М.: Наука, 1998. 726 с. *Прим. ред.*

с авангардом собственных войск, и римляне — находясь в меньшинстве! — одержали победу[116].

Боясь прогневать начальника, подчиненные нередко утаивают правду — полностью или частично. Одно исследование показало, что 60% сотрудников IT-служб не сообщают о возникающих киберрисках, пока те не приобретают угрожающий характер. В итоге с ними куда труднее справиться. Более того, сотрудники признались, что стараются скрывать плохие новости до тех пор, пока это возможно[117].

Примерно ту же опасность таит традиционная управленческая мудрость «Не сообщайте мне о проблемах, а сразу предлагайте решение». Да, этот тезис иногда мотивирует подчиненных не пасовать перед возникшей проблемой, а сразу искать выходы, однако в сфере кибербезопасности он зачастую контрпродуктивен. IT-сотрудник может не иметь полномочий для решения проблемы, поскольку оно требует действий, лежащих за пределами его компетенций. Как показала история с утечкой информации из SingHealth, страх сотрудников, что сообщение о проблеме, не имеющей решения, негативно скажется на их карьере, привел к слишком долгому замалчиванию.

---

[116] John Rickard, "Battle of Tigranocerta, 6 or 7 October 69 B. C.," accessed January 22, 2019, http://www.historyofwar.org/articles/battles_tigranocerta_69_bc.html#:~:text=The%20battle%20of%20Tigranocerta%2C%206,unable%20to%20take%20advantage%20of.

[117] Sean Martin, "Cyber Security: 60% of Techies Don't Tell Bosses About Breaches Unless It's 'Serious,'" *International Business Times*, April 16, 2014, https://www.ibtimes.co.uk/cyber-security-60-techies-dont-tell-bosses-about-breachesunless-its-serious-1445072.

Иногда плохие новости не доходят до руководства компании по другим причинам. Например, тут может сказаться конфликт интересов, связанных с последствиями их извещения.

Возьмем некую компанию, недавно сменившую собственника. Когда-то она создавалась как альянс государственного предприятия и иностранного частного холдинга. По словам сотрудников команды кибербезопасности, в тот период компанию неоднократно атаковали, но все попытки сетевых проникновений были относительно примитивными и легко отражались. Ситуация изменилась, когда государственная компания выкупила долю партнера и стала единоличным собственником. Вскоре после этого средства мониторинга оповестили сотрудников команды кибербезопасности о том, что некоторые администраторы авторизовались в критически важных компьютерных системах вне штаб-квартиры компании. Решив, что эти люди в отпуске или в командировках, специалисты проверили записи о пользовании электронными пропусками и обнаружили, что нет, администраторы должны находиться в офисе. Следовательно, кто-то позаимствовал их логины и пароли, чтобы удаленно проникнуть в компьютерную систему компании.

Это означало, что кибератаки на компанию стали, несомненно, сложнее. Сотрудники команды безопасности подозревали, что причина — в смене собственника. Страна происхождения государственного предприятия долгое время находилась в напряженных отношениях со страной происхождения частного холдинга, а та уже была замечена

в атаках против других стран. Более того, недавние атаки на компанию очень их напоминали.

В скором времени ожидался визит высокопоставленного члена правительства, который представлял собственника компании. Сотрудники команды кибербезопасности посчитали нужным сообщить ему о появлении новых, более серьезных киберрисков. Они доложили о своих находках, подозрениях и рекомендациях начальству, вплоть до CEO. Однако CEO решил, что существует слишком много проблем, требующих обсуждения с представителем нового собственника, и вообще не упомянул о кибератаках.

Еще один пример конфликта интересов — Twitter. Его инженеры обратили внимание на то, что в России, в Украине и других странах бывшего СССР регистрируется множество подозрительных аккаунтов. Чувствуя неладное, инженеры рекомендовали их удалить[118]. Однако у них не было полномочий сделать это. Такие полномочия имелись у так называемой команды роста, входившей в состав отдела маркетинга, а ее участники не согласились с этой рекомендацией. В первую очередь они беспокоились о том, чтобы догнать Facebook по количеству пользователей, и удаление аккаунтов нисколько этой цели не способствовало. Аккаунты остались на месте и, возможно, сыграли свою роль в президентских выборах в США в 2016 году.

В обоих случаях сотрудники располагали ценной информацией о киберрисках, но не имели других каналов ее

[118] David Dayen, "How Twitter Secretly Benefits from Bots and Fake Accounts," *Intercept*, November 6, 2017, https://theintercept.com/2017/11/06/how-twitter-secretly-benefits-from-bots-and-fake-accounts/.

передачи, кроме корпоративной управленческой цепочки. В результате руководство компании осталось в неведении.

Как показывают эти и другие примеры, мотивация и интересы отдельных сотрудников — серьезный фактор, способный подорвать управление киберрисками. Мы неоднократно убеждались, что поиск козлов отпущения контрпродуктивен. Более того, вы вряд ли убедите сотрудников доводить до руководства информацию о кибербезопасности, противоречащую их интересам. Скорее, вам следует убедиться в том, что компания учитывает вышеописанные страхи людей. Помимо прочих мер безопасности, рекомендуем внедрить процедуру, позволяющую любому работнику предупредить руководство о проблемах в сфере кибербезопасности в обход организационной иерархии. В противном случае вы ничего не узнаете.

Человек и система

Помимо помех в получении критически важной информации, «отстрел гонцов с дурными вестями» попросту несправедлив и никак не способствует совершенствованию киберзащиты. Как говорилось в предыдущей главе, отдельно взятая процедура контроля вряд ли спасет от кибератаки; для этого требуется скорее система согласованных процедур. Аналогично и действия одного сотрудника редко играют решающую роль в том, сумеет ли компания защититься или падет жертвой кибератаки. В ситуации с компаниями, пострадавшими от вируса WannaCry,

не имело смысла обвинять сотрудников, вовремя не установивших обновление безопасности или не сделавших резервную копию жесткого диска. Если вам непременно надо кого-либо или что-либо обвинить, лучше обратите внимание на систему ведения бизнеса и деятельность в сфере кибербезопасности в целом. Упомянутые сотрудники — не более чем ее винтики. Именно здесь надо искать возможности для совершенствования.

Управление по исследованиям и оценке качества медицинского обслуживания опубликовало статью под названием Advances in Patient Safety: New Directions and Alternative Approaches («Разработки в области обеспечения безопасности пациентов: новые направления и альтернативные подходы»), где утверждало, что «...неблагоприятные последствия зачастую наступают в результате сбоев системы, а не из-за некомпетентности или халатности отдельных сотрудников». Именно поэтому многие компании в отрасли перестали объяснять ошибки исключительно некомпетентностью и больше не считают «...взыскания подходящими способами мотивировать сотрудников работать эффективнее»[119]. Они понимают, что кнут — деструктивное решение. «Замалчивание практически лишает людей возможности учиться на ошибках, а юристы зачастую поощряют такую практику, чтобы минимизировать риск судебных исков по делам о врачебных ошибках»[120].

---

[119] Linda Emanuel et al., "What Exactly Is Patient Safety?" *Advances in Patient Safety: New Directions and Alternative Approaches*, vol. 1 (Rockville, MD: Agency for Healthcare Research and Quality, 2008).

[120] Там же.

Куда полезнее обратить внимание на совершенствование бизнес-систем и процессов, где задействованы те или иные сотрудники. Недавние исследования в Китае подтвердили, что в случае возникновения проблем следует в первую очередь проверять работу систем, а не отдельных людей: «Если вся рыба погибла, дело не в рыбе, а в воде». Процессы идентификации и нейтрализации рисков, описанные в предыдущей главе, и практическое внедрение системы управления рисками, о которой мы говорили выше, повышают эффективность практик компании в сфере кибербезопасности лучше, чем фокус на действиях отдельно взятого сотрудника.

В этой области ваша задача — удостовериться, что компания:

- ☐ формирует среду, в которой сотрудники быстро и с готовностью докладывают о ситуации с кибербезопасностью, особенно если новости плохие.

Рекомендации для этого шага приведены в главе 12 (таблица 16).

Глава 10

Руководство в кризисных ситуациях

Избегать киберкризисов и предотвращать их — ваша первостепенная задача, но, увы, справиться с ней удается не всегда. Если, несмотря на все усилия по предотвращению, кибератака увенчается успехом, компания должна быть готова к бою. Придется и противостоять злоумышленникам, и отвечать потребностям и ожиданиям пострадавших стейкхолдеров, и в то же время постепенно возвращаться к работе. Из предыдущих глав вы уже многое знаете о сценариях киберугроз и о разработке планов по смягчению атак. Все это поможет вам подготовиться к кризису задолго до его наступления.

Технический ответ на кибератаку требует наличия квалифицированной команды и проверенных на практике процедур реагирования. Если ваша компания прежде сталкивалась с подобными угрозами, вы уже знаете, где необходимо сосредоточить внимание.

Топ-менеджеры несут основную ответственность за взаимодействие со стейкхолдерами, средствами массовой информации и государственными органами. У всех этих

коммуникаций разные задачи, начиная от признания вины и заканчивая получением компенсации или помощи. Если вы заблаговременно разработаете план по устранению киберрисков и проанализируете возможные последствия, вашим коллегам будет намного проще в момент кризиса: они будут знать, что сказать и какие действия предпринять. Если потребуется ваше непосредственное участие, вы сможете и сами использовать заранее подготовленные материалы. Но прежде чем погрузиться в их разработку, полезно взглянуть на некоторые уникальные характеристики кибератак и кризисов.

