Эллисон Сэрра

Кибербезопасность: правила игры

Как руководители и сотрудники влияют на культуру безопасности в компании

Перевод с английского

PRO
Москва
2022

Фрэнку, любви всей моей
жизни, — тому, кто читал
каждую написанную мною
страницу, включая эту.
Спасибо, что любишь меня
и поддерживаешь.

Глава 1

Как я испортила Пасху

Бывали у меня воскресенья и получше.

16 апреля 2017 года, Пасха. Мы с мужем сидели дома, только закончили ужинать. Настало долгожданное время насладиться покоем и нашим новым увлечением — запойным просмотром Netflix. Знала бы я тогда, что вот-вот сыграю главную роль в собственной драме, заслуживающей гораздо большего внимания…

Загорелся экран моего телефона — пришло сообщение от Шатель, руководителя нашего отдела по подбору персонала. Мы с ней тесно общались. Всего 12 дней назад мы помогли McAfee отделиться от Intel в качестве одной из крупнейших независимых компаний в области кибербезопасности. Я не удивилась ее сообщению на Пасху — думала, она просто прислала мне поздравления с праздником. Но речь там шла не об этом.

«Загляни к нам в соцсети. Дело плохо».

Я открыла страницу McAfee в очень известной социальной сети, название которой не буду здесь упоминать, — и пришла в ужас.

Кто-то взломал профиль нашей новорожденной компании, которой едва исполнилось 12 дней, и исписал страницу самыми грязными и непристойными выражениями, какие только могут прийти в голову. Такое не лучшим образом сказалось бы на любой фирме. Но стоит объяснить, насколько плохо, бесконечно плохо это было для нас.

Оскорбительные надписи резко противоречили всему, что представляла наша организация. Мы только что перезапустили бренд с новым слоганом «Вместе — сила», отражавшим нашу веру в то, что для защиты мира от киберугроз нужно использовать все возможные средства. Мы только что представили сотрудникам новые ценности компании, одна из которых — *всеобъемлющая* открытость и прозрачность. И мы были лидерами в области *кибербезопасности*. Что подумают клиенты о нашей способности сохранить их самые ценные цифровые активы, если мы не можем защитить даже собственный профиль в одной из крупнейших соцсетей? И вдобавок ко всему, именно моя команда — маркетинговая организация — отвечала за

управление профилями компании во всех социальных медиа, включая этот, «опороченный» прямо у меня под носом.

Я начала действовать. Нужно было связаться с главой нашей диджитал-команды, чтобы понять, что происходит. Я сразу дозвонилась ей, и мне не пришлось объяснять, что звонок никак не связан с Пасхой.

— Я знаю, почему ты звонишь. Мы разбираемся. Наш аккаунт взломали. Мы на связи с [социальной сетью], решаем проблему.

Я начала думать о худшем. Взломанный аккаунт — это одно. Но что если это скоординированная атака на McAfee? Вдруг хакеры нацелились на добычу покрупнее и отвлекли наше внимание этой «пожарной тревогой», чтобы параллельно проникнуть в систему компании?

Руководитель диджитал-команды тут же уверила меня, что наш директор по информационной безопасности уже все проверил и подтвердил: все системы в порядке. На миг я испытала облегчение, но тут же осознала, что нужно сделать еще один звонок. Генеральный директор должен быть в курсе происходящего. И лучше бы мне сообщить ему новости лично. Итак, я набрала его номер, собираясь испортить и ему пасхальное воскресенье. Он взял трубку почти мгновенно.

— Крис, один из наших аккаунтов в социальных сетях взломали.

— Насколько все плохо? — сдержанно спросил он.

— Корпоративные сервера в порядке, Крис. Взломана страница компании на сайте социальной сети.

Я объяснила ему, что случилось. Первым проблему обнаружил Гэвин, наш SMM-специалист. Он был дома и занимался тем же, чем и многие фанаты социальных сетей на выходных, — сидел в сети. Около пяти часов вечера он увидел, что статус на странице компании поменялся на произвольный набор букв. Гэвин предположил, что сообщение случайно написал кто-то из его команды, — и удалил пост.

Затем он связался с сотрудниками, чтобы выяснить, чьих это рук дело. Об обновлении никто ничего не знал.

Вскоре появился новый бессмысленный пост. И теперь он был неслучайным.

Гэвин залогинился в социальной сети и перешел в настройки аккаунта. Имена всех людей, имеющих доступ к управлению страницей, были ему знакомы. Но чтобы перестраховаться, он начал закрывать доступ другим администраторам из списка.

Пока он делал это, страница в браузере обновилась — и его «выкинуло» из аккаунта.

Теперь сомнений в злонамеренности действий не осталось. За секунду Гэвин сообразил, что удаление поста сообщило хакеру: в

McAfee знают о взломе. Началась классическая гонка из криминальных фильмов о технологиях: пальцы летали по клавиатуре, появлялись и скрывались значки программ, всплывали сообщения — все в лучших традициях Голливуда. Гэвин и злоумышленник на всех парах в режиме онлайн неслись к одной цели. Даже отсутствие напряженного саундтрека не снижало накала страстей. Гэвин рассказал: «Я старался удалить всех остальных администраторов, и хакер делал то же самое. Он сработал быстрее».

Прежде чем закончить разговор с генеральным директором, мне пришлось поделиться с ним еще одной неутешительной новостью.

— И еще, Крис, зайдя на нашу страницу, вы увидите не только оскорбительные посты, но и картинку, которой заменили лого нашей компании — что-то вроде птицы. Присмотритесь. Это вовсе не птица. Это… кхм… это части тела.

Распространенная вещь в хакерском сообществе — «украшать» взломанные сайты непристойными рисунками, чтобы пометить тех, кто был, как говорят на сленге, «унижен», кого «хакнули». Хакер уже знал, что мы заблокированы и ситуация под его контролем; он повесил пошлую картинку вместо нашего нового логотипа просто так, на всякий случай.

Моя команда максимально вовлекла службу поддержки социальной сети в решение проблемы. Но… в праздники все происходит дольше. Поскольку был уже поздний вечер, нас перевели на сотрудников группы, работающей в Азиатско-Тихоокеанском регионе. Создавалось впечатление, что время физически преодолевало океан, разделяющий нас и службу поддержки. Минуты ползли со скоростью улитки.

Казалось, ожидание длилось целую вечность. Взломали не наши сервера, и у меня не было возможности подключить команду специалистов из McAfee к решению сторонней проблемы. Мы могли лишь каждые несколько минут связываться со службой поддержки, чтобы снова получать ответ: «Мы работаем над этим».

Примерно через полчаса они сообщили, что заблокировали *всех* администраторов нашей корпоративной страницы, и доступ к ней остался только у них. Это были хорошие новости: по крайней мере, большего вреда нанесено не будет.

А что насчет плохих новостей? Они не могли просто откатить страницу до версии 30-минутной давности. Согласно протоколу, страницу заблокировали, чтобы никто больше не мог изменять ее, а затем должны были последовать процедуры проверки и анализа. В ходе первой они должны были удостовериться, что мы действительно те, за кого себя выдаем, а не хакер, только притворяющийся McAfee (какая

ирония!). Анализ же призван был определить степень взлома — и только затем можно было предпринимать дальнейшие действия.

Но как быть с непристойным аватаром? Он все еще висел на нашей корпоративной странице. Хуже того: платформа работала таким образом, что в личных профилях всех сотрудников McAfee в социальной сети вместо логотипа компании также отображалась эта пошлая картинка.

И в моем тоже.

Когда мы снова связались со службой поддержки, нам сообщили, что «процедуры» еще не закончены. Если следовать их логике, выходило, что единственный шанс откатить страницу — реактивировать, то есть разблокировать аккаунт, но они не сделают этого до тех пор, пока не закончат проверку безопасности.

Серьезно? Как это вообще возможно? С нашей страницей *ничего* нельзя было сделать до окончания проверки. Мы были в полной их власти. Все, что могли предпринять наши сотрудники, — удалить любое упоминание о McAfee из собственных профилей. Те, кто был в курсе происходящего, так и сделали.

Но этого было недостаточно. Я продолжила портить другим пасхальное воскресенье — сообщила о происшествии команде руководителей. Мы позаботились о безопасности серверов компании, но это не означало, что McAfee не будет атакован в других социальных каналах. И, конечно, мы не знали, станут ли следующей мишенью злоумышленников наши руководители — или их профили в соцсетях.

Я разослала руководителям письма и сообщения с просьбой немедленно включить в личных профилях всех социальных сетей многофакторную аутентификацию (подробнее о ней — чуть позже).

Последовав собственному совету, я начала судорожно укреплять безопасность в личных профилях — пока одна очень популярная социальная сеть не завела меня в тупик. Не знаю, что это было: то ли мое тело полностью перешло в режим мобилизации «бей или беги» (когда организм перенаправляет кровоток к основным группам мышц, чтобы скрыться от угрозы или подготовиться к бою — иными словами, уводит подальше от мозга), то ли соцсети стоило сделать настройки безопасности более очевидными. Скорее всего, и то, и другое. Как бы там ни было, я запаниковала и прибегла к отчаянной мере: полностью удалила оттуда личный профиль — и всю его историю.

Час ожидания превратился в два, затем в три, а потом и в четыре. Я регулярно звонила генеральному директору с необходимыми, но раздражающими новостями об «униженном и оскорбленном» профиле нашей компании. Диалоги сводились к следующему:

— Крис, мы все еще работаем с ними. Они не завершили проверку безопасности. Надеемся, все закончится в течение получаса.

Как в том анекдоте про программиста: «намылить, смыть, повторить» — снова и снова, каждые полчаса.

Во время очередного звонка руководитель вытащил козырь из рукава.

— Эллисон, я устал ждать, пока они нами займутся. Я знаю кое-кого из владельцев этой соцсети. Звоню ему.

— Отлично, Крис. Мы пока продолжим подгонять службу поддержки.

Крис связался со своим знакомым и рассказал о нашем случае. Через 30 минут после звонка страницу восстановили в исходном виде. Доподлинно неизвестно, повлиял ли звонок Криса или они просто закончили проверку, но я знала, что теперь ситуация под контролем.

Утром понедельника мы выпустили статью в интранете, чтобы все сотрудники узнали о случившемся в выходные. Помните, я говорила про одну из важных ценностей McAfee — всеобъемлющую открытость и прозрачность? Мы были обязаны объяснить людям, что случилось, особенно учитывая, что публикация отвратительной картинки вместо лого нашей компании затронула их личные страницы. Быть открытым и честным в неловких ситуациях очень сложно, но совершенно необходимо, чтобы жить в соответствии с ценностями.

***

Я рассказала эту историю не только потому, что она интересная, и не для того, чтобы вы подумали: «О, лучше уж она, чем я!» В ней заключается краткое содержание всего, о чем пойдет речь в этой книге, потому я и начала с нее.