Характеристики кибератак

Кризис — это всегда неопределенность. Информации не хватает, а внешние факторы ограничивают ваши действия и коммуникации. Даже если компания привыкла действовать в кризисных условиях, все равно важно оценить три основные проблемы антикризисного управления: масштаб кризиса, отсутствие видимости и реакцию общественности — через призму киберпространства.

Масштабы кризиса

Оценить ущерб, особенно вначале, — сложная задача при любом раскладе. Но у киберпреступлений есть отличительная черта: их географические и организационные

масштабы могут значительно превышать масштабы любых других кризисов. Волнения и беспорядки могут привести к закрытию офиса или фабрики в одной части мира, но не повлияют на деятельность филиалов за пределами региона. Случай с утечкой данных TJX показал, что кибератака, начавшаяся в одном месте, способна быстро распространиться по всему миру. Хакеры вообще не ограничены географией. Этот факт напоминает нам о том, что ответ руководства на киберкризис может потребовать решения проблем стейкхолдеров в гораздо более широком диапазоне, чем мы привыкли.

Предсказать, как долго продлится кризис, также сложно. Учитывая отсутствие географических ограничений и масштабы ущерба, выявление всех последствий и проведение всех необходимых восстановительных мероприятий может занять много времени.

Отсутствие видимости

Кибератаки трудно обнаружить по нескольким причинам. В отличие от физических атак они незаметны. Кражу оборудования с завода заметить легко. А вот кража программного обеспечения на этом оборудовании не так очевидна.

Начало кибератаки может долго оставаться незамеченным. Недавнее исследование показало, что среднее время между совершением киберпреступления и его обнаружением — так называемое «время ожидания» или «время

идентификации» – колеблется от 101 до 197 дней[121]. Почему так долго? Одни компании не ищут тревожные сигналы вообще, другие не могут в них разобраться, а третьи ищут что-то не то. Кроме того, даже если система безопасности о чем-то предупреждает, не всегда понятно, является ли сбой компьютера результатом кибератаки, обычной ошибкой администратора или багом программного обеспечения.

Кроме того, трудно определить, кто стоит за кибератакой. Любые идентификационные данные: о местоположении, часовом поясе и языке, на котором создано вредоносное ПО, – вполне могут оказаться недостоверными. Десятилетиями хакеры сбивают противников со следа: сначала берут под контроль компьютеры в одной части мира, а затем оттуда атакуют другие регионы. Учитывая богатый рынок хакерских инструментов и услуг, описанный в главе 2, найти специалиста по вредоносным программам, который может читать и программировать на другом языке, не составляет труда. Предположение, что хакеры «выходят на тропу войны» только в рабочее время, также не верно, поскольку не учитывает ни их преступный азарт, ни ненормированный режим дня, характерный для программистов.

---

[121] Среднее «время ожидания» – 101 день (справедливо для обеих Америк, Европы, Ближнего Востока, Африки и Азиатско-Тихоокеанского региона). FireEye M-Trends 2018 Report, https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf. Среднее время идентификации (MTTI) – 197 дней (включает 15 стран/регионов по всему миру, n = 477 компаний). Ponemon Institute, "2018 Cost of a Data Breach Study," https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf.

Национально-государственная атрибуция

Многие государства развивают свой хакерский арсенал. Они делают это либо самостоятельно, как Кибернетическое командование США (US Cyber Command), либо приобретая инструменты на стороне, например у миланской Hacking Team[122]. И некоторые страны очень даже не против атаковать те или иные компании.

Жертвы кибератаки, широко освещенной в СМИ, всегда могут заявить, что за ней стоит государство-агрессор, — так они наверняка избегнут обвинений. В конце концов, какой бизнес справится с таким мощным противником?

Правительственные учреждения и компании, специализирующиеся на кибербезопасности, могут извлечь выгоду из «государственной» атаки. Подобные инциденты подтверждают необходимость их услуг и продуктов.

Страх прямых финансовых потерь также играет здесь свою роль. Об этом свидетельствует развивающийся рынок киберстрахования. После атаки NotPetya производитель продуктов питания Mondelēz International подал иск по своему киберстраховочному полису в Zurich American Insurance. Страховщик отклонил претензию, сославшись на пункт, по которому убытки от враждебных

[122] US Cyber Command, accessed January 28, 2019, https://www.cybercom.mil/; Hacking Team, accessed January 28, 2019, http://www.hackingteam.it/.

действий другого государства не покрываются ни полностью, ни частично[123].

Реакция общественности

Многие люди, даже не дочитав заголовок новостной заметки о кибератаке, бросаются обвинять компанию, а не хакеров. Это легкий способ найти козла отпущения и припомнить ему все громкие взломы прошлого.

Но правильно ли это? Обвинять компанию в том, что она стала жертвой киберпреступления, все равно что винить хорошо одетого человека в том, что его ограбили. Правда, есть существенное различие: если во втором случае пострадает только жертва грабителя, то последствия кибератак обычно затрагивают куда больше людей. Кроме того, как в случае атаки на Equifax, когда возник риск кражи личных данных более чем 140 млн человек, даже не обязательно иметь деловые отношения с компанией, чтобы оказаться в числе пострадавших.

Люди также склонны думать, что им лгут об истинной природе и масштабах кибератак. Недостаточная осведомленность самой компании о проблеме и непонимание руководителями того, что и когда лучше раскрыть, только

[123] John Pletz, "Keep a Close Eye on This Cyberterror Dispute between 2 Giant Companies," ChicagoBusiness.com, January 11, 2019, https://www.chicagobusiness.com/john-pletz-technology/keep-close-eye-cyberterror-dispute-between-2-giant-companies.

укрепляют недоверие. Оно может усугубиться, если руководители что-то утаивают в личных интересах. Так, например, руководство Equifax продало свои акции до того, как объявило о взломе компании[124].

Реагирование на киберинциденты

Реагирование на атаку требует и владения техническими основами кибербезопасности, и опыта координации сотрудников, и командной работы. Какие конкретно навыки вам пригодятся, зависит от характера атаки.

Не позволяйте технической природе киберинцидента загнать вас в тупик. Вы можете проверить боеготовность компании, задав несколько нетехнических вопросов. Вы должны убедиться, что ваша компания:

- собрала команду с необходимыми навыками и опытом для реагирования на наиболее значимые кибератаки;
- разработала в деталях процедуры реагирования на киберинциденты;
- проводит регулярное обучение по отработке методов реагирования и выявлению областей, нуждающихся в повышенном внимании.

[124] Liz Moyer, "Former Equifax Executive Charged with Insider Trading for Dumping Nearly $1 Million in Stock Ahead of Data Breach," CNBC.com, March 14, 2018, https://www.cnbc.com/2018/03/14/former-equifax-executive-charged-with-insider-trading-ahead-of-data-breach.html.

Команда реагирования

Как правило, она включает команду кибербезопасности и IT-отдел. Хотя некоторые общие навыки применимы к любому киберинциденту, специализированные навыки, необходимые вашей команде реагирования, зависят от типов атак, с которыми она, вероятно, столкнется. Например, справиться с вирусом поможет специалист по обратной разработке вредоносных программ. Эксперт в области компьютерной криминалистики будет полезен при реагировании на киберинцидент, связанный с финансовым мошенничеством сотрудников. Описания атак, включенные в сценарии киберугроз, помогут директору по кибербезопасности вашей компании решить, какие навыки необходимы команде.

В зависимости от характера атаки сотрудники других отделов — юридического, кадров, физической безопасности или по взаимодействию с правоохранительными органами — дополняют команду реагирования. В единичных случаях, требующих уникальных навыков, можно еще нанять кого-то со стороны. Но в целом достаточно иметь специалистов с необходимым базовым опытом, продвинутых экспертов же приглашать разово. Реагирование на киберинциденты требует глубокого понимания бизнес-процессов компании — и лучше поручить его коллегам, а действия, которые выиграют от выхода за рамки компании, разумнее делегировать третьим лицам.

От вас требуется обеспечить наличие в компании:

- команды реагирования, обладающей необходимыми навыками, чтобы эффективно противостоять самым разрушительным кибератакам.

Рекомендации для этого шага приведены в главе 13 (таблица 17).

Процедуры реагирования на киберинцидент

Первое, что нужно сделать, — определить, подвергается ли ваша компания атаке сейчас или уже подвергалась. Следующие важные элементы реагирования — ограничение масштабов атаки и ликвидация последствий. Здесь в свои права вступают чрезвычайное и кризисное управление бизнесом.

Мы уже отмечали, что навыки, необходимые для противостояния кибератаке, зависят от ее типа; некоторые процедуры реагирования варьируются по тому же принципу. Процедуры реагирования, основанные на специфике атак, описывают необходимые в конкретных условиях действия и вспомогательные инструменты. Прежде чем наступит киберкризис, ваша компания должна разработать как общие процедуры реагирования на киберинциденты, так и более специфические — для отдельных видов атак.

Ваша задача — проследить, чтобы у компании был:

- необходимый регламент реагирования на киберинциденты для борьбы с наиболее разрушительными кибератаками.

Рекомендации для этого шага приведены в главе 13 (таблица 18).

Практика реагирования на киберинциденты

Подготовиться к киберинциденту — одно, начать действовать с холодной головой — совсем другое. То, что выглядит ясным и простым на бумаге, в реальности может оказаться куда сложнее. Ключевую роль здесь играют технические навыки и умение ответить на следующие вопросы:

1. Как понять, указывают ли недавние сигналы и события на кибератаку?
2. Как настроить сети для предотвращения дальнейшего вторжения в компьютерную структуру вашей компании?

Еще два важных аспекта — логистика и координация. Да, звучит не так захватывающе, как «обратная разработка вредоносных программ», но это необходимо для успешного реагирования на киберинцидент. Зачастую их недооценивают. А ведь если, например, сотрудникам необходимо переустановить ПО на пострадавшем компьютере,

они должны знать, где этот компьютер стоит. В планах реагирования ключевые «узлы» часто обозначены кратко – по названию департамента. Это позволяет реже обновлять планы, но в кризисной ситуации отнимает время. Здесь важно знать конкретных людей, с которыми нужно связаться, и их телефонные номера, а также быть уверенным, что они быстро сориентируются и поймут, что делать.

В этом разделе мы используем слова «практика» и «подготовка». Мы специально избегаем слова «тест», которое подразумевает, что вы будете оценивать персонал. Ваша цель другая – выявить «зоны роста». Упражнения по реагированию на киберинциденты нужны не для анализа эффективности работы. Напротив, они должны быть достаточно сложными для проверки технических навыков, коммуникаций, логистики и способности принимать решения. Если ваши сотрудники не допускают ошибок и дают только правильные ответы, такая практика ничему их не научит. Это пустая трата ресурсов.

В конечном счете цель подготовки – создать обоснованную уверенность в технической и организационной готовности компании к кибератакам. Привлекая внимание к важности таких упражнений для укрепления бизнеса, вы тем самым задаете нужный настрой.

Ваша задача – проконтролировать, что компания:

- проводит тренинги по реагированию на киберинциденты и устранению наиболее значительных киберрисков;

- ☐ не забывает об упражнениях, позволяющих выявить области повышенного внимания и совершенствования.

Рекомендации для этого шага приведены в главе 13 (таблица 19).

Что делать топ-менеджерам?

Киберкризис – кризис бизнеса, вызванный кибератакой. Это означает, что здесь можно полагаться на существующие системы и процессы антикризисного управления, на прежние наработки в этой области. Вам стоит взять их на вооружение, но рассматривать через призму трех характеристик киберкризиса, выявленных ранее в этой главе.

Что должны делать или говорить топ-менеджеры? Это зависит от характера кризиса, состояния компании и ее позиции в области кибербезопасности. Так или иначе, можно подготовиться к ситуациям и решениям, с которыми бизнес, вероятно, столкнется в случае киберкризиса. Для этого требуется:

- определить приоритеты подготовки к киберкризисам;
- внедрить принципы принятия решений на корпоративном уровне;
- руководить действиями по восстановлению как компании, так и интересов пострадавших стейкхолдеров;

— предоставлять общественности своевременную достоверную информацию, учитывая интересы стейкхолдеров.

Приоритеты подготовки к киберкризисам

Если вспомнить о разнообразии потенциальных киберрисков, придется признать: подготовиться ко всему невозможно. Мы рекомендуем учитывать три фактора.

Значимость и воздействие

Вы должны уделять первостепенное внимание атакам, которые угрожают наиболее важным видам деятельности вашей компании и чреваты самыми серьезными последствиями. Некоторые кибератаки могут буквально сокрушить ваш бизнес, и такие риски стоит рассматривать с особой тщательностью.

Хороший пример значимой, широкомасштабной деятельности — передача электроэнергии. Перебои, особенно длительные, наносят значительный ущерб населению, и для этой отрасли кибератака куда опаснее, чем физические атаки на отдельные передающие подстанции.

Учитывая, что злоумышленниками чаще всего движут какие-то цели, важно ответить на вопрос: для кого привлекательна та или иная бизнес-цель? Сценарии киберугроз, составленные компанией для наиболее важных видов деятельности, служат основой при определении

приоритетов — помогают оценить значимость тех или иных бизнес-процессов, рисков и последствий.

Состояние киберзащиты

Другой важный момент — насколько ваша компания готова себя защитить. Развертывание средств обнаружения и предотвращения кибератак в масштабах всей организации может занять много времени. Если одни ваши системы уже отлично защищены, то другие пока более уязвимы. Кроме того, сама эффективность мер контроля может варьироваться по ряду причин. Штатное расписание, уровень инвестиций и характер кибератак влияют на то, насколько хорошо работает защита. Топ-менеджеры должны учитывать все это при определении приоритетов.

Портфолио киберкризисов

Разные киберкризисы бросают вам и вашим коллегам разные вызовы; каждый уникален. Например, экологический ущерб, вызванный атакой на Maroochy Water Services, и кража программного обеспечения у производителя турбин AMSC ставят перед руководителями этих компаний совершенно разные задачи. Можно составить показательный портфель киберкризисов на основании разных сценариев угроз, чтобы топ-менеджеры могли быстрее адаптироваться к ситуациям.

Ваша задача — помочь компании грамотно определить приоритеты подготовки к киберкризисам на основе:

- значимости и силы воздействия кибератак;

- состояния киберзащиты ключевых видов деятельности;
- разных типов киберкризисов.

Рекомендации для этого шага приведены в главе 13 (таблица 20).

Сценарии киберкризиса

Итак, вы определили типы киберкризисов, с которыми может столкнуться ваша компания. Теперь необходимо разработать сценарии для топ-менеджеров. Такие сценарии начинаются с описания деловых, политических и социальных факторов, способных привести к кибератаке, а также включают выявление потенциальных противников, их целей и мотивов. Почему мишенью можете стать именно вы?

Чтобы сценарий был реалистичным, стоит начать с краткого объяснения того, почему противники выбрали именно этот тип атаки и что им нужно для успеха. Предстоит перечислить необходимые знания (например, как работает то или иное оборудование) и инструменты, которые могут варьироваться от набора для взлома до болтореза. Кроме того, в сценарии нужно описать положение противника, как географическое (находится ли он поблизости или атакует удаленно), так и организационное (сотрудник это, подрядчик или кто-то со стороны). Далее должны быть обозначены основные этапы кибератаки.

Не забудьте о первом принципе цифрового управления: «Если вы этого не понимаете, вам плохо объяснили». Сценарий должен завершаться описанием грозящих последствий. Как кризис повлияет на вашу компанию, операции и оборудование, на клиентов и стейкхолдеров? Опишите все риски. Основная часть нужной информации уже содержится в сценариях киберугроз.

Ваша обязанность — убедиться, что компания включила в сценарии киберкризиса следующую информацию:

- ☐ факторы, при воздействии которых могут произойти кибератака и последующий кризис;
- ☐ описание кибератаки;
- ☐ последствия как для вашей компании, так и для стейкхолдеров.

Рекомендации к этому шагу приведены в главе 13 (таблица 21).

Быть в курсе событий

Чтобы эффективно руководить компанией во время киберкризиса, топ-менеджерам необходимо знать следующее:

- — как произошла кибератака;
- — какие меры защиты принимались, а также почему они провалились;
- — последствия для компании и стейкхолдеров;
- — прогресс в реагировании на киберинцидент.

Всегда существуют конкретные детали, которые компания предсказать не может. Но сценарии киберугроз дают отправную точку для определения типов атак, способных вызвать кризис, и диапазона последствий.

Чтобы понять, почему не удалось отразить атаку, необходимо ознакомиться с планами по устранению киберрисков: там описаны меры, принятые для смягчения удара. Кроме того, статус выполнения планов дает информацию о том, в каком состоянии компания находилась в момент атаки, насколько высоки были киберриски.

Невозможно заранее собрать информацию о текущих мероприятиях по реагированию на киберинциденты. Но можно подготовиться к тому, чтобы все источники такой информации были доступны, а руководители получали своевременные и точные сведения.

Всё как в тумане

Когда началась кибератака? Каковы масштабы ущерба? Это сложные вопросы, на которые нельзя быстро ответить. Такое отсутствие прозрачности может затруднить принятие антикризисных управленческих решений и взаимодействие со стейкхолдерами. В киберкризисных коммуникациях оперативность и точность диаметрально противоположны.

Например, американский ритейлер Target в 2013 году заявил, что взлом его платежной системы затронул 40 млн клиентов, но уже через месяц, в январе 2014 года,

увеличил это число до 70 млн. К тому времени, когда судебная сторона дела была улажена, количество пострадавших достигло 110 млн, что почти втрое превысило первоначальную оценку[125]. В сентябре 2016 года Yahoo объявила о взломе 500 млн учетных записей в 2014 году (рекорд на тот момент), но через три месяца обнаружила, что в 2013 году был еще один взлом, при котором пострадал 1 млрд пользователей. К октябрю 2017 года компания снова пересмотрела цифры: взлом затронул все 3 млрд учетных записей Yahoo[126].

Руководители компаний в таких случаях сталкиваются с трудным выбором: раскрыть информацию пораньше, но подорвать доверие из-за возможных неточностей или отложить заявления и подвергнуться обвинениям в непрозрачности или нежелании сотрудничать.