Чтобы вы почувствовали, как покупка этой книги начала оправдывать себя с первой же главы, я расскажу вам, как произошел взлом и что мы делали после. И самое главное — я опишу действия, которые вы можете предпринять *утром следующего рабочего дня*, чтобы с вами этого не случилось.

Наученные горьким опытом

Снова получив контроль над аккаунтом, мы попросили службу поддержки социальной сети назвать имя администратора, ответственного за изменения.

Оказалось, это была сотрудница одного из наших агентств по размещению в СМИ (назовем ее Джули), которая больше не работала в компании. Ее учетные данные были украдены подростком, связанным с

крупным киберпреступным синдикатом. Джули допустила ошибку, которую совершали многие до нее: проигнорировав правила цифровой гигиены, установила слишком простой пароль. Она использовала один и тот же код для доступа к нескольким учетным записям, включая профиль в этой социальной сети. И поскольку она была авторизованным администратором корпоративной страницы, ее личные учетные данные открывали доступ не только к ее профилю, но и к нашему. И когда злоумышленники взломали один из ее аккаунтов и продали данные в даркнет, хакеры просто опробовали этот пароль и в других социальных сетях. После этого они нанесли удар по корпоративной странице McAfee через административный доступ Джули. Остальное было детской забавой.

Задним умом мы все крепки, и этот случай — не исключение. Итак, уязвимость номер один: ***Джули использовала один пароль*** для своего личного и нашего корпоративного аккаунта на платформе соцсети (будучи одним из администраторов нашей страницы) — тот же, что и для других своих учетных записей. Если бы она вводила уникальные пароли, тогда данные, купленные злоумышленниками в даркнете, были бы бесполезны. Что хуже? Узнав о взломе аккаунта, Джули быстро сменила пароль. Но ей не удалось изменить его в других учетных записях, в том числе в важной для этой истории. Это ее вина.

Уязвимость номер два: ***мы должны были требовать двухфакторной аутентификации в социальных сетях от всех администраторов.*** Это означает, что для входа в систему им понадобилось бы ввести не только правильный пароль, но и одноразовый код, отправленный, например, на телефон. Если не ввести код в течение нескольких секунд или минут после попытки входа, вы не попадете в систему. Существует несколько версий этого типа аутентификации, и я, конечно, все упрощаю — но в целом все понятно. Это наша вина.

Уязвимость номер три: ***мы проводили проверку аккаунта недостаточно часто и не поняли вовремя, кому больше не нужен доступ***. Джули работала на нас, но мы должны были исключить ее из списка администраторов после окончания проекта. Нас могли взломать и пока она активно сотрудничала с нами, но отсутствие «гигиены» только усугубило ситуацию. Это точно на нашей совести.

Все эти действия могли значительно снизить вероятность взлома. Но, допустим, каким-то невероятным образом достаточно мотивированный, везучий и даровитый хакер смог проникнуть в нашу учетную запись в соцсети. Давайте разберемся, как превентивные меры помогли бы нам после обнаружения взлома.

Мы могли ***разработать процедуру блокировки действий всех администраторов страницы, не позволяющую хакерам узнать, что мы в курсе атаки.*** Удалением бессмысленных постов мы только привлекли их внимание. А когда они увидели, как мы закрываем доступ администраторам, они стали работать на опережение.

Нам повезло, что Гэвин оказался на взломанной странице в пасхальное воскресенье. В противном случае мы могли бы не узнать об атаке так быстро. Теперь у нас есть инструмент, который использует средства машинного обучения для обнаружения необычных изображений, ненормативной лексики, оскорблений и других аномальных материалов на страницах социальных сетей. Он *немедленно предупреждает* нескольких членов нашей команды о такой необычной активности.

Примечание. Я не буду называть конкретный инструмент по двум причинам. Во-первых, программы приходят и уходят, у каждой из них свой уровень эффективности и каждой из них — свое время. Иными словами, в период запуска инструмент может быть очень эффективным — до тех пор пока хакеры не найдут способ его обойти. Я не знаю, когда вы будете читать эту книгу, а потому не стану хвалить то, что, возможно, больше не использую.

Вторая причина, по которой я скрою название этого инструмента, заключается в том, что McAfee является важной мишенью для хакеров по всему миру. Оставляя их теряться в догадках, какие именно средства мы используем, мы помогаем снижать угрозу. Поискав описания инструментов в сети, вы быстро найдете то, что можно опробовать. Вернемся к урокам, которые мы вынесли.

Мы не были знакомы с протоколом действий службы поддержки соцсети в подобных ситуациях. И очень зря. Только постфактум мы узнали о том, что их политика требует блокировки аккаунта на много часов, вне зависимости от того, насколько велики изменения на странице. ***Теперь мы узнаем о подобных процедурах заранее*** — до размещения корпоративных страниц на других сайтах.

Мы на собственном горьком опыте убедились, как много значат деньги. Поскольку мы тратили приличную сумму на продвижение в социальной сети через агентства, самой платформе мы казались менее значимым аккаунтом, чем были на самом деле. Это могло повлиять на быстроту реакции. Теперь ***мы оплачиваем продвижение напрямую на платформах социальных сетей*** — чтобы наши инвестиции были на виду и приносили нам уровень сервиса, которого мы заслуживаем.

Кроме того, мы узнали, что ***сторонние компании, с которыми мы ведем бизнес, могут не иметь надежных методов обеспечения безопасности***. Это особенно важно, если это ваши филиалы или у них

есть доступ к вашим системам. В частности, у небольших сторонних компаний, с которыми вы поддерживаете отношения, может не быть подразделений ИТ и безопасности, не говоря уже о строгой политике киберзащиты.

И наконец, последний удар под дых. Как показало вскрытие, McAfee даже не был изначальной целью атаки. Когда хакер получил доступ к личным данным Джули, он понятия не имел о том, что она администратор корпоративной страницы компании. Он не знал, кто такая Джули: ему было все равно. Он просто охотился за паролями, стремился определить, к чему они откроют доступ, — к личному банковскому счету, сети компании или чему-то еще. Как только он нашел тот, который случайно подошел к странице McAfee в этой социальной сети, он вывалил на всех, кого мог, целый ушат оскорблений, унизив при этом компанию. *Даже для хакеров удача иногда важнее мастерства.*

Еще несколько важных уроков

Составьте список людей, с которыми вы можете связаться в такой ситуации. Держите их контакты под рукой — там, где вы и ваша команда легко сможете их найти. Эти списки должны быть не только у ваших людей, но и у сотрудников, обслуживающих сайт компании, ее социальные сети, облачное хранилище и так далее.

В чьи-то рабочие обязанности должна быть включена регулярная проверка доступа к аккаунту, а помимо этого — удаление из списка администраторов людей, чья работа больше не связана с текущими проектами.

Используйте многофакторную аутентификацию. Некоторые наши системы автоматически определяют, когда пользователи входят в них, а когда выходят — даже если выключение произошло всего на несколько минут, например, для смены компьютера. При работе в системах с меньшим уровнем прямого контроля — таких как облачные сервисы, например, — мы просим сотрудников присылать скриншоты, показывающие, что многофакторная аутентификация включена.

Можете себе представить, как тщательно мы теперь изучаем социальные сети, прежде чем разместить там свою страницу. В дополнение к мерам, описанным выше, мы задаем следующие вопросы:

- Как вы обрабатываете личную информацию?
- Какую технологию вы используете? (На основе ответов мы проводим оценку уязвимости).
- Как работает ваша система управления доступом?

- Какие сторонние инструменты можно подключить к вашей платформе, чтобы автоматизировать откат контента, необходимый после взлома?
- Каков алгоритм возвращения взломанного хакерами аккаунта под контроль?
- Какого соглашения об уровне реагирования на атаку и возвращения клиенту контента в том виде, каким он был до взлома, вы придерживаетесь?

Чья это вина?

Безусловно, провайдер социальной сети сможет доказать, что мы сами не сделали несколько очевидных шагов — не свели к минимуму количество администраторов, регулярно проверяя их список, не настояли на использовании уникальных надежных паролей и так далее. Но решению проблемы не способствовала и его жесткая политика, в рамках которой очевидно взломанная грубейшим образом страница должна была оставаться неизменной до окончания проверки. И, конечно, сотруднице агентства не стоило использовать одинаковый пароль для нескольких учетных записей.

Но обратите внимание: главу я назвала «Как *я* испортила Пасху». Нет, я не взламывала корпоративную страницу McAfee. Не я предоставила такую возможность злоумышленнику. И в то пасхальное воскресенье я *меньше всего* хотела разбираться с ситуацией, возникшей в результате цепи нелепых ошибок. С учетом всего сказанного я могу лишь взять на себя ответственность за все произошедшее. Ведь, в конце концов, эта корпоративная страница находилась в ведении моей команды. И мы не выполнили свой долг — не приняли разумных мер для ее сохранности.

Личная ответственность — вещь неприятная. Немногим из нас доставляет удовольствие обдумывать, что можно было сделать лучше или иначе для предотвращения несчастного случая. Уклонение — гораздо более нормальная человеческая реакция. Тем не менее именно наша тяга к отказу от личной ответственности остается ключевым оружием в арсенале хакерского сообщества.

Слишком долго кибербезопасность была «чьей-то там» проблемой. Слишком многие считают кибербезопасность мутной темой, не заслуживающей их личного времени, не говоря уже об ответственности. Эта книга ставит целью изменить данную парадигму, хотя бы помочь сделать скромный шаг к признанию ответственности, которую мы все разделяем как сотрудники — и, в конечном итоге, защитники — наших организаций. Если наша компания не может рассчитывать, что мы примем разумные меры предосторожности, чтобы уберечь ее драгоценные цифровые активы, то кому она вообще может доверять?

Однако позвольте мне отвлечься от своей «мелодрамы» и обозначить настоящую проблему. Дело не в том, что сотрудники в большинстве своем *не хотят* поступать правильно. Гораздо чаще они просто не знают, *как* это делать.

Кибербезопасность — это командный спорт, в котором каждый должен играть на своей позиции в любую минуту. Дополнительные инструменты могут быть чрезвычайно полезными; но только когда люди, программы, процедуры, регулярные проверки и другие факторы работают вместе, они образуют эффективную защиту.

Помните о важном факторе

Еще один важный элемент, позволяющий минимизировать киберугрозу, — честность. Я определенно выхожу из зоны комфорта, начиная книгу со своим именем на обложке с описания досадного сбоя в системе безопасности, произошедшего у меня под носом. Могло ли быть хуже? Конечно. Этого никогда не должно было произойти? Конечно.

Могли ли вы оказаться на моем месте? И снова — конечно.

Рассказывая эту историю, я хочу задать тон честности, который необходим и в вашем бизнесе, нацеленном на сопротивление плохим парням. Вам необходимо развить культуру безопасности, которая позволит людям не только помогать друг другу, но и быть взаимно честными при обнаружении подозрительных действий. И честность эта — без гнева, обвинений или возмездия — позволит культуре работать.

Кроме того, я описываю взлом нашей страницы, чтобы вы сразу учли наши уроки и применили полученные знания, чтобы устранить щели в броне вашей безопасности.