Ваша цель – убедиться, что компания готова предоставить руководителям информацию:

- ☐ о кибератаке;
- ☐ киберзащите и причинах, почему ее пробили;
- ☐ прогрессе в реагировании.

---

[125] Hiroko Tabuchi, "$10 Million Settlement in Target Data Breach Gets Preliminary Approval," *New York Times*, March 19, 2015, https://www.nytimes.com/2015/03/20/business/target-settlement-on-data-breach.html.

[126] Alina Selyukh, "Every Yahoo Account That Existed in Mid-2013 Was Likely Hacked," NPR.com, October 3, 2017, https://www.npr.org/sections/thetwo-way/2017/10/03/555016024/every-yahoo-account-that-existed-in-mid-2013-was-likely-hacked.

Рекомендации для этого шага приведены в главе 13 (таблица 22).

Топ-менеджмент и реагирование на киберинциденты

Все сказанное ранее описывает технические и координационные аспекты реагирования на киберинциденты. Но некоторые действия могут иметь серьезные последствия для вашей компании и ее стейкхолдеров.

Например, что делать в сам момент атаки? Первый вариант – позволить злоумышленнику остаться в сетях компании: это даст возможность собрать больше информации, чтобы затем оценить ущерб и проанализировать методы взлома. Другой вариант – отключить сетевые соединения и остановить атаку, однако это может привести к нарушению рабочих процессов компании, как внутренних, так и связанных с клиентами. Нужно ли закрывать онлайн-платформу или сборочный конвейер, если системы безопасности сигнализируют о кибервторжении? Эти вопросы выходят за технические рамки и требуют вашего решения.

Учитывая неизбежный цейтнот в момент кибератаки, важно заранее установить основные правила технического реагирования и сформулировать четкие рекомендации относительно того, когда нужно ввести в курс дела руководство. Начните со вспомогательных систем, описанных в ваших сценариях киберугроз. Компания должна понимать, как

действия по реагированию могут повлиять на ту или иную технику и бизнес-процессы, которые она обеспечивает.

Руководители должны быть осведомлены обо всем этом и одобрить намеченный курс до наступления кризиса. Это не требует каких-либо технических знаний. Уровня детализации, который мы использовали выше при описании потенциального компромисса между блокировкой хакера и потерей клиентов, вполне достаточно. Главное, чтобы ответ на кибератаку не увеличил ущерб и ответственность вашей компании сверх того, что она уже понесла.

Вы также должны рассмотреть другие аспекты реагирования на киберинцидент. Например, привлекать ли в таких ситуациях правоохранительные органы, включая полицию и прокуратуру? Их интересы совпадают с интересами компаний, подвергшихся кибератаке, но не во всем. Если основная задача бизнеса – восстановиться после кризиса, то цель правоохранительных органов – найти преступников и привлечь к ответственности. Правоохранительные органы могут в качестве улик конфисковать у вас что-нибудь ценное или сделать публичные заявления, которые будут противоречить интересам компании.

Ваша задача – чтобы топ-менеджеры компании:

- ☐ понимали, как те или иные аспекты реагирования на киберинциденты скажутся на бизнесе, и взвешенно принимали решения.

Рекомендации для этого шага приведены в главе 13 (таблица 23).

Планы по восстановлению

Еще до кибератаки важно решить, как вы будете устранять понесенный ущерб. Нельзя предсказать, когда именно случится беда, но можно прикинуть, насколько пострадают стейкхолдеры и компания. Все это описано в соответствующем сценарии киберкризиса.

Как и при любом кризисе, нужно подготовиться к ликвидации последствий, будь то перерыв в оказании услуг или в производстве, повреждение программного обеспечения или оборудования. Основываясь на опыте, извлеченном из кибератаки, компания может улучшить систему безопасности, чтобы снизить риск повторных инцидентов. Руководство при поддержке управленческой команды и экспертов по безопасности должно пересмотреть уровень устойчивости компании к киберрискам.

В большинстве случаев, пережив киберкризис, компании продолжают деятельность. Но бывают и другие примеры. Банк в Юго-Восточной Азии, который пострадал от массового мошенничества с дебетовыми картами, вышел из бизнеса. Его руководители поняли, что и в будущем не смогут управлять рисками. Они учитывали не только собственные возможности киберзащиты, но и внешние факторы: благоприятствующую махинациям схему комиссии за эквайринг и отсутствие сотрудничества с другими банками при расследовании таких преступлений.

Принятие решений о поддержке, которую ваша компания окажет пострадавшим стейкхолдерам, — одно из наиболее значимых действий в период киберкризиса. При

обсуждении подготовки руководителей к киберкризисам Ланкастер из CLP заявил: «Наши ценности должны учитывать все, что мы как компания делаем в кризис, и первый пункт здесь – защита жизни». В соответствии с масштабом возможного ущерба от кибератаки действия, которые компания предпринимает для помощи пострадавшим, могут отличаться от действий при других типах кризисов.

Разные типы атак наносят ущерб в разных масштабах, но независимо от этого, планируя дальнейшие действия, важно учитывать несколько общих моментов. Во-первых – юридические последствия, включая многочисленные обязательства вашей компании. Кроме того, создание прецедентов может наложить на вас обязательства в будущем, если ситуация повторится. Во-вторых, следует понимать, какое бремя вы возлагаете на пострадавших стейкхолдеров. Хорошая иллюстрация – единое корпоративное реагирование на утечку персональных данных. Обнаружив ее, компании обычно отправляют всем потенциально пострадавшим лицам электронные письма с инструкциями, как выяснить, коснулась ли утечка их данных. Другая распространенная практика – предложение дополнительных услуг, например годового мониторинга, но, чтобы воспользоваться ими, пострадавшие также должны принять меры.

Стейкхолдеры реагируют на это по-разному, в том числе негативно. Они могут счесть полученные инструкции оскорбительными – с учетом уже причиненного ущерба. Другой важный аспект связан с эффективностью оказываемой помощи. Если получить ее после атаки будет слишком сложно, люди не станут этого делать. Значит, они

по-прежнему будут уязвимы перед рисками, которым подверглись.

Ваша обязанность — убедиться, что топ-менеджеры приняли решение:

- ☐ о шагах по восстановлению;
- ☐ действиях по оказанию помощи пострадавшим стейкхолдерам.

Рекомендации для этого шага приведены в главе 13 (таблица 24).

Отчетность и ответственность

Пока вы будете решать вопросы подотчетности в области кибербезопасности внутри организации, киберкризис может повлечь за собой и внешнее давление, вплоть до призывов сменить руководство или выплатить штрафы. Лучше предвидеть это и подготовить ответные меры. Кроме того, можно подготовиться к тому, с какими запросами или расследованиями вы, скорее всего, столкнетесь во время киберкризиса.

Информация, предоставляемая руководителям, а также их решения по восстановлению деятельности и подотчетности — и есть материал, необходимый для взаимодействия со стейкхолдерами. Отделы корпоративных коммуникаций и связей с общественностью могут использовать их. При киберкризисе возникают те же вопросы

взаимодействия со стейкхолдерами, как и при любом другом кризисе, хотя ответы могут отличаться.

Также ваша компания должна рассмотреть два дополнительных вопроса.

1. Нанесет ли публичное раскрытие определенной информации вред?

   Например, если ваша компания в настоящее время подвергается активной кибератаке, публичное объявление об этом может насторожить злоумышленников и побудить их использовать другие, более скрытные методы. В этом случае раскрытие информации подорвет оборону вашей компании.

2. Причинит ли нераскрытие информации вред?

   Если ваша компания публично не заявит о кибератаке, подвергнет ли это клиентов и других стейкхолдеров новым рискам, которые они не могут смягчить, потому что не узнают о них?

Ваша задача — убедиться, что руководители компании:

- ☐ готовы привлечь общественность в случае возникновения киберкризиса.

Рекомендации для этого шага приведены в главе 13 (таблица 26).

Часть IV

Памятки-помощники

В трех предыдущих частях описаны действия, которые помогут вам и вашим коллегам управлять киберрисками, эффективно решать вопросы кибербезопасности и обеспечивать грамотное руководство в случае киберкризиса. Чтобы помочь вам контролировать эту деятельность, мы предлагаем воспользоваться памятками.

Здесь представлены конкретные вопросы о корпоративной кибербезопасности и средства, помогающие руководителям быстро и объективно оценить ответы. Памятки не охватывают все представляющие потенциальный интерес вопросы – так и задумано. Мы по собственному опыту знаем, что за каждое связанное с кибербезопасностью действие, которое предпринимает компания и которое вы контролируете, приходится платить не только деньгами, но и временем и концентрацией внимания. Ресурсы, включая внимание, ограниченны. Мы составили памятки, исходя из более чем 35 лет работы в области кибербезопасности. Все это время мы управляли, проверяли и отчитывались перед правлениями компаний по самым разным аспектам кибербезопасности. Мы побывали более чем в 40 странах. Мы выбрали наиболее важные и порой упускаемые из виду вопросы. Как уже отмечалось, многие вещи, необходимые для эффективного управления киберрисками, часто игнорируются, потому что в них не видят рыночной или корпоративной необходимости, а также личной заинтересованности.

Мы разрабатывали памятки таким образом, чтобы их использование не требовало узкоспециализированных скиллов и технического опыта. Но при этом, безусловно, обращение к нашим материалам расширит и углубит ваше понимание кибербезопасности. Вы можете начать использовать памятки прямо сейчас. Благодаря им вы ясно увидите, какую информацию запрашивать у сотрудников, — в противовес более распространенной ситуации, когда они сами решают, какие данные вам предоставить.

Каждая памятка состоит из четырех блоков. Перечислим их.

Запрос. Здесь содержатся вопросы, ответы на которые должны быть утвердительными, или информация, которую ваши сотрудники должны предоставить. Мы сформулировали запросы таким образом, чтобы вы могли сразу воспользоваться ими.

Обоснование. Краткое объяснение роли того или иного запроса по киберзащите и управлению киберрисками компании.

Документация. Примеры и описания материалов, которые отвечают на запрос. Они могут также включать указания о том, как и кому их разрабатывать и обновлять.

Контроль. Описание ваших действий по надзору, связанных с запросом. Здесь может быть три варианта действий.

1. *Подтвердить наличие документов.*
   Документация в некоторых памятках носит технический характер. Она может быть связана, например, с инвентаризацией компьютерных систем, без которых невозможны ключевые виды деятельности. Вам достаточно знать, что эти технические меры произведены и перепроверять вам ничего не нужно. Департамент внутреннего аудита может предоставить вам такие подтверждения и регулярно обновлять информацию. Если сотрудники не могут предоставить подтверждающие документы по тому или иному запросу, рекомендуется глубже и детальнее проработать область, к которой он относится.

2. *Предоставить консультацию по запросу.*
   Некоторые памятки затрагивают чисто деловые вопросы и вопросы бизнес-рисков — например, определение приоритетных видов деятельности и вероятных рисков в будущем. Учитывая широту вашего опыта, вы прекрасно сможете обсуждать эти и другие нетехнические вопросы.

3. *Принять к сведению.*
   Некоторые памятки преследуют дополнительные цели, помимо оценки действий вашей компании в области кибербезопасности. Они дают вам возможность больше узнать о киберугрозах для компании. Как было показано в главе 8 на примере кризиса в графстве Маручи, нетрудно описать связь между

атаками, контрмерами для их смягчения и возможными последствиями. Поскольку мы говорим об этом в контексте ваших обязанностей как руководителя, такое обучение пойдет вам на пользу больше, чем, например, посещение курсов и тренингов по кибербезопасности — с точки зрения как потраченного времени, так и приобретенных знаний.

Глава 11

Памятка: управление киберрисками

Цель этой памятки — подтвердить, что вы уделяете внимание самым значимым рискам и что инвестиции в кибербезопасность направлены на их снижение. Для начала необходимо определить наиболее важные виды деятельности вашей компании и осознать, каким образом кибератаки могут подвергнуть их риску. Эта информация станет основой для выбора инструментов контроля и планирования.

Выявление киберугроз

Таблица 4. Ключевые виды деятельности и риски

Запрос 1	Каковы наиболее важные виды деятельности компании? Какую ценность они создают? С какими наиболее значимыми бизнес-рисками здесь можно столкнуться?
Обоснование	Эти вопросы обеспечивают основу для подхода, который фокусируется на конкретных рисках для бизнеса, а не на общих рисках для компьютерной сети компании. Это первый шаг к тому, чтобы ваши инвестиции в кибербезопасность были непосредственно связаны с приоритетами компании
Документация	— Для каждого ключевого вида деятельности — краткое описание, обоснование ценности и перечень наиболее существенных бизнес-рисков. Рассмотрите виды деятельности, которые касаются продуктов и услуг вашей компании, ее внутренних процессов и перспектив. — Протоколы заседаний или другая документация, которая поможет выявить сотрудников, участвующих в определении этих видов деятельности и связанных с ними рисков. Нужно подтвердить, что именно эти руководители контролируют процесс и отвечают за него
Контроль	— Подтвердить, что описания видов деятельности и рисков составлены при участии руководства. — Выдвинуть предложения по выбору ключевых видов деятельности и связанных с ними рисков

Таблица 5. Ключевые компьютерные системы

Запрос 2	Располагает ли компания актуальными данными о состоянии компьютерных систем, на которых базируются ее ключевые виды деятельности?
Обоснование	Кибератаки подрывают ее важнейшие процессы, находя уязвимые места в компьютерных системах. Чтобы понять, с какими киберрисками вы можете столкнуться, сначала нужно выяснить, какие ваши системы могут пострадать и в чем именно они уязвимы. Кроме того, внедрение мер кибербезопасности может быть длительным процессом. Оно должно проходить поэтапно и определяться важностью поддерживаемых процессов. В случае кибератаки команда реагирования должна знать, где находятся пострадавшие компьютеры, чтобы решить проблему
Документация	— Отчеты об инвентаризации компьютерных систем, включая данные по «железу», программному обеспечению и расположению компьютеров для каждого из ключевых видов деятельности. Обычно инвентаризацию «железа» и ПО проводит IT-отдел, хотя зачастую эти данные не обновляются или не включают информацию о местоположении. — Описание процессов и инструментов, используемых компанией для поддержания компьютерных систем в рабочем состоянии, а также несколько примеров обновления описи
Контроль	— Подтвердить, что данные инвентаризации существуют и обновляются корректно и регулярно

Таблица 6. Кибератаки и их последствия

Запрос 3	Какие типы кибератак могут спровоцировать наиболее критичные бизнес-риски, какова широта и мощь их воздействия на компанию и стейкхолдеров?
Обоснование	С помощью этого запроса вы гарантируете, что отношение вашей компании к киберрискам согласуется с общим управлением бизнес-рисками. Кибератаки часто бьют по бизнесу больнее, чем другие проблемы. Это важно учитывать, выстраивая работу по снижению рисков и выбирая меры контроля
Документация	— Описание кибератак, способных создать крупные риски, и масштабов их потенциального воздействия. Кибератаку можно осуществить практически неограниченным количеством способов. Нет смысла перечислять все. Достаточно определить основные типы угроз – например, внешняя атака с использованием вредоносного ПО или злоупотребление полномочиями со стороны сотрудника
Контроль	— Подтвердить, что ваша компания выявила наиболее существенные риски, возникающие в результате кибератак, и масштаб воздействия. — Этот запрос дает вам возможность узнать больше о типах кибератак и степени ущерба, который они могут нанести компании

Таблица 7. Киберпротивники

Запрос 4	Кто может организовать кибератаку против компании и каковы мотивы и ресурсы этих людей?
Обоснование	Знание противников, у которых есть мотивы вредить вашему бизнесу, полезно при оценке вероятности кибератаки

Документация	— Список вероятных киберпротивников, их мотивы и ресурсы для атак. Эти мотивы могут быть связаны с конкретными аспектами — например, с деловой репутацией вашей компании, коммерческой тайной или географией рынков сбыта
Контроль	— Убедиться, что ваша компания учитывает эту информацию при разработке стратегии кибербезопасности. — Составить список вероятных киберпротивников и их мотивов

Смягчение киберрисков

Таблица 8. Приоритетность кибератак

Запрос 5	Предоставить приоритетный список кибератак исходя из следующих факторов: — их способность генерировать риски для ключевых видов деятельности; — масштаб и широта возможных воздействий; — ресурсы, необходимые для успешной атаки; — мотивы и возможности вероятных киберпротивников
Обоснование	Этот список — изложение приоритетов вашей компании в области снижения киберриска и гарантия, что они базируются на смягчении наиболее вероятных и самых мощных ударов
Документация	— Подробный список кибератак в приоритетном порядке
Контроль	— Убедиться, что в перечне учтены четыре фактора, указанные выше

Таблица 9. Выбор мер контроля

Запрос 6	Предоставить список рекомендуемых мер контроля, выбор которых основан на их способности смягчить последствия кибератак
Обоснование	Запрос обеспечивает уверенность в том, что ваши инвестиции в кибербезопасность направлены на устранение наиболее значимых киберрисков и что преимущества защиты понятны в широком бизнес-контексте
Документация	— Список рекомендуемых мер киберконтроля с указанием атак, которые смягчает каждый инструмент, и рисков, которые он помогает предотвратить. Как правило, для смягчения кибератак используется не один инструмент, а целый набор
Контроль	— Убедиться, что рекомендуемые меры киберконтроля выбраны с учетом особенностей указанных атак и отлаженных бизнес-процессов. — Запрос позволяет узнать больше о взаимосвязи между кибератаками, видами деятельности, которые они могут нарушить, и мерах, которые компания принимает для снижения рисков

Таблица 10. Оценка эффективности контроля

Запрос 7	Какие меры компания принимает для преодоления нетехнических препятствий, влияющих на эффективность киберконтроля?
Обоснование	Даже сложнейшие инструменты контроля за кибербезопасностью могут оказаться бесполезными, если не учитывать нетехнические факторы, связанные с использованием этих инструментов и поведением сотрудников
Документация	— Описание мер, при помощи которых компания нейтрализует нетехнические факторы, подрывающие администрирование и настройку инструментов контроля. Сюда можно отнести недопонимание, как использовать тот или иной инструмент, и ожидаемый отказ это делать, если он мешает выполнению функционала и текущих задач. В первую очередь проблема затрагивает отдел кибербезопасности и IT-персонал. — Описание мер, при помощи которых компания обеспечивает предсказуемую реакцию сотрудников на инструменты контроля. Сюда относятся ситуации, в которых правильное использование тех или иных мер дается слишком тяжело или препятствует работе. Это касается остальных ваших коллег
Контроль	— Подтвердить, что ваша компания учитывает нетехнические факторы. Если подобных препятствий не выявлено, рекомендуется изучить вопрос еще раз