Почему я?

На рынке не наблюдается недостатка в книгах по кибербезопасности от заслуживающих доверия талантливых авторов с самым разным опытом. Вы можете прочитать расследования журналистов, проанализировавших самые знаменитые взломы в истории. Можете ознакомиться с авторитетным мнением корифеев — основателей отрасли. Еще больше информации вы найдете у технических экспертов, которые весьма подробно разбирают сложные элементы кибербезопасности.

Однако же в то время, когда я это печатаю, найдется крайне мало книг по кибербезопасности, написанных маркетологами. А уж маркетологами, проработавшими в сфере всего несколько лет, — и того меньше. Так зачем доверять такому автору в столь серьезном вопросе?

Считайте мою книгу чем-то вроде гибрида маркетинга и технологий. Всю свою карьеру я переводила технические концепции на обычный язык. Я изучала взаимодействие работы и технологий, чтобы понять, как меняется корпоративная культура.

Так что если вы в целом не разбираетесь в технологиях, будьте уверены: моя цель — дать вам достаточно знаний для понимания нюансов этой сложной темы, не загружая техническими деталями. Но если вы технологически подкованнее меня, уверяю: я не собираюсь все упрощать. Просто предложу рецепты, которые каждый сотрудник — как технический, так и любой другой — может применить для защиты своей организации. И, наконец, если вы один из моих собратьев по кибербезопасности, надеюсь, вы с удовольствием прочитаете эту книгу, восприняв ее как возможность дать другим заглянуть в наш мир. А после — передадите коллегам, не связанным с киберзащитой, чтобы они тоже вступили в наши ряды борцов за безопасность.

Почему вы?

Вы можете считать себя человеком, которому нечего привнести в сферу киберзащиты. В конце концов, как могут сотрудники, менеджеры, руководители и члены совета директоров, работа которых не связана с данной сферой, сыграть значимую роль в игре, правил которой, возможно, даже не понимают?

И здесь я обращусь за вдохновением к миру профессионального спорта — он дает нам много примеров успеха командной работы. Я не фанат спорта, но питаю слабость к американскому футболу. У меня остались очень теплые воспоминания из раннего детства: мы с отцом сидим на диване в гостиной и смотрим игру его любимой команды Dallas Cowboys.

Как и миллионы других болельщиков, в мире профессионального спорта я всего лишь зритель. Просмотр игры — это самое короткое расстояние, на которое большинство из нас может к ней приблизиться. Зрители практически не влияют на исход игры. Эта роль возложена на гораздо более важные персоны — спортсменов и тренеров, — чьи талант, упорство и командная работа в конечном счете определяют, одержат ли они победу.

Раньше я верила в это. Но потом узнала о 12-м игроке Seattle Seahawks — американской профессиональной футбольной команды. Во время любого матча на поле выходят по 11 футболистов от каждой команды. Но Seahawks признают 12-го игрока — не менее важную толпу зрителей.

Со временем я поняла, что мы с папой не желали встречи наших «ковбоев» с Seattle Seahawks на их поле. На их стадионе соперников не ожидает теплый прием. Уровень шума, создаваемый «двенадцатым игроком» команды, всего на пару децибел ниже, чем на летной палубе авианосца. И, как оказалось, поддержка зрителей существенно повлияла на исход нескольких игр. За три сезона Seahawks на своем поле одержали 26 побед против двух поражений. «Двенадцатый игрок» дважды установил мировой рекорд по шуму, создаваемому толпой, и даже спровоцировал как минимум одно небольшое землетрясение.

Эта заслуженная футбольная команда знает, насколько важны зрители. 15 декабря 1984 года из уважения к своим болельщикам они изъяли из обращения 12-й номер. Гигантский флагшток с цифрой 12 гордо реет над их стадионом. А когда команда вышла на поле перед игрой в Супербоуле, шествие возглавлял человек с флагом — также с изображением заветного числа.

Неужели «12» (как называют фанатов Seahawks) действительно такие громкие? В целом — да. Но оказалось, что их стадион был специально спроектирован так, чтобы усиливать шум. В отличие от других полей под открытым небом, где шум рассеивается естественным образом, на стадионе Seahawks есть своего рода вторая палуба и навес, которые направляют шум вниз, создавая какофонию, когда болельщики кричат [1]. Руководство команды приложило немало усилий, чтобы сделать «двенадцатого игрока» полноправным участником матчей и прибавить его коллективную мощь к своей.

История о двенадцатом игроке учит нас тому, что зрители могут влиять на исход. Но для этого их нужно вовлекать. Они должны быть полноправными участниками происходящего. И вот теперь — ваш выход. Я написала эту книгу, чтобы каждый осознал важность собственного участия в непрекращающемся соревновании за кибербезопасность. Никто не обвинит вас в том, что вы не надели форму раньше. Но после прочтения этой книги никто не сможет оправдать вашего отказа от ответственности.

В этой книге я хочу продолжить диалог с того места, на котором заканчивалось так много других текстов: дать новичкам в сфере бизнеса план действий, который они могут немедленно воплотить в жизнь, чтобы стать частью борьбы за кибербезопасность. Если вы все еще сомневаетесь, стоит ли вступать в битву, знайте: вы уже в ней. Киберпреступники надеются на равнодушие и отстраненность сотрудников — так им будет проще наносить удары. Если вы не активный игрок, выступающий за свою компанию, вероятно, вы пешка в руках врага. Если вы цените онлайн-свободу, если вам важно, чтобы данные, которые вы используете для принятия решений, не были

скомпрометированы, если хотите, чтобы ваши девайсы использовались во благо, а не во вред, то вы уже разделяете миссию профессионалов сферы кибербезопасности. У вас больше общего с нами, чем вы могли себе представить.

W.I.S.D.O.M.

Руководство McAfee серьезно относится к развитию. Каждый квартал мы собираемся вместе, чтобы снова и снова превращать просто «работу» в «командную работу». Мы учимся у коллег, делимся личными историями о наших профессиональных буднях и даем обещание быть более искренними друг с другом и с нашими сотрудниками. В конце этих встреч мы практикуем инструмент W.I.S.D.O.M. (аббревиатура, складывающаяся в англ. слово «мудрость» — Прим. пер.), о котором узнали от группы компаний AIP, нашего партнера по развитию лидерства. Расшифровывается аббревиатура так: **W**hat **I**'ll **S**ay (and do) **D**ifferently **O**n **M**onday — «Что я скажу (и сделаю) иначе в понедельник». Каждый из нас берет на себя обязательство проработать одну из ключевых областей развития, которые мы обсудили.

Позвольте мне и вас вооружить такой же «мудростью». В конце каждой главы вы найдете советы о том, что можете сделать в понедельник для повышения уровня кибербезопасности вашей организации. Некоторые из них на первый взгляд очевидны, но могут существенно повлиять на ваш успех. Другие потребуют больше работы, но, скажем так: вид стоит того, чтобы забраться на гору. Советов каждый раз будет не более пяти, так как я верю: 20% усилий дают 80% результатов.

Рекомендации, которые вы найдете на этих страницах, можно применить на очень широком спектре предприятий. McAfee обслуживает сотни миллионов потребителей по всему миру. Мы работаем с крупнейшими правительственными и корпоративными организациями. Наши решения защищают и задние дворы, и залы заседаний. Мы действительно вас понимаем.

Использовать советы смогут люди, занимающие различные позиции, — от членов совета директоров крупных компаний до рядовых сотрудников. Кибербезопасность слишком важна, чтобы оставлять ее в ведении специалистов узкого технического профиля. Каждый сотрудник, каждое заинтересованное лицо играет свою роль. Эта книга содержит основы, которые помогут вам применить те или иные техники в организации.

Готовясь к выпуску этой книги, в 2017 году McAfee проинтервьюировала 50 руководителей с различным функционалом (включая генеральных директоров, финансовых директоров, ИТ-директоров, директоров по маркетингу и т.д.), — чтобы проверить уровень кибербезопасности их подразделений. Для этой же цели мы провели этнографическое онлайн-исследование, в котором приняли участие 69 сотрудников компаний (можете считать это своеобразной онлайн-фокус-группой). Мы задавали им вопросы, а также давали упражнения, которые подразумевали сотрудничество на протяжении нескольких дней. В начале каждой главы приведены цитаты этих респондентов, которые помогут более четко сформулировать тему обсуждения и рекомендации.

Вы, «двенадцатый игрок», нужны нам в битве. Вы можете определить ее исход. Эта книга научит вас играть, а также снабдит инструментами и советами — чтобы вы знали, когда кричать с трибуны надо еще громче. Стоит вам вступить в бой, и враг узнает: дом, в который он вошел, легко не сдастся. Мы будем снова и снова сражаться в битве, которую просто не можем позволить себе проиграть.

А теперь давайте зачислим вас в состав.

Глава 2

Мистер/миссис Целлофан

Очень простая аналогия, которую я использую, говоря о кибербезопасности и защите с советом директоров, — это бейсбольный матч. Мне нужно провести идеальную игру. Противникам же достаточно и одного сингла. Причем даже необязательно, чтобы к вам пробрался какой-то негодяй. Достаточно, чтобы кто-то просто пропустил один шаг при настройке сервера. Реальность в кибербезопасности такова, что, если вы на стороне защиты, вам нужно каждую игру проводить идеально. А этого не будет.

Старший/исполнительный вице-президент компании, работающей в сфере услуг

Бедняга Эймос. Его жена хладнокровно убивает своего любовника и заявляет, что защищалась от человека, которого называет «неизвестным» взломщиком. Эймос покорно остается рядом с ней, даже узнав уродливую правду об их романе. Куда бы ни отправился Эймос, он — всего лишь тень на фоне жуткой истории своей жены; никто вокруг его не замечает.

Я говорю о персонаже знаменитого мюзикла «Чикаго». Эймос сетует на то, что его не замечают, в сольном номере под метким названием «Мистер Целлофан»:

«А в общем, чтоб друг друга замечать,
Совсем необязательно кричать,
Но не заметят и при свете дня
Невзрачного, прозрачного меня.
Целлофан, мистер Целлофан,
Я б назвался сам мистер Целлофан.
По мне проводят взглядом,
Ходят рядом,
Не увидав меня».

Многие из нас могут разделить чувство Эймоса, что нас не замечают. Чувство не из приятных и сопровождается обычно ощущением, что нас недооценивают и не признают. И уж совсем невесело, когда тебя неправильно понимают.

Слишком долго руководители по информационной безопасности оставались в наших организациях этакими мистерами и миссис Целлофан, обреченными трудиться в условиях виртуальной анонимности и постоянно сосредоточенными на том, чтобы с честью исполнять свой долг по обеспечению безопасности. Они живут в тени тех, кого защищают. Более того, если они сбросят свою мантию невидимости, проблемы неизбежно возникнут с обеих сторон.

Как сотрудники, мы не желаем, чтобы нас беспокоили директора по ИБ или их отделы. Мы рассчитываем лишь на защиту с их стороны. Фактически они существуют где-то на задворках наших организаций, где их буквально не видно и не слышно. Если они осмеливаются появиться в поле нашего зрения со своими надоедливыми обновлениями системы безопасности, которые замедляют работу, мы начинаем жаловаться. Еще хуже, если они пытаются отключить доступ к нашим излюбленным службам или устройствам: мы просто найдем способ обойти их запрет.

Наглядный пример: по данным McAfee, в среднестатистической организации в любой момент времени используется порядка 2000 облачных сервисов. А сколько их, по мнению ИТ-подразделения? Ближе к 30 [2]. В образовании этой пропасти между представлением и реальностью можно хотя бы отчасти винить теневые ИТ — феномен, при котором сотрудники бесчинствуют и используют облачные сервисы без ведома и уж тем более без разрешения своего ИТ-отдела.

Что может быть хуже для директора по ИБ, чем стать видимым для сотрудников? Стать таковым для правления. Исторически сложилось, что руководители так же мало хотят связываться с кибербезопасностью, как и сотрудники. Если правление приглашало директора по ИБ на встречу, то обычно не для того, чтобы узнать стратегически важные новости о ситуации с кибербезопасностью в компании или сердечно

отблагодарить его за работу. Скорее всего, его вызывали затем, чтобы задать сложные вопросы о взломе системы.

Deloitte [3], глобальная сеть компаний, предлагающих услуги в сфере аудита и консалтинга, регулярно проводит исследования, в ходе которых опрашивает первых лиц сотен публичных компаний. Так, выяснилось, что в 2014 году лишь в 5% крупнейших компаний при совете директоров функционировали комитеты, занимавшиеся объединенными вопросами «кибербезопасности и ИТ» [4].

Итак, в нашем метафорическом мюзикле руководитель по информационной безопасности во многом принял на себя роль Эймоса — он посвятил себя защите тех, кто этого совсем не ценит, и обречен оставаться в тени.

Однако преступники со своими злыми намерениями взялись переписать этот мюзикл. Не проходит и дня, чтобы газетные заголовки (или компании) не объявили об очередном взломе. Настроение первых лиц меняется. Многие осознают, что рискуют, уводя директора по ИБ в тень. Когда в 2016 году Deloitte повторили свое исследование, по уровню внимания от высшего руководства кибербезопасность поднялась до проблемы номер один, при этом 25% компаний в течение последних двух лет столкнулись со взломами [5]. Мистер и миссис Целлофан были освобождены из заточения в самом темном углу самого дальнего офиса и даже время от времени получают приглашения посетить заседание совета директоров.

Однако тот факт, что благодаря хакерам на директоров по ИБ обратили внимание, не решает проблему кибербезопасности. Отрадно наблюдать, что главные лица компаний держат вопрос под контролем, но просто принять проблему — это лишь первый шаг. Чтобы повысить уровень кибербезопасности компании, эти стороны — техническая (директор по ИБ) и стратегическая (управленцы) — должны научиться понимать друг друга.

Давайте в первую очередь попытаемся понять роль директора по ИБ, которая, по моему мнению, из всех высших должностей трактуется наименее корректно. Это пойдет на пользу не только первым лицам компании, но и всем ее сотрудникам. Директора по информационной безопасности, в свою очередь, наконец выберутся из тени.

Новенький

Корпорации, как и включающие их функциональные дисциплины, существуют уже сотни лет. Одними из самых ранних корпораций стали банки и мануфактуры, а значит, нет ничего удивительного в том, что многие из крупнейших на сегодняшний день публичных компаний

обладают обширными познаниями в финансах и операционной деятельности — исходных дисциплинах, ставших основой основ для наших корпоративных предков.

И действительно, согласно отчету Deloitte о практике советов директоров, по состоянию на 2016 год среди первых лиц, которые с наибольшей вероятностью регулярно посещали заседания правления, помимо генеральных директоров и главных юристов были финансовые директора (отмеченные примерно в 99% опрошенных компаний) и главы подразделений (до 47%). А как же директора по информационной безопасности? Для сравнения, они регулярно присутствовали на заседаниях на высшем уровне лишь в 11% опрошенных компаний [6].

Никого не должно удивлять, что директора по ИБ только прокладывают себе дорогу на эти закрытые мероприятия. В конце концов, если учесть, что другие функциональные дисциплины существуют уже столетия, если не тысячелетия (так, юристы могут утверждать, что их функциональные корни уходят аж во времена Древнего Египта), то роль специалиста по информационной безопасности насчитывает всего какие-то десятилетия. В те времена мы даже не называли это киберзащитой. Ее пионеры обозначали сферу своей деятельности как «информационную безопасность», зародившуюся внутри информационных технологий.

Нам крайне важно совершить короткое, но важное путешествие к истокам кибербезопасности, чтобы понять сравнительно новую роль директора по ИБ. В свое время безопасность информационная и физическая были в широком смысле одним и тем же. Помню (не так уж и давно это было), если мне нужно было получить доступ к сети компании, я делала это через стационарный компьютер, подключенный к Ethernet-кабелю, выводившему меня в локальную сеть. Как сам компьютер, так и технология Ethernet — все это располагалось в помещениях компании. А значит, единственным способом получить доступ к корпоративной сети было физически войти на территорию самой фирмы, что, в свою очередь, требовало наличия определенного уровня допуска — вроде моего бейджа. Физическая и информационная безопасность были для меня неделимы — как в мыслях, так и на практике.

Меня поражает, как сильно все изменилось, и только на моем веку. Работа перестала быть местом, куда я хожу; она стала именно занятием. Я все больше работаю за пределами безопасного, физически ограниченного периметра, принадлежащего компании. Я органично совмещаю профессиональную жизнь с личной — отвечаю на электронные письма с мобильного устройства, выхожу на связь практически из любого места, где можно найти Wi-Fi, и получаю доступ

к бесчисленному множеству облачных сервисов, которые облегчают мне жизнь.

И я не единственная, кто считает, что работа во многом стала «беспроводной». Давайте рассмотрим, как наши относительно новые рабочие привычки оказывают несравненно большее, чем раньше, давление на руководителей по ИБ, защищающих нас и наши компании. В любой момент времени наш директор предпринимает как минимум одно из трех стратегических усилий:

1. Преобразования

Любое внедрение технологии, будь то мобильность, облако или интернет вещей, подвергает компанию все большему риску. Дело в том, что в процессе нововведений безопасный периметр предприятия продолжает разрушаться.

Приведем пример: кому принадлежит интернет? Это запутанный лабиринт такой сложности, от которой и у самых технически подкованных из нас головы пойдут кругом.

Кому принадлежит инфраструктура облачных хранилищ вроде тех, что предоставляют Amazon, Google и Microsoft? На этот вопрос ответить уже легче: за физическую безопасность облачной среды отвечает компания, ее предоставляющая. Однако это равносильно утверждению, что в их власти и обеспечение физического доступа к огромным дата-центрам — примерно в том же смысле, что и наши компании обеспечивают защиту зданий, где мы работаем. Кража данных из облачных хранилищ обычно не является результатом физического взлома дата-центров крупнейших интернет-компаний изобретательными ворами: киберпреступники получают доступ к данным, хранящимся в вышеупомянутых дата-центрах или проходящим через них.

На ком же в конечном счете лежит ответственность за эти данные? Это самый однозначный и самый простой вопрос: ваша компания — и только она — несет ответственность за сохранность собственных данных, и неважно, где они хранятся — хоть на серверах, находящихся на территории, принадлежащей вашему работодателю, хоть на тех, что арендуются на общедоступном облаке.

Облако — лишь один из примеров убывающего контроля специалиста по информационной безопасности над инфраструктурой, используемой для хранения или передачи данных его компании. Концепция использования сотрудниками собственных устройств прочно обосновалась в бизнес-сфере, а значит, корпоративные мобильные устройства могут скоро стать пережитками прошлого. Есть

весомая причина, по которой в столь многих компаниях не задумываясь позволяют своим сотрудникам по желанию работать на любом устройстве (или нескольких). Согласно данным Frost & Sullivan, использование смартфонов в рабочих целях позволяет сотрудникам сэкономить в день почти час; при этом их эффективность вырастает на 34% [7].

У старых технологий очень длительный срок годности, что только усложняет внедрение преобразований. Даже при том, что бизнес-подразделения спешат развернуть облачные сервисы (с формального согласия ИТ-отдела или без оного), за ними все равно тянется длинный хвост локальной инфраструктуры, которую необходимо поддерживать. В качестве примера рассмотрим USB-накопители. В 2017 году исследователи из Университета имени Бен-Гуриона документально зафиксировали 29 известных векторов атаки, компрометирующих USB-накопители [8]. А компания Apricorn, производитель USB-накопителей без программного обеспечения с аппаратным шифрованием, в 2017 году сообщила: из 90% сотрудников, использующих USB, только 20% делают это с шифрованием [9].

Поскольку унаследованная технология редко исчезает полностью и никогда — быстро, все эти попытки преобразований влекут за собой рискованное расширение зоны охвата и ответственности.

Что же остается делать нашему директору по ИБ? Легкомысленно поддержав среду всеобщего доступа и вседозволенности, он оставит свою организацию незащищенной от возрастающих рисков. Став отделом «Нет», чтобы сдержать возможную угрозу, — скорее всего, лишится поддержки среди тех самых сотрудников, которых должен оберегать (вы же помните о тех 2000 облачных сервисов, которые в среднестатистической компании используют без ведома ИТ-специалистов?).

Директор по ИБ оказывается в незавидном положении. Он должен одновременно защищать самые ценные цифровые активы своей компании и способствовать ее преобразованию. К сожалению, более противоречащие друг другу задачи и придумать сложно.

2. Управление рисками

Киберпреступления — огромный бизнес: если быть точным, то в 2017 году его оборот составил $600 млрд, что на $100 млрд больше, чем в 2014-м [10]. С точки зрения глобальных последствий киберпреступность — третье по важности экономическое бедствие после коррупции во власти и наркотиков.

Как же мы дошли до этого? Еще живы в памяти времена, когда киберзащита была относительно «проста». Как уже говорилось, информационная безопасность обеспечивалась физической, да и справляться с угрозами тогда было несравнимо легче. В 2006 году McAfee обнаруживал в день по 25 новых угроз. Через 10 лет эта цифра подскочила до 500 000 — более пяти новых угроз в секунду!

И масштаб — это лишь часть проблемы. Раньше обнаруживать угрозы было достаточно просто. Они исходили от вредоносного ПО — программных средств, разработанных плохими парнями, намеревавшимися навредить своим жертвам. «Традиционные» вредоносные программы включали в том числе противные вирусы, которые все вы давно знаете и ненавидите. Когда-то у вредоносного ПО была заранее известная длина строки, что и позволяло определять его как вредоносное. Это сигнатура — своего рода программный отпечаток пальца. Если полиция при поиске преступника обращается к национальной базе данных, содержащей отпечатки пальцев, то специалисты по кибербезопасности заносят сигнатуры вредоносных программ в собственные базы. Если в файле обнаруживаются характерные признаки атаки, он блокируется, а угроза устраняется.