Таблица 11. Разработка плана по устранению киберрисков

Запрос 8	Предоставить подробный план устранения киберрисков. Как и когда развертывание выбранных инструментов контроля и связанных с ними мероприятий снизит самые значимые киберриски до приемлемого уровня?
Обоснование	Помимо создания «дорожной карты» кибербезопасности, план устранения киберрисков представляет собой отчет об инвестициях и мероприятиях, которые компания считает достаточными для защиты ключевых видов деятельности. Подразумевается, что как только компания задействует инструменты контроля, начнет развивать их и внедрять в рабочие процессы, эти ключевые виды деятельности обретут необходимый уровень киберзащиты
Документация	— План устранения киберрисков. По сути, он представляет собой отчет о мерах и инвестициях, необходимых для снижения киберрисков до приемлемого уровня
Контроль	— Подтвердить разработку плана устранения киберрисков — Обеспечить принятие финансовых решений. Необходимо подключить к этому процессу руководителей, чья деятельность связана с теми киберрисками, которые планируется смягчить и/или устранить

Глава 12

Памятка: укрепление компании

Цель этой памятки — подтвердить, что ваша компания способна управлять киберрисками на постоянной основе. Такое управление включает внутренние процессы с точками контроля и грамотное распределение обязанностей по выявлению новых киберрисков и их устранению. Кроме того, в памятке представлены рекомендации, как сотрудники могут информировать вас о текущем положении дел. Наконец, здесь рассматриваются структурные и операционные вопросы, которые существенно влияют на эффективность деятельности компании в области кибербезопасности.

Прогнозирование киберрисков

Таблица 12. Систематизированный анализ бизнес-изменений

Запрос 1	Как компания отслеживает изменения, которые могут привести к появлению новых киберрисков? Это в том числе: — освоение новых видов деятельности и модернизация старых; — изменение структуры бизнеса; — изменения внешней бизнес-среды; — изменения, связанные с ведением предпринимательской деятельности
Обоснование	Отслеживание перечисленных изменений – практичный подход. Он помогает выявить модификации и дополнения в компьютерных системах, чреватые новыми киберрисками для компании. Вы сможете последовательно управлять киберрисками, только если анализ изменений будет интегрирован в ваши бизнес-процессы
Документация	— Документация по управлению всеми изменениями. Она должна содержать следующую информацию: • якоря и промежуточные точки контроля для отслеживания динамики; • обоснование того, какие бизнес-изменения *необходимо дополнительно проверить* на предмет киберрисков; • меры по смягчению последствий киберрисков; • зоны ответственности и необходимые компетенции. — Образцы записей, электронных писем и т. д., касающихся изменений в области кибербезопасности и необходимых исправлений

Контроль	— Подтвердить, что компания управляет изменениями, фиксирует их, не упуская нюансы, связанные с кибербезопасностью, и при необходимости устраняет киберриски

Управление новыми киберрисками

Информация, необходимая вашей компании для понимания новых киберрисков и управления ими, аналогична описанной в главе 8 для уже существующих рисков. Таким образом, для контроля над управлением новыми киберрисками опирайтесь на таблицы из главы 11. Поскольку многие новые риски будут связаны с текущей деятельностью и обеспечивающими ее техническими системами, можно использовать бóльшую часть этого предварительного анализа и документации для оценки будущих киберрисков.

Определение текущей ситуации с киберрисками

Таблица 13. Тестирование мер контроля

Запрос 2	Предоставить результаты тестирования мер контроля, выбранных для снижения киберрисков. Нужна количественная оценка эффективности
Обоснование	Есть заметная разница между внедрением мер киберконтроля и защитой, которую они должны обеспечить. С помощью этого запроса вы подтверждаете обоснованность инвестиций в инструменты киберконтроля, а также их надежность

Документация	— Результаты тестирования мер киберконтроля и разъяснения значимости результатов с точки зрения предотвращения бизнес-рисков. Нельзя оценить эффективность мер киберконтроля, проверяя только сами меры контроля
Контроль	— Подтвердить, что ваша компания провела тестирование мер контроля. — Углубить понимание взаимосвязей между разными инструментами киберконтроля и защитой вашей компании от наиболее серьезных рисков

Таблица 14. Прогресс в снижении киберрисков

Запрос 3	Предоставить актуальную информацию о состоянии плана по снижению киберрисков. Вместе с результатами тестирования мер контроля необходимо описать оставшиеся риски, с которыми сталкивается компания
Обоснование	Это поможет объективно измерить прогресс компании в снижении наиболее значительных киберрисков. В сочетании с результатами тестирования по предыдущему запросу и ранее установленными связями между мерами контроля и теми видами деятельности, которые они защищают, вы поймете, как обстоят дела с кибербезопасностью в вашей компании и куда двигаться дальше
Документация	— Отчет *о состоянии плана по снижению* киберрисков. — Результаты предыдущего тестирования, отчеты об актуальных рисках для всех приоритетных видов деятельности из запроса «Ключевые виды деятельности и риски». Желательно спрогнозировать даты, когда оставшиеся киберриски достигнут приемлемого уровня

Контроль	— Подтвердить, что компания разработала отчет и он актуален. — Этот запрос поможет ответить на один из ключевых вопросов, возникающих у вас и ваших коллег: «Насколько хорошо наша компания защищена от киберрисков?»

Оптимизация эффективности кибербезопасности

Таблица 15. Место команды кибербезопасности в структуре компании

Запрос 4	Обосновать включение в штат директора по кибербезопасности и команды кибербезопасности. Описать, как при этом учитывается интеграция с остальными отделами компании, насколько специалисты по кибербезопасности свободны в своих действиях и оптимизированы ли их коммуникации с высшим руководством
Обоснование	Позиционирование команды по кибербезопасности в компании очень важно: от него зависит, насколько эффективно эти специалисты будут работать. Исторически такие команды часто создавались в IT-отделах, хотя между директором по кибербезопасности и IT-директором наблюдается конфликт интересов. Если ваша команда кибербезопасности привязана к IT-отделу и ее невозможно переместить, нужно убедиться, что компания сможет справиться с конфликтом интересов. Этот вопрос находится в компетенции высшего руководства и не сводится к критике вашего IT-директора

Документация	— Обоснование положения команды кибербезопасности в структуре компании. — Меры для предотвращения потенциальных конфликтов интересов, которые могут подорвать эффективность работы IT-директора
Контроль	— Подтвердить, что ваша компания следует этим рекомендациям

Таблица 16. Повышение прозрачности

Запрос 5	Как компания способствует созданию корпоративной среды, где информация о кибербезопасности, особенно негативная, легко и быстро достигает адресата?
Обоснование	Причина этого запроса – нежелание многих сотрудников сообщать плохие новости, особенно если роль «гонца» может им повредить. Способность вашей компании защититься от кибератак зависит в большей степени от быстрого распространения дурных новостей, чем от хвастовства успехами. Как член совета директоров вы обладаете уникальными возможностями влиять на корпоративную культуру. За счет развития коммуникаций вы сумеете улучшить положение дел компании в области кибербезопасности
Документация	— Официальные корпоративные материалы, подчеркивающие важность передачи информации о кибербезопасности. Нужно сделать акцент на отсутствии карательных последствий для сотрудников, чьи действия, возможно, способствовали возникновению киберрисков. — Примеры внутрикорпоративных коммуникаций, повышающих осведомленность об этой политике. — Меры по соблюдению этой политики на практике
Контроль	— Провести исследование и подтвердить, что нужные документы созданы

Глава 13

Памятка: управление в период кризиса

Цель этой памятки — подтвердить, что ваша компания готова к кризису, вызванному кибератаками, и способна грамотно реагировать в экстремальных условиях. Это подразумевает как технические возможности дать отпор, так и готовность руководства выстраивать коммуникации в это острое время. Хотя в каждом кризисе есть свои неожиданности, типы технических навыков и ресурсов, которые вам понадобятся, а также решения, которые вам предстоит принять, в значительной степени предсказуемы и могут быть проработаны задолго до кризиса.