Как же изменились времена! Самые коварные угрозы перестали быть явными: они больше не оставляют хорошо известный и легко распознаваемый отпечаток пальца. Преступники стали куда умнее. Когда вы возьмете в руки эту книгу, она почти наверняка не будет содержать указаний на новейшие киберугрозы; сейчас же, когда я пишу эти строки, моя индустрия сосредоточена на «бесфайловых» атаках. Они используют доверенные технологии внутри вашей организации, например санкционированные инструменты и приложения, а затем наносят вред: обычно это получение доступа к крупномасштабной сети вашей компании и похищение ее данных.

Я говорю «обычно», так как кража данных более не является единственной целью онлайн-преступников. Вирусы-вымогатели — еще одна злободневная тема: здесь злоумышленники даже не утруждают себя кражей данных, чтобы продать их в даркнете. Они значительно сокращают свой путь к прибыли, блокируя (или шифруя) файлы своей жертвы и требуя выкуп за ключ (или дешифрование), прежде чем окончательно их уничтожить.

Данные и деньги могут и не являться конечной целью злоумышленника. Он может быть более склонен сеять хаос, перекрывая доступ к критически важным системам своей жертвы, ставя при этом всю компанию на колени. Или же хакеры могут вести информационную войну, когда сами данные становятся орудием для создания хаоса: просто задумайтесь об объемах данных, которые каждый день

генерирует ваша компания, и о том, какой значительный вред могут нанести малейшие манипуляции с ними вашему работодателю. Или, возможно, цель хакера — репутация вашей компании, в чем McAfee удостоверились на собственном горьком опыте при взломе нашей страницы в соцсети.

Вы понимаете, о чем я. Угрозы становятся не только во много раз опаснее, но и значительно сложнее и коварнее. А их масштаб, разнообразие и сила дополнительно повышают риск.

Как же можно ожидать, что директора по ИБ объяснят хитросплетения этой реальности первым лицам своих компаний, которые, по данным Deloitte, собираются не чаще шести раз в год в среднем на четыре часа? Это значит, что среднестатистический совет директоров располагает всего 24 часами в год, чтобы обсудить темы от стратегии компании и ее финансовых показателей до деликатных вопросов слияния и поглощения. Стоит ли удивляться, что кибербезопасности с ее сложной и высокотехнологичной природой на советах директоров уделяют крайне мало внимания?

Но так быть не должно. Кибербезопасность — тема действительно сугубо техническая. Но при этом по сути своей она крайне проста. Речь здесь в основном идет об управлении рисками — а этим языком большинство членов советов директоров владеют в совершенстве.

Вопросы снижения рисков для директоров по ИБ можно сравнить с ходьбой по канату. Им нужно поддерживать баланс между противодействием масштабным угрозам, которые, вероятнее всего, не приведут к катастрофическим последствиям, и незначительным по объему, но нацеленным атакам, которые могут потопить компанию.

Все мы, как члены правления, так и остальные сотрудники, можем понять директоров по ИБ в том, что касается управления рисками, ведь и сами балансируем на этой тонкой грани. У себя в ванной мы стелим коврики, снижающие риск падений (что является относительно небольшой угрозой для большинства людей моложе определенного возраста). В домах устанавливаем датчики дыма и покупаем страховку, чтобы избежать более серьезных рисков вроде пожара. И хотя в нашей жизни может произойти и нечто поистине катастрофическое — скажем, обрушится метеорит (что действительно произошло с одним бедолагой в 1954 году [11]), — мы спокойно игнорируем подобные риски, учитывая их бесконечно малую вероятность.

Примерно так же классифицировать риски для своих компаний должны и директора по ИБ. Их задача — упростить тему для подачи высшему руководству, не делая ее при этом примитивной. В чем же состоит задача членов совета директоров? Погрузиться в обсуждение, понять, что скрытая бездна проблем вряд ли предусматривает

однозначное решение. Война не располагает к ясности. То же касается и кибербезопасности.

3. Автоматизация и эффективность

«Делать больше при меньших затратах» — это раздражающее клише современного предприятия. А кроме того, это нелегкая обязанность директора по ИБ. Мало того, что масштаб угроз и не собирается снижаться, так еще и спрос на специалистов по кибербезопасности намного превышает предложение на рынке труда. По данным Cybersecurity Ventures, к 2021 году в сфере кибербезопасности будет более 3,5 млн незакрытых вакансий [12] — такого количества людей хватит, чтобы заполнить 50 арен Национальной футбольной лиги!

И проблема лишь усугубляется. В 2014 году было подсчитано, что в сфере кибербезопасности не хватает одного миллиона профессионалов по всему миру. К 2015 году показатель вырос до полутора миллионов вакансий. В 2016-м аналитики предполагали, что к 2019 году нехватка специалистов по кибербезопасности составит 2 млн специалистов [13]. Угрозы продолжают расти, а вместе с ними и потребность в квалифицированных профессионалах.

Не располагая достаточным количеством людей, которых можно было бы бросить на решение проблемы, директора по ИБ могут обратиться к множеству продуктов, предоставляемых огромным батальоном поставщиков услуг по кибербезопасности. Программных продуктов, соперничающих за ограниченный бюджет, которым располагает директор по ИБ, существует в избытке, что резко контрастирует с ситуацией на рынке труда. На момент написания этих строк директоров по ИБ осаждали порядка 3500 поставщиков услуг в области кибербезопасности [14]. Каждый поставщик предлагал как минимум одну технологию для защиты от угроз, обещая решить небольшую (а то и большую) часть проблем с кибербезопасностью.

Но порой перебор хорошего — это плохо, и слишком большой выбор технологий кибербезопасности прекрасно иллюстрирует эту аксиому. Директора по ИБ в попытках предвосхитить следующую угрозу традиционно спешат с внедрением новейших защитных технологий.

Однако тут они попадают в невыгодное положение. Дело в том, что разрозненные поставщики, конкурирующие за каждый доллар, открывают перед ними темный омут технологий, по большей части плохо сочетающихся друг с другом. Слишком часто случается, что эти технологии продвигают, приобретают, а затем откладывают на полку. Бюджеты тратятся, «полочное» ПО множится, и компании больше не

могут быть уверены в оправданности своих инвестиций в разного рода инициативы и инновации. Даже если технология будет «снята с полки» и внедрена на практике, велика вероятность, что ее не удастся совместить с остальными защитными системами компании.

Представьте, что отправляетесь на войну, а в вооружении у вас царит хаос. Представьте, как непоследовательно применяете оружие против врага, прикрывая свои тылы. А теперь добавьте к этой картине тот факт, что ваши бойцы не могут общаться между собой и делиться информацией об угрозах, с которыми сталкиваются, чтобы совместными силами укрепить вашу организованную оборону.

Скорее всего, вам ничего и не придется выдумывать. Просто посетите свой центр мониторинга информационной безопасности, если у компании таковой имеется, где ваши коллеги, отвечающие за кибербезопасность, первыми реагируют на бесконечные атаки. Этим профессионалам, сражающимся на передовой, часто достается в наследство целый клубок технологий и инструментов, приобретенных за многие годы и чаще всего при разных директорах по ИБ. Многие из этих продуктов не передают информацию об угрозах, не говоря уж о том, чтобы хоть чуть-чуть облегчать жизнь специалистам по киберзащите. Слишком уж часто на поверку выходит, что это ваши коллеги из кибербезопасности работают на свои инструменты, а не наоборот.

Enterprise Strategy Group (ESG), независимые аналитики, изучающие рынок ИБ, сообщают, что в 40% организаций развернуто более 25 инструментов кибербезопасности. Примерно такой же процент компаний признают, что собирают «разведданные» вручную. А 27% считают, что команда, отвечающая за безопасность, большинство времени проводит, «туша пожары», а не работая над стратегическими проектами [15], что приводит к выгоранию и текучести персонала — катастрофическим последствиям для директора по ИБ в условиях глобальной нехватки кадров.

Мало того, у индустрии кибербезопасности есть секрет, от которого никуда не деться: ни один продукт не способен победить киберпреступность. Может, вас это и не удивляет. В противном случае это означало бы, что в войну можно вступать, имея в арсенале всего одно оружие.

Но и это еще не все. Дело не только в том, что пресловутой магической защиты, способной отразить все угрозы, не существует. Любая защитная технология наиболее эффективна тогда, когда только появляется на рынке. И это полностью противоречит общепринятой в ИТ точке зрения.

Задумайтесь об этом. Когда на рынке появляется новая технология, большинство компаний не отваживаются быть первопроходцами в ее внедрении. В конце концов, зачем становиться подопытным кроликом, когда новшество еще не проверено? Пусть первыми начнут другие, устранят ошибки, улучшат (и удешевят) технологию. И только после этого можно поспешить с ее применением. Это выглядит гораздо более разумной схемой внедрения обычных технологий.

Однако технология кибербезопасности в корне отличается от описанных выше. Когда ИТ-организация внедряет новейшую технологию, призванную заполнить пробелы, на другой стороне нет противника, предпринимающего активные действия против ее успеха. С кибербезопасностью все обстоит не так. Когда значительная доля компаний на рынке внедряет защитную технологию, показавшую высокую эффективность в борьбе с угрозами, злоумышленники снова запираются у себя в лабораториях, чтобы разработать контрмеры. В конце концов они находят способ обойти защитную технологию, если не ослабить ее. (Именно в этот момент поставщики услуг по кибербезопасности, такие как McAfee, запираются у себя в лабораториях и разрабатывают контрмеры против их контрмер, и гонка продолжается.)

В кибербезопасности время на вес золота. Особенно важно выйти на рынок с новой защитной технологией как можно раньше, ведь максимум эффективности она обеспечит именно первым пользователям.

Итак, давайте попробуем рассуждать как директор по ИБ:

1. Не существует одной защитной технологии, способной отразить все виды кибератак: их слишком много, и злоумышленники каждый день придумывают что-то новое. Чтобы обеспечить наилучшую защиту, вам придется использовать множество продуктов от разных поставщиков.
2. Каждая защитная технология показывает наибольшую эффективность, когда только появляется на рынке. Иными словами, вам лучше одним из первых внедрять новейшие технологии кибербезопасности, так как на ранней стадии у злоумышленников пока не было стимула или времени разработать план действий против нее. Когда они сделают это, между поставщиками услуг по кибербезопасности и злоумышленниками начнется игра в кошки-мышки, в которой каждая сторона будет разрабатывать новые способы противодействовать противнику.
3. Итак, важно быть первым, кто начнет действовать. Но вы (как и вся отрасль) страдаете от недостатка талантов, и для быстрого внедрения защитных технологий вашей команде элементарно не хватает людей. Даже если вам это удастся, велика вероятность, что вы не развернете эти средства скоординированно, таким образом, чтобы все технологии в вашей системе функционировали слаженно, обеспечивая обмен информацией об угрозах и работу с совместимыми программными средствами.