Реагирование на киберинциденты

Таблица 17. Команда реагирования

Запрос 1	Имеет ли компания достаточный штат сотрудников для эффективного реагирования на наиболее разрушительные киберинциденты?
Обоснование	Хотя существует общий набор навыков, необходимых для реагирования на любой киберинцидент, многое зависит от специфики. Запрос даст вам информацию о том, насколько компания готова к киберинцидентам, способным нанести ей наиболее серьезный ущерб
Документация	— Список основных членов команды реагирования на киберинциденты, их функционал и квалификация. — Расширенный список. Туда входят члены других подразделений компании, дополняющие основную команду. Описаны их роли и типы киберинцидентов, к работе с которыми их нужно привлекать. — Перечень сторонних служб реагирования, их обязанности и ситуации, в которых необходимо привлекать этих людей. — Описание, как компания продолжит работу, пока персонал будет бороться с киберинцидентом
Контроль	— Подтвердить, что информация связана прежде всего с приоритетными кибератаками, выявленными в запросе 5 (таблица 8). — Этот запрос дает вам возможность узнать о разных навыках, необходимых для реагирования на киберинциденты в вашей компании

Таблица 18. Подготовка и процедуры реагирования на киберинциденты

Запрос 2	Какое планирование провела компания, чтобы подготовиться к реагированию на киберинциденты?
Обоснование	Реагирование на разные типы киберинцидентов требует не только разных навыков, но и разнообразных ответных действий и инструментов. Вам нужно удостовериться, что команда реагирования предусмотрела все типы инцидентов, с которыми может столкнуться, виды ответных мер и провела необходимую подготовку
Документация	— Перечень процедур реагирования на киберинциденты и стандартных шагов, связанных с любым инцидентом, а также дополнительных мероприятий, имеющих отношение к конкретным типам инцидентов. — Списки необходимых инструментов реагирования и способов доступа к ним. Можно использовать несколько самых распространенных инструментов внутри компании, а в особых случаях прибегать к услугам третьих лиц
Контроль	— Подтвердить наличие процедур реагирования на киберинциденты и рассмотреть приоритетные кибератаки, выявленные в запросе 5 (таблица 8). — Подтвердить, что ваша компания имеет доступ к необходимым процедурам реагирования на инциденты и юридическим мерам для приоритетных кибератак

Таблица 19. Практика реагирования на киберинциденты

Запрос 3	Как компания обучает сотрудников реагированию на киберинциденты? Что можно улучшить благодаря тренингам? Какое обучение планируется?
Обоснование	Давление и сложность, присущие реагированию на киберинциденты, часто таковы, что вашей компании полезно потренироваться заранее. Внимание, которое вы уделите такому обучению, очень важно. Оно поможет выявить слабые места намного эффективнее, чем демонстрация текущих возможностей в сфере кибербезопасности
Документация	— План тренингов по реагированию на киберинциденты, где рассматриваются атаки, чреватые наиболее серьезными рисками и кризисами. — Отработка процедур реагирования на киберинциденты достаточной сложности. Они помогут протестировать технические навыки, скорость принятия решений, коммуникации и логистику. — Планы по улучшению реагирования, составленные по итогам этих учений
Контроль	— Посещать практические занятия по реагированию на критически важные типы киберинцидентов. — Подтвердить, что компания проводит такое обучение и намечает области дальнейшего совершенствования

Действия топ-менеджеров

Таблица 20. Определение приоритетов подготовки к киберкризису

Запрос 4	К каким киберкризисам необходимо подготовить топ-менеджеров компании?
Обоснование	Невозможно быть во всеоружии перед каждым киберкризисом, с которым компания может столкнуться. Но важно, чтобы топ-менеджеры были готовы хотя бы к некоторым. Таким образом, нужно решить, какие типы киберкризисов приоритетны. С помощью этого запроса компания подготовит высшее руководство к наиболее значимым киберкризисам
Документация	— Описание киберкризисов, к которым необходимо подготовиться, а также обоснование выбора, включающее: • значимость затрагиваемых видов деятельности и серьезность воздействия; • уровень риска из-за недостатка контроля; • кейсы разных типов киберкризисов
Контроль	— Подтвердить выбор киберкризисов и его обоснованность. — Представить свои идеи о дополнительных типах киберкризисов, на которые стоит обратить внимание

Таблица 21. Сценарии киберкризиса

Запрос 5	Разработать сценарии киберкризиса. Какие атаки способны его вызвать? При каких условиях может произойти атака? Каковы возможные последствия?
Обоснование	Чтобы дискуссии о потенциальных киберкризисах были конструктивными, сценарии должны быть реалистичными. Они должны четко связывать кибератаку на компьютерные системы вашей компании с воздействием на бизнес
Документация	— Сценарии для каждого приоритетного киберкризиса, которые включают: • условия, при которых могут произойти кибератака и последующий кризис; • описание кибератаки, ресурсов, необходимых для ее успеха, и основных этапов; • последствия киберкризиса как для вашей компании, так и для стейкхолдеров
Контроль	— Убедиться, что сценарии содержат необходимую информацию. — Использовать этот, а также другие запросы, чтобы получить больше информации о киберкризисах, с которыми может столкнуться ваша компания

Таблица 22. Топ-менеджмент и осведомленность

Запрос 6	Описать подготовительные меры, включая источники информации и распределение обязанностей по информированию руководителей в период киберкризиса
Обоснование	Руководители нуждаются в своевременной и точной информации как для антикризисного управления компанией, так и для взаимодействия с общественностью. Учитывая цейтнот во время кризиса, лучше подготовиться заранее
Документация	— Планы информирования руководства: • о кибератаке; • киберзащите (и о том, почему ее пробили); • прогрессе в реагировании на киберинцидент
Контроль	— Подтвердить, что ваша компания определила источники информации и внедрила соответствующие процедуры

Таблица 23. Топ-менеджмент и реагирование на киберинциденты

Запрос 7	Проинформировано ли руководство о том, как те или иные действия по реагированию скажутся на бизнесе? Определена ли стратегия информирования общественности о решениях в этой области?
Обоснование	Некоторые действия по реагированию на киберинциденты, такие как разрыв интернет-соединений, могут сказаться на деятельности вашей компании и иметь негативные последствия для других стейкхолдеров. Руководству следует оперативно об этом докладывать, чтобы оно могло принять правильные решения и дать верные указания. Чтобы избежать ненужных задержек в реагировании на киберинцидент, все лучше продумать заранее
Документация	— Для каждой приоритетной кибератаки – описание процедур реагирования, которые могут повлиять на бизнес, и анализ компромиссных решений. Анализ должен включать соизмерение эффективности разрешения киберинцидента с ущербом для компьютерных систем, поддерживающих критически важные виды деятельности. — Протоколы заседаний, электронные письма и другие доказательства того, что команда кибербезопасности, IT-отдел и задействованный оперативный персонал провели этот анализ. — Основанный на бизнес-приоритетах план действий, позволяющий руководителям принять решения по реагированию на инциденты
Контроль	— Подтвердить, что ваша компания провела анализ компромиссов и сформировала план действий

Таблица 24. Планы по восстановлению

Запрос 8	Что предпримет компания для восстановления работы и помощи пострадавшим стейкхолдерам?
Обоснование	Эффективное восстановление деятельности и возмещение ущерба, причиненного кибератакой, дают прямые финансовые выгоды. То, как ваша компания помогает пострадавшим стейкхолдерам после киберкризиса, серьезно влияет на сохранение и улучшение ее репутации. Чтобы обеспечить достаточное время для аргументированного обсуждения и проведения необходимых подготовительных мероприятий, эти действия должны осуществляться задолго до киберкризиса
Документация	— Планы по восстановлению операционной деятельности компании, ее компьютерных систем и оборудования. — Описание планируемой помощи пострадавшим стейкхолдерам. — Документы, например заказ-наряды или контракты, показывающие, что компания провела необходимые приготовления
Контроль	— Подтвердить, что ваша компания продумала действия для помощи пострадавшим стейкхолдерам. — Изложить свои соображения о целесообразности запланированных восстановительных мероприятий

Таблица 25. Отчетность и ответственность

Запрос 9	Как компания готовится к внешнему давлению?
Обоснование	Справедливо или нет, но после кибератаки многие возложат вину и ответственность на вашу компанию. Вы должны уметь реагировать
Документация	— Стратегия на случай требований смены руководства. — Список вероятных запросов и грозящих расследований, а также планов реагирования
Контроль	— Подтвердить, что компания учла возможную внешнюю реакцию и требования общественности. — Выдвинуть предложение о целесообразной реакции компании на смену руководства

Таблица 26. Вовлечение стейкхолдеров

Запрос 10	Как мы готовы привлекать общественность в случае киберкризиса?
Обоснование	Используя памятки, ваша компания уже собрала и проанализировала бóльшую часть информации, необходимой для эффективного руководства в условиях киберкризиса. Запрос поможет удостовериться, что компания использовала эту информацию в подготовке информационных материалов для руководителей задолго до киберкризиса. Также он подтвердит, что процедуры и обязанности, необходимые для поддержки топ-менеджеров в кризисный период, определены
Документация	— Для каждого киберкризиса – заранее подготовленные материалы. Описание принятых мер, включая актуальную информацию о ходе кибератаки и реагировании на нее. Наработки материалов, проясняющих для руководителей следующие вопросы: • Какая кибератака вызвала кризис? (Лучше начать с запроса 3 в таблице 6.) • Как она повлияла на компанию и стейкхолдеров? (Тот же запрос.) • Почему компания не смогла отразить кибератаку? (Лучше начать с запроса 3 в таблице 14.) • Каковы планы компании по решению проблем пострадавших стейкхолдеров? (Лучше начать с запроса 8 в таблице 24.)
Контроль	— Подтвердить, что компания провела все подготовительные мероприятия по киберкризисным коммуникациям. — Выдвинуть свои предложения по поводу деятельности совета директоров / топ-менеджеров во время киберкризиса

Выводы

В начале книги мы высказали два замечания о проблемах кибербезопасности, уже знакомых большинству людей. Любой, кто читает новости, в курсе, что уровень и разрушительный потенциал киберпреступности продолжают расти, сколько бы инвестиций ни вливалось в кибербезопасность и как бы ни наращивалась осведомленность в этой области. Зачастую многие руководители компаний с опаской относятся к теме кибербезопасности, потому что не имеют релевантного опыта. Кажущаяся неприступность этой сферы только усиливает их тревогу.