4. Поскольку ваши защитные технологии не обеспечивают эффективного обмена данных об угрозах, вашей малочисленной команде, отвечающей за кибербезопасность, остается лишь заполнять бреши. Учитывая, что и объем, и сложность угроз резко возрастают, ваша команда должна распознать сигнал среди шума, обнаружив и устранив самые коварные угрозы — и не дав соперникам опередить вас и нанести вред компании.

Кто готов вступить в такую схватку? Немногие. Вот почему профессионалы в сфере кибербезопасности на самом деле являются невоспетыми героями наших компаний. Они сражаются за нас, оставаясь в тени, невидимые и в значительной степени недооцененные, с учетом всех их стараний.

Вернемся к нашему директору по ИБ: «делать больше с меньшими затратами» для него — не просто фигура речи. Это необходимость. Ему нужно найти способ автоматизировать как можно бóльшую часть рабочих процессов, чтобы позволить своему самому скудному и ценному ресурсу — сотрудникам — сосредоточиться на охоте за наиболее изощренными атаками. Кроме того, ему нужно настойчиво внедрять новые технологии киберзащиты, не ставя при этом под угрозу свои средства обеспечения безопасности неинтегрированными решениями.

Теперь вы понимаете, с чем приходится сталкиваться вашему директору по ИБ, и можете поставить себя на его место:

- Вы способствуете трансформации своей компании, защищая расширяющуюся область, по которой можно нанести удар — облачные, мобильные технологии и приложения интернета вещей.
- Вы управляете рисками своей компании в условиях стремительного роста масштабов и изощренности угроз.
- Вы повышаете эффективность, внедряя продукты сразу после их появления на рынке и встраивая их в единую систему защиты. Кроме того, вы автоматизируете рабочие процессы, чтобы высвободить потенциал вашего самого дефицитного ресурса — талантливых сотрудников — для прицельной работы с самыми сложными и опасными угрозами.

W.I.S.D.O.M. для генерального директора и правления

Все, кто читают эту книгу, являются либо частью проблемы кибербезопасности компании, либо — частью ее решения. Генеральный директор и члены правления — не исключение. Есть множество способов наконец заметить среди нас мистеров и миссис Целлофан,

отдать им должное и оказать поддержку, которую они по праву заслуживают.

Во-первых, кибербезопасность не должна быть темой, поднимающейся на совете директоров по случаю или нерегулярно. Это не тот вопрос, который можно игнорировать, пока в защите не будет пробита неизбежная брешь. Первые лица компании должны ввести кибербезопасность в круг регулярно обсуждаемых тем. Я не столь наивна, чтобы полагать, будто кибербезопасность способна привлечь столько же внимания и времени, как, например, финансовые показатели компании. Но если первые лица вообще озабочены снижением риска (а я уверена, что таких большинство), то кибербезопасности следует выделить разумную долю времени в повестке дня.

Сколько именно? Зависит от того, насколько хорошо ваше руководство уже разбирается в теме. Если ваш директор по ИБ еще не дал первым лицам достаточное представление о текущем состоянии вашей кибербезопасности, выделите на эту тему не менее 90 минут. За это время ваш руководитель по ИБ должен осветить наиболее важные для компании в целом вопросы.

Для этого потребуются плотные консультации с руководителями бизнес-подразделений. Правильный ответ может не лежать на поверхности. Например, данные о клиентах могут не быть важнейшим активом вашей организации (хотя, скорее всего, в списке приоритетов будут занимать очень высокое место). Но если вы управляете крупным производственным предприятием, эти данные могут быть важнейшим вашим стратегическим активом, скомпрометировать или закрыть от вас который заинтересованные хакеры смогут с помощью подключенных устройств, дающих доступ ко всем аспектам бизнеса.

Ваш директор по ИБ должен предоставить руководству данные о текущем положении дел с уязвимостью по каждому активу в порядке убывания их стратегической ценности. Не слишком упрощая задачу, вы можете представить себе систему координат, одна ось которой представляет степень уязвимости, другая — стратегический приоритет. Активы, являющиеся одновременно стратегически важными и крайне уязвимыми, требуют немедленного перераспределения бюджета.

Большинство руководителей высшего звена склонны раскошеливаться лишь тогда, когда уже происходит взлом — и это в лучшем случае. Вот что показало проведенное в 2017 году компанией EY глобальное исследование информационной безопасности: 76% руководителей признали, что выделение дополнительных средств на кибербезопасность могло быть инициировано только в случае взлома, который нанес реальный ущерб. Взлом без последствий? Около 2/3 заявили, что подобное не требует дополнительных расходов [16].

Очень важно обладать достаточными знаниями в области кибер-безопасности, чтобы обеспечивать эффективный надзор за кибер-рисками. Однако на деле владеют им менее 40% первых лиц компаний [17].

Как только вы скооперируете первых лиц компании и руководителя по ИБ, постарайтесь сделать последнего постоянным участником заседаний совета директоров. Кибербезопасность развивается с головокружительной скоростью. Ваши противники крайне заинтересованы в том, чтобы навредить вам. Они не устраивают себе выходных. И вам не следует расслабляться.

На каждом заседании правления как минимум 30 минут посвящайте вопросам кибербезопасности. Если в среднем совет директоров собирается шесть раз в год на четырехчасовое совещание, то я прошу вас уделить менее 15% времени обсуждению этой важнейшей темы. Deloitte сообщает, что регулярно вопросы кибербезопасности включаются в повестку заседаний правления менее чем в 20% компаний [18]. Если принять на веру подсчеты Deloitte и учесть, что кибербезопасность относится к самым высоким рискам для большинства руководителей, посвятить этому вопросу три часа в год кажется более чем разумным.

Попросите директора по ИБ обновлять оценку степени риска к подобным заседаниям. Он должен быть готов рассказывать об изменчивой ситуации с уязвимостями. Получить эту информацию он сможет из результатов так называемых атак «красной команды» или тестирования на проникновение. Настаивайте на проведении таких упражнений как на отдельном направлении деятельности. Это моделирование атаки злоумышленников на вашу компанию, в ходе которой можно проверить ее защитные системы. Директор по ИБ сформирует две команды: «красную» (атакующие) и «синюю» (защитники). «Красная» команда, в которую обычно входят эксперты из сторонних организаций, пытается взломать «синюю» (представителей компании). С помощью этого упражнения в компании находят ранее неизвестные уязвимости в своей системе безопасности.

Знайте: «красная» команда всегда побеждает. И это хорошо. Вы же хотите обнаружить уязвимости своей системы раньше, чем это сделают хакеры? Заплатить сторонним агентствам за то, чтобы узнать слабые места своей кибербезопасности, гораздо более выгодное решение, чем расплачиваться со злоумышленниками (и органами регулирования) в случае настоящего взлома.

Наконец, рассмотрите возможность назначить членом совета директоров человека с опытом в сфере кибербезопасности. Он привнесет в заседания свое уникальное видение проблем. Как человек,

стоящий на страже киберзащиты, он позаботится о том, чтобы правление не сделало шаг назад, снова задвинув эту функцию на задний план. Думаю, у нас немало работы на этом фронте. По данным Deloitte, за последние два года более 80% компаний не вводили в состав совета директоров никого, кто обладал бы опытом в сфере кибербезопасности [19].

Как сделать мистера/миссис Целлофан видимыми

Директор по ИБ — незаменимый, часто недооцененный член руководящего состава. Хотя за кибербезопасность несет ответственность каждый сотрудник компании, правление и генеральный директор обязаны задать верное направление с самой верхушки организации. Вы должны сыграть свою роль в том, чтобы киберзащита поднялась в вашей системе ценностей на ту высокую ступень, которой она заслуживает.

Одна из моих любимых киноцитат — из фильма «Подозрительные лица»: «Величайший трюк дьявола состоял в том, чтобы убедить весь мир, будто его не существует». Вашим противникам нужно одно: чтобы вы продолжали держать ваших мистера или миссис Целлофан спрятанными в тени. Злоумышленники рассчитывают, что вы точно так же проигнорируете и их — растущий легион хакеров, ищущих возможность нанести урон вашей компании. Эти злодеи хотят, чтобы вы обесценили кибербезопасность, отнеся ее к нестратегическим инвестициям. Не дайте им добиться этого.

Если здесь вас постигнет неудача, вы рискуете потерять одного из самых ценных членов руководящего состава — мистера или миссис Целлофан. И в условиях нехватки талантливых специалистов в этой отрасли, о чем я уже упоминала, оперативно найти замену вам будет крайне сложно.

Век директора по безопасности в компании относительно недолог — всего 24 месяца по некоторым отраслевым данным. ESG попытались выяснить, почему руководители по ИБ не задерживаются на своих местах. Спрос на рынке труда в сфере кибербезопасности сегодня превышает предложение, и в обозримом будущем ситуация не изменится (благодаря все той же нехватке талантов). Однако ESG выяснили, что, когда директора по ИБ оставляют свою компанию и переходят в другую, руководствуются они далеко не только вопросом заработной платы:

36% уходят, когда их работодатель не поддерживает корпоративную культуру с упором на кибербезопасность (очень хорошо, что вы читаете эту книгу!);

34% — когда не чувствуют, что активно участвуют в исполнительном руководстве и советах директоров; и, наконец,

30% — когда бюджеты, выделяемые на кибербезопасность, несоизмеримы с масштабами организации или отрасли [20].

Генеральный директор и правление могут сделать многое, чтобы поучаствовать в решении проблемы кибербезопасности, и в том числе дать право голоса директору по ИБ. Помимо того, чтобы допустить его к обсуждениям, предложите ему провести собрание, где он сможет обосновать необходимость выделять больше ресурсов (учитывая вышесказанное, его аргументы в пользу увеличения бюджета скорее правомерны, чем нет). Относитесь к нему как к управленцу и изучайте его аргументы, задавая вопросы по существу. Постарайтесь сначала глубже изучить проблему кибербезопасности — надеюсь, прочтение этой главы поддержало вас в данном стремлении.

На самом деле директор по ИБ может быть сделан из чего угодно, только не из хрупкого целлофана. Выстоять в суровых ветрах преобразований ему помогает стальной позвоночник; железные кулаки — выдержать бесконечный натиск атак; бетонная челюсть — принимать удары упреков, которые более слабых выведут из строя. Когда вы наконец распознаете и оцените твердость и решимость, отличающие самого недопонятого члена руководящей группы, вы выведете кибербезопасность на свет, а вместе с ней — и неприятелей, которые больше всего хотели бы остаться в тени.

Глава 3

Звонок-будильник

Я бы сказал, что никогда сознательно не нарушал политику кибербезопасности своей компании. Но все же я считаю большей проблемой недостаток четкой информации об этой политике. О таких вещах менеджеры, как правило, не распространяются, потому что сами не всегда в них сильны. *Я считаю, большинство людей не осознает всех последствий своих действий в том, что ка*сается кибербезопасности и защиты данных компании. Многие внутри организаций делают все возможное, чтобы обезопасить себя при использовании различных технологий. Но все же это вечный бой, который ИТ-группы ведут практически в любой компании.

Респондент этнографического онлайн-исследования McAfee

С детства мне привили здоровое уважение к власти. Мои мама с папой были достаточно строги. Они ожидали от меня соблюдения разумных правил. Выполняй домашнюю работу. Возвращайся к определенному

часу. Убирай в комнате. Уважай старших. В общем, делай все, что положено ответственному и полезному члену общества.

Поэтому, получив однажды ранним утром выходного дня от мамы голосовое сообщение, в котором она говорила, что меня разыскивает кто-то из правоохранительных органов, я на мгновение растерялась, прежде чем взять себя в руки и перезвонить.

— Элли, нам позвонил шериф из Нэшвилла. Он ищет тебя. Говорит, на тебя выписан ордер за пропущенное судебное заседание в округе Дэвидсон.

Пока мама эмоционально передавала мне сообщение этого шерифа, сердце у меня колотилось все быстрее.

— Мама, тут что-то не так. Я уже 20 лет как не живу в Нэшвилле! И никто не сообщал, что мне нужно явиться на суд.

— Дорогая, я ему сказала то же самое. И обещала, что ты перезвонишь.

Муж встает намного позже меня, так что я решила постараться разобраться с этим, пока он не проснулся.

Я набрала номер, начинающийся с кода Нэшвилла — 615.

— Шериф Джонсон. Слушаю.

Вас когда-нибудь заставало врасплох то, что трубку взял именно тот, кто вам нужен? Очень странное чувство. Вы надеетесь на ответ и в то же время нет. Примерно это я испытала, услышав его голос. Я поймала себя на том, что с трудом подбираю слова.

— Эм-м, здравствуйте, шериф. Это Эллисон Сэрра. Насколько я знаю, сегодня утром вы разговаривали с моей мамой.

Ему подбирать слова совершенно не понадобилось.

— Да, госпожа Сэрра. Я позвонил вашей матери, так как мы не могли вас разыскать. У меня на руках действующий ордер: вы должны предстать перед судьей [такой-то] в округе Дэвидсон, штат Теннесси, из-за неявки в суд в августе. Я вижу, вы раньше проживали в Нэшвилле, верно?

Власть — мощная сила, особенно для того, кто всю жизнь питал к ней уважение. С раннего детства я знала: если кто-то, обладающий властью, обращается к тебе, ты не можешь ответить вопросом на вопрос. Ты просто отвечаешь.

— Да, верно.

— Что ж, довожу до вашего сведения, что на вас выписан ордер за неявку на судебное заседание 15 августа.

Власть также заставляет вас исправлять неточности. Быть такого не может, чтобы этот шериф был прав. Но вместо того, чтобы дать волю реакции «бей или беги», заставляющей насторожиться, мое непреодолимое почтение к власти заставило меня объясняться.

— Извините, сэр. Это явно ошибка. Я жила в Нэшвилле всего несколько месяцев в 1995 году. В августе меня там даже не было.

— Госпожа Сэрра, я не знаю, что вам сказать. Ордера выписывает судья. Вам нужно будет задать этот вопрос ей.

И вот история приняла неожиданный оборот. Разговаривая с мошенником, вы ожидаете, что он немедленно начнет свою презентацию из разряда «но если вы назовете номер своей кредитки, мы обязательно все уладим», которая немедленно вызвала бы подозрения.

Но он ничего подобного не делал. Он просто продолжал задавать вопросы о моей биографии.

А я продолжала отвечать.

— Я вижу, что вы жили по такому-то адресу, это верно?

— Да, сэр. Все верно.

— И теперь вы проживаете в округе Дентон. Правильно?

— Да, вместе с мужем.

Обратите внимание: я полностью подпала под влияние власти, отвечая на вопросы даже более подробно, чем требовалось. Этот парень меня подловил.

Тут из спальни, сонно протирая глаза, появился муж. Однако он был достаточно бодр, чтобы заметить серьезность моего разговора, совершенно не похожего на рабочий.

— Что происходит?

Шериф все еще подтверждал информацию. Я отключила звук на телефоне, чтобы быстро ввести своего благоверного в курс дела.

— Мне позвонила мама. С ней связался шериф из Нэшвилла и сказал, что на меня выписан ордер за неявку в суд. Я сейчас с ним на телефоне, пытаюсь разобраться.

— Как это вообще возможно? Ты сто лет как не живешь там.

(В этот момент я разозлилась на мужа за то, что утверждал очевидное.)

[Сквозь зубы:] — Я знаю. Потому и пытаюсь разобраться.

И тут мой муж, только-только проснувшийся, выдал вопрос, который я должна была задать себе сама еще до того, как набрать номер шерифа:

— А ты уверена, что этот парень не мошенник?

Вам знакомо это ощущение, когда мысли у вас в голове проносятся с такой скоростью, что вы можете заново проиграть последние мгновения своей жизни за какие-то наносекунды? В моем случае это были последние полчаса с того момента, как я получила сообщение от мамы, которое сейчас снова покручивала в голове. Впервые за эти 30 минут все стало предельно ясно.

Голова шла кругом, а сердце колотилось уже по совершенно другой причине. «Шериф Джонсон» продолжал что-то бормотать, но реакция «бей или беги» наконец сработала. Я попыталась привести мысли в порядок и снова включить мозг, который меня подвел.

— Шериф, я абсолютно уверена, что это какая-то ошибка. Спасибо, что предупредили меня. Я перезвоню вам, и мы решим проблему.

Я спешила закончить этот разговор. Он же был на удивление любезен. Никаких последних отчаянных попыток получить номер кредитной карты. Никаких угроз, что полицейские вот-вот постучатся ко мне в дверь.

— Конечно, госпожа Сэрра. Я понимаю. Можете перезвонить мне по этому же номеру.

Гудок.

Я еще не успела повесить трубку, а муж уже звонил по мобильному шерифу округа Дэвидсон.

Вы, наверно, и сами догадаетесь, чем кончилась эта история. Не было там никакого шерифа Джонсона. Как и не было никакого ордера за неявку в суд — как, впрочем, и вообще ничего на меня не было. Очевидно, это довольно распространенная афера, что подтвердил настоящий полицейский, с которым говорил мой муж.

— Мы получаем подобные звонки как минимум раз в неделю. Это аферисты. Передайте супруге, что при наличии ордера мы звонить не станем. Мы просто позвоним вам в дверь. (Ага. Почувствуй себя идиотом.)

Однако я на всякий случай сходила в местный полицейский участок, чтобы убедиться, не водится ли каких-либо грехов в личном деле одного ответственного-и-полезного-для-общества гражданина. Я спросила офицера за столом, не собирается ли он арестовать меня за что бы то ни было. Наконец меня накрыла волна облегчения: он посмотрел на меня так, будто я только что с Марса свалилась, но ответил единственным словом, которое я хотела услышать, — «нет».

***

Возможно, вы уже сомневаетесь, стоило ли покупать книгу о защите своей компании от киберугроз, написанную автором, который только что сознался в совершении столь бестолковой ошибки. И будете не столь уж неправы. В конце концов, я уже сказала, что почувствовала себя крайне глупо, после того как вскрылись все обстоятельства.

Но прежде чем слишком строго осудить мои действия, давайте представим, что эта история — всего лишь единичный пример того, что происходит с ничего не подозревающими жертвами вроде меня

буквально по тысяче раз в день. В индустрии кибербезопасности такое мошенничество называют «социальной инженерией».

Одна из разновидностей такой деятельности знакома вам как фишинг: киберпреступники рассылают вредоносные электронные письма, выдавая себя за авторитетную личность и прося своих жертв поделиться конфиденциальными данными или перейти по ссылке. Мы в некоторой степени недооцениваем изобретательность тех, кто занимается фишингом. Эта деятельность со времен «Помогите, я нигерийский принц и мне очень нужны деньги» добилась большого прогресса. Только в 2018 году McAfee обнаружила более миллиона новых фишинговых URL-адресов [21].

Социальная инженерия выходит за рамки цифровой среды, доказательством чему служит мой случай. Я работаю в индустрии, поэтому научилась определять вредоносные письма. Но я никак не ожидала старомодной попытки телефонного обмана.

Чтобы действовать эффективно, мошенникам даже не нужно быть особенно изощренными. Они знают: доверие — неотъемлемая часть существования нашего общества. Кроме того, им известно, что я не одна воспитана таким образом. Многие из нас — ответственные, полезные члены общества, приверженные консервативным ценностям — уважению и доверию.

Меньше всего я хочу, чтобы кто-то из нас поддался нагнетанию страха, которое стало в нашем мире слишком уж обычным делом. Доверие необходимо для прогресса. И все же, не будучи излишне доверчивыми, мы можем также не быть слишком пугливыми. Здесь есть тонкая грань, как, собственно, и в остальных случаях, с которыми вы столкнетесь, раскрывая для себя такую сложную тему, как кибербезопасность.

Вместо того чтобы броситься с головой в омут апокалиптических пророчеств, где хакеры отбирают все, что нам принадлежит, я сосредоточусь на отрезвляющей реальности: любой, кто читает эту книгу, представляет собой одно из сильнейших или слабейших звеньев цепи в борьбе их компании с киберпреступностью.

Задумайтесь о силе этого утверждения. Компания Gartner, отраслевой аналитик, предсказала, что в 2018 году организации со всего мира потратят более $114 млрд на продукты и услуги в области кибербезопасности [22]. Это ставит кибербезопасность в один ряд с такими многомиллионными ($100 млн и выше) отраслями, как цифровое телевидение и видео, цифровой маркетинг и игровая индустрия.

И все же никакие инвестиции не заменят сотрудников, делающих то, что нужно, и так, как нужно.

Лучшая защита

Тысячелетняя военная история свидетельствует: лучшая защита — это нападение. Потому-то Джордж Вашингтон и включил этот проверенный временем совет в свои сочинения почти через четверть века после того, как привел молодое государство к победе в Войне за независимость. Этот совет пригодится в схватке с противником: пролейте первую кровь, и он будет больше отвлекаться на самозащиту, чем нападать на вас. В спорте команды стараются первыми заработать очки, чтобы получить начальный импульс в игре. В бизнесе компании стремятся получить преимущество первопроходца при выпуске нового продукта или услуги, чтобы на раннем этапе захватить свою долю рынка.

В вопросе кибербезопасности для компании не существует такого понятия, как нападение. Она по определению не может нанести первый удар. Это всегда делает противник. Преимущество первопроходца всегда на его стороне. Нашим компаниям суждено вечно играть от обороны. В кибербезопасности лучшая защита — это хорошая (если не отличная) защита.

Как я уже говорила, я считаю, что большинство сотрудников хотят помочь защитить свои организации, просто не знают, как делать это эффективно.