Ключевая причина обеих проблем такова: центральное место в попытках обеспечить кибербезопасность отдается технологиям. Из-за акцента на программном обеспечении, сетях и оборудовании игнорируются многие нетехнические факторы, необходимые для создания успешной защиты. При таком характере диалога о кибербезопасности упускаются важные моменты и тормозится сотрудничество. Из-за обилия специализированной терминологии членам советов директоров и высшему руководству трудно участвовать в обсуждении и принятии решений о киберрисках, с которыми сталкиваются их компании.

Несмотря на неспособность защитить себя в цифровом мире, многие возлагают надежды на все более сложные

и дорогостоящие IT-продукты и IT-услуги: вдруг это поможет держать хакеров в страхе? Аналогичным образом в большинстве рекомендаций, которые дают советам директоров, подчеркивается важность обучения основам кибербезопасности, в связи с чем плодятся соответствующие курсы и сертифицированные программы.

Из-за отсутствия действенного подхода к кибербезопасности страх вытесняет аргументы разума; все чаще звучат пессимистичные заявления в духе «Вопрос не в том, будут ли вас взламывать, а в том, когда» или «Есть два типа компаний: те, кто знает, что их взломали, и те, кто еще не в курсе». Этот дух смирения сместил акценты, и вместо предотвращения или заблаговременного обнаружения кибератак принимаются только ответные меры борьбы — после того как атака уже произошла. Но ведь мы не отказываемся от ремней и подушек безопасности в пользу развертывания армий машин скорой помощи и вертолетов, чтобы доставить жертв катастроф в реанимацию?

Меняем угол зрения и вектор действий

Вы и ваши коллеги по совету директоров лучше всех поможете компании развить новый взгляд на кибербезопасность. Начать стоит с конкретных деловых решений, а не абстрактных битов и байтов. К тому же вы можете многое изменить, просто выполняя свои обязательства по надзору. Наше руководство по цифровому управлению

включает инструменты, необходимые вам для расширения контроля над кибербезопасностью. Детализируя информацию, которую сотрудники должны вам предоставить, мы также подсказываем, какие шаги полезно предпринять, чтобы эффективно управлять киберрисками. Эти действия подразумевают выход за рамки технологических подходов к кибербезопасности и смещение акцента на прочие факторы, которые обычно игнорируются.

Главы про задачи и памятки-помощники содержат важную информацию о том, что нужно сделать и какие документы вам потребуются. Есть несколько взаимосвязанных факторов, поясняющих, почему нужен такой уровень детализации. Во-первых, мы хотим сделать контроль над кибербезопасностью максимально простым и понятным, предоставив четкие рекомендации. Кроме того, мы хотим показать, как выйти за пределы технических вопросов, чтобы собрать и проанализировать все необходимые данные для защиты от киберрисков. Это включает предоставление вам и другим членам совета директоров актуальной информации в доступной форме. Первый принцип цифрового управления гласит, что вы заслуживаете понятных объяснений.

Мы написали эту книгу не только чтобы вам было легче управлять кибербезопасностью, но и чтобы команде кибербезопасности было проще выполнять свою работу. Если ваши сотрудники смогут объяснить, например, связь между сбоями в критически важных бизнес-процессах и кибератаками, то будут знать, на чем сосредоточить усилия по киберзащите. Также они получат больше возможностей просить о финансировании, потому что

выгода от инвестиций будет предельно ясна. Кроме того, мы хотим показать, что все действия, которые компании должны предпринять для эффективного управления киберрисками, реалистичны и просты. Не нужны ни магия, ни армия консультантов. Сотрудники, которые хорошо знают, как работает их бизнес, выполняют эти действия наиболее эффективно.

С помощью запросов вы улучшите работу вашей компании и укрепите рубежи обороны в области кибербезопасности. Проще говоря, вы добьетесь прогресса, сместив акценты с технологий на бизнес, который на этих технологиях держится. Это не только повысит эффективность управления киберрисками, но и снизит нагрузку на совет директоров, топ-менеджеров и команду кибербезопасности. В результате обсуждение вопросов кибербезопасности и принятие решений для вас и ваших коллег значительно упростится. Обращаться к нетехническим факторам и разговаривать с людьми гораздо проще, чем решать многие технические задачи. Тем самым фокус сместится со сложных, но менее полезных задач на более легкие и полезные.

Взгляд в будущее

Мы уже говорили о том, что вы с коллегами из совета директоров могли бы стать отличными лидерами в области кибербезопасности для вашей компании. Но если рассмотреть вопрос лидерства в этой области шире? Кто может здесь руководить?

Вполне естественно ожидать, что лидером в области кибербезопасности станет правительство страны, учитывая традиционно выполняемые им функции по обеспечению национальной обороны и правоохранительной деятельности. Иногда правительственные учреждения уведомляют компании о внешних сетевых атаках, о которых те не знают. Но при ближайшем рассмотрении оказывается, что у правительств недостаточно возможностей. Например, они никогда не смогут разобраться в тонкостях вопросов кибербезопасности внутри компании. Кроме того, они способны мобилизовать количество сотрудников, достаточное для оказания помощи лишь небольшой части коммерческих предприятий. А что делать остальным и населению в целом?

Все предстает совершенно иным, если перевести взгляд с высших органов власти на мир бизнеса. Такие компании, как ваша, а вовсе не правительство, создают, владеют и управляют подавляющим объемом информации, большинством объектов инфраструктуры, продуктов и услуг, от которых зависят государство, экономика и общество в целом. Компании находятся на передовой кибератак и кибероборо-ны. И то, как вы защищаете свои продукты и услуги, влияет на то, что будет с вашими клиентами в случае кибератаки.

С этой точки зрения добросовестная и эффективная деятельность в области кибербезопасности приносит пользу не только самой компании и стейкхолдерам, но и всему миру. Управляя кибербезопасностью собственного бизнеса, вы вносите существенный вклад в более безопасное цифровое будущее.

И вы можете начать прямо сегодня.

Благодарности

Мы в долгу перед нашими многочисленными клиентами, чье профессиональное, географическое, культурное и организационное разнообразие дало возможность протестировать и усовершенствовать наши методы работы.

Поддержка Harvard Business Review Press, которую они оказывали на протяжении подготовки этой книги, действительно неоценима. В частности, мы хотим поблагодарить Джули Деволл, которая обеспечила синхронизацию с первой нашей книгой; Тима Салливана, который начал этот процесс; и Кевина Эверса, который руководил нашей работой.

Наконец, хотим сказать спасибо нашим семьям. Наши жены, Янг и Беверли, признали важность написания этой книги и поддерживали нас все время. Наши дети – Мартин, Жаклин, Шарлотта и Натали – и будущее, которое они олицетворяют, были нашим источником вдохновения. В свою очередь мы надеемся, что эта книга вдохновит их изменить мир.

Об авторах

Томас Дж. Паренти – международный эксперт в области кибербезопасности и защиты информации. Более 35 лет работал в Агентстве национальной безопасности, неоднократно выступал в Конгрессе США по вопросам шифрования и национальной безопасности, консультировал правительственные учреждения и транснациональные корпорации по противодействию киберугрозам. Популярный лектор и спикер, он часто пишет для таких изданий, как Wall Street Journal, New York Times, Economist и South China Morning Post. Соучредитель компании Archefact Group и автор книги Digital Defense: What You Should Know About Protecting your Company's Assets (Harvard Business School Press, 2003).

Джек Дж. Домет – эксперт по менеджменту. Более 25 лет работает с транснациональными корпорациями, помогая им посредством организационных изменений адаптироваться к инновациям, глобализации и консюмеризму, а также эффективно управлять киберрисками, с которыми сталкиваются компании. Является соучредителем Archefact Group, где отвечает за развитие лидерского и организационного потенциала в области цифрового управления.

Научно-популярное издание

Томас **Паренти**
Джек **Домет**

Кибербезопасность
Что руководителям нужно знать и делать

Издано при поддержке компании «Код Безопасности»

Шеф-редактор *Ренат Шагабутдинов*
Ответственный редактор *Анна Красова*
Литературный редактор *Екатерина Гришина*
Арт-директор *Алексей Богомолов*
Дизайн обложки *Наталия Майкова*
Верстка *Елена Бреге*
Корректоры *Наталья Мартыненко, Юлия Молокова*

Подписано в печать 11.02.2021
Формат 84×108/32 . Гарнитура NewBaskerville.
Бумага офсетная. Печать офсетная.
Усл. печ. л. 15,87. Тираж 2000 экз.
Заказ 1640.

ООО «Манн, Иванов и Фербер»
mann-ivanov-ferber.ru
facebook.com/mifbooks
vk.com/mifbooks

Отпечатано в АО «Первая Образцовая типография»,
филиал «УЛЬЯНОВСКИЙ ДОМ ПЕЧАТИ»,
432980, Россия, г. Ульяновск, ул. Гончарова, д. 14
http://www.uldp.ru