Но давайте представим на секунду, что я ошибаюсь и вы не испытываете никаких альтруистических побуждений в отношении своей компании. Это не значит, что вы желаете ей вреда. Вы бы не стали намеренно толкать своего работодателя под автобус, например. Но, может быть, вы и не из тех, кто ради своей компании коня на скаку остановит.

Это относит вас к категории равнодушных сторонних наблюдателей. Вы считаете, что компания тратит достаточно средств на кибербезопасность, нанимает людей, которые отвечают за защиту. Если бы вы стремились выполнять такого рода работу, у вас были бы соответствующее образование и должность. Но это не так. Вы отвечаете в компании за другие вопросы и рассчитываете, что задачи кибербезопасности решаются (и должны решаться) в другом месте. Если ваша компания действительно пострадала от взлома, который произошел не по вашей вине, тогда это и впрямь не ваша проблема. Может, компании придется раскошелиться или даже потерять некоторых клиентов. Но жизнь и работа на этом не остановятся.

Если вы попали в эту категорию, то вы не одиноки. Проводя свое этнографическое онлайн-исследование среди сотрудников, таких же, как вы, мы в McAfee слышали схожие мнения, задавая вопрос:

Какую роль играют рядовые сотрудники в обеспечении кибербезопасности в вашей организации? Как вы считаете, вы лично играете ключевую или второстепенную роль?
Респондент 1: *Думаю, в обеспечении кибербезопасности компании я играю совсем незначительную роль. Мне важно знать, чем я могу поспособствовать защите данных, но общая безопасность должна обеспечиваться сотрудниками более высокого уровня.*
Респондент 2: *Моя роль скорее второстепенная, так как всю закулисную работу по обеспечению кибербезопасности ведет наш ИТ-отдел.*
Респондент 3: *Думаю, моя роль небольшая. В первую очередь за это отвечают технологии нашей ИТ-команды, во вторую — сама команда, и только затем рядовые сотрудники.*
Похоже, ряд сотрудников полагает, что кибербезопасность стоит полностью доверить инструментам или людям внутри ИТ-отделов, а то и вовсе переложить всю ответственность на высшее руководство компании. И вот в чем загвоздка с обеими точками зрения.

Во-первых, на решение проблемы не хватает персонала (вспомним о нехватке специалистов по кибербезопасности, о которой я говорила в предыдущей главе). А киберугрозы требуют свистать всех наверх.

Во-вторых, если вы считаете, что с проблемой лучше всего справятся именно важные шишки вашей компании, возможно, вам не стоит слишком на это полагаться. Да, генеральный директор и правление ответственны за то, чтобы с самых верхов задавать курс на кибербезопасность. Однако 60% руководителей высшего звена и ИТ-руководителей заявляют, что человек, непосредственно отвечающий за защиту информации, — это точно не член совета директоров [23].

Понятно, почему такое перекладывание ответственности за кибербезопасность очень распространено в организациях. В индустрии кибербезопасности известно состояние, которое можно назвать «усталостью от взломов». Именно это происходит, когда мы позволяем привычке к опасности заглушить в нас чувство, что нужно срочно реагировать. Либо мы считаем, что в конечном итоге за нас расплатится кто-то другой (даже если это потребители, которые несут основную тяжесть взломов из-за повышения цен), либо отказываемся от контроля над собственной судьбой и решаем, что мы лично ничего не можем сделать для предотвращения взломов.

В этой книге делается попытка пересмотреть последнюю точку зрения через предложение практических шагов, которые вы можете предпринять, чтобы помочь своей компании избежать взлома. Вы должны знать, что можете сделать. Но если вы относитесь к лагерю тех,

кому все равно, позвольте воспользоваться моментом и объяснить, почему вам следует позаботиться об этом.

Не так давно я получила письмо от сотрудницы нашего отдела персонала. Она переслала мне сообщение, которое получила на личный ящик. В письме была просьба дать инструкции, как изменить автоматические отчисления с заработной платы. Адрес отправителя указывал на то, что это личный аккаунт, и, предположительно, мой.

К счастью, чутье не подвело ее, и она переслала это письмо на мой рабочий адрес, сопроводив его простым вопросом:

«Эллисон, я сегодня получила вот это письмо. Ты действительно его отправляла?»

Я очень быстро ответила категорическим «нет». Мы сообщили об инциденте в наш Центр обеспечения безопасности. Они отследили адрес и выяснили, что хакер взломал ее личную учетную запись.

Я не сомневаюсь, что в список должностных обязанностей этой сотрудницы отдела персонала не входит забота о «кибербезопасности». Готова поспорить: в нем нет формулировок, призывающих ее быть бдительной в том, что касается киберугроз в отношении сотрудников компании. Никто не мог требовать от нее обратиться ко мне напрямую, чтобы подтвердить легитимность полученного письма. Однако именно так она и поступила, и я рада была видеть проявление ее здравого смысла и неравнодушия. Бдительность не позволила ей ответить простым копированием инструкций из нашего интранета, объясняющих, как легко изменить свои отчисления. Нам ужасно повезло: ее инстинкты значительно усложнили задачу тому хакеру. Кроме того, она избавила меня от долгих часов расстройства в попытках исправить плачевные последствия. Кризис, по крайней мере для меня, был предотвращен.

Порой целью хакеров является не просто наша компания. Порой их цель — мы. Наши работодатели располагают обширной информацией о каждом из нас, включая номера социального страхования, реквизиты счетов (как показал мой пример с автоматическими отчислениями) и многое другое. Самая знаменитая утечка данных сотрудников в современной истории произошла с правительством США, когда его Управление кадровой службы было скомпрометировано взломом более 21,5 млн записей. Какая добыча среди прочего досталась мошенникам? Обширная справочная информация о людях, которые могли даже не быть действующими или бывшими сотрудниками Управления [24].

Если и этого аргумента недостаточно, чтобы убедить вас в необходимости быть неравнодушным, то как насчет такого: цена утечки информации для вашей компании никогда не была выше. Спасибо регулирующим органам, старающимся мотивировать компании

защищать данные клиентов. Ко всем компаниям, ведущим бизнес или контролирующим деятельность субъектов в Евросоюзе, применяется Общий регламент по защите данных. Компании могут потерять до 4% глобального годового дохода, если будет установлено, что они не соблюдают стандарты Общего регламента в отношении сбора и защиты данных своих клиентов. В 2018 году компания Ponemon отчиталась, что средняя цена утечки данных составила $3,86 млн — и это еще задолго до вступления в силу Общего регламента по защите данных [25]. Любая компания с годовым доходом более $100 млн, ведущая дела в Евросоюзе, уже может рассчитывать заплатить больше — вероятно, значительно больше в зависимости от ее дохода — за взлом, нарушающий Общий регламент.

Риск утечки данных крайне высок. Цена взлома и того выше. Не думайте, что ваша компания переживет следующий взлом только потому, что в прошлом уже справлялась с подобным. Финансовое давление может привести и к другим последствиям, вплоть до сокращений. Если вы хотите сохранить текущую работу и видеть вашу компанию дееспособной, сделайте заботу о кибербезопасности пунктом своих должностных обязанностей. Трусливое равнодушие с вашей стороны — только этого врагам и надо.

W.I.S.D.O.M. для сотрудников

Согласно отчету Verizon об исследовании утечки данных 2018 года, сотрудники прямо или косвенно ответственны более чем за четверть всех взломов. Более чем в 60% подобных случаев вина лежит на равнодушном сотруднике. А значит, почти 20% всех взломов — дело рук нерадивых работников [26]. Вот почему персонал — одно из сильнейших или слабейших звеньев на страже кибербезопасности своей компании.

К счастью, сотрудники могут многое предпринять, чтобы поспособствовать обеспечению кибербезопасности, а не стать ее угрозой. Во-первых, нужно остерегаться мошенничества с использованием социальной инженерии. Киберпреступники знают, как играть на доверчивости сотрудников. И их методы совершенствуются. Адресный фишинг — это тактика целенаправленного воздействия на определенных лиц или компании через вредоносные сообщения, такие как электронные письма. В отличие от традиционного фишинга, который скорее можно отнести к тактике «пальцем в небо» (киберпреступники крайне мало прибегают к таргетингу, если вообще прибегают), адресный фишинг гораздо более эффективен, поскольку

преступник прикладывает большие усилия, чтобы персонализировать свое сообщение.

Уэйлинг является одной из разновидностей адресного фишинга: злоумышленник, выдавая себя за высокопоставленного руководителя компании, например, генерального или финансового директора, требует неких действий от ничего не подозревающего сотрудника. Так, под личиной финансового директора мошенник может нацелиться на рядового сотрудника финансового отдела и отдать распоряжение перевести средства компании на некий счет.

Социальная инженерия — один из наиболее очевидных способов повлиять на наивных сотрудников. Согласно отчету Verizon, жертвами любой фишинговой кампании склонны стать 4% людей. И, пожалуй, самое удивительное в том, что они вряд ли будут учиться на своих ошибках. Чем на большее количество фишинговых писем откликнулся человек, тем больше вероятность, что он сделает это снова [27].

Социальная инженерия крайне эффективна на разных уровнях организации. Да, в том числе и на самом высоком. В 2018 году Forbes сообщил, что порядка 80 000 фирм в США, Великобритании и Европе перевели злоумышленникам более $12 млрд в рамках пятилетней целенаправленной кампании по уэйлингу. Кто же из сотрудников, того не ведая, помогал злоумышленникам грабить компании? Их собственные финансовые директора. Выяснилось, что у преступников была база данных, куда входило более 50 000 финансовых директоров, которых в афере использовали в качестве «меток» [28]. В данном случае киберпреступники использовали персонализированные электронные письма, будто бы отправленные генеральным директором и содержавшие требование к директору финансовому немедленно совершить банковский перевод. Мы все можем сделать выводы из этого дорогостоящего урока. Любого из нас можно обмануть.

Итак, первое правило W.I.S.D.O.M. для сотрудников — **не поддаваться на фишинг.** Ищите признаки, выдающие вредоносное письмо, например адрес отправителя. Не переходите по ссылкам из неизвестного источника. Вместо этого поищите сведения о компании или перейдите прямо на ее домен. Но будьте осторожны. Большой популярностью пользуется фарминг: киберпреступники создают вредоносные сайты, куда заманивают жертв, чтобы получить свою награду — финансовую или другую личную информацию. Вы можете даже ввести имя домена вручную — и все равно попасть на поддельный сайт.

Помимо того, чтобы не попадаться на фишинг, **проявите активность и немедленно сообщите о попытке своему ИТ-отделу или специалистам по безопасности.** По данным отчета Verizon,

у компаний есть 16 минут до того, пока кто-то из сотрудников не клюнет на приманку фишинга первым кликом мыши. А когда специалистам по безопасности поступает первый отчет о произошедшем? Через 28 минут [29]. В течение этих 12 минут время выступает на стороне вашего противника и становится в его руках еще одним орудием, с помощью которого он может нанести компании значительный вред.

Как показывает мое признание в начале главы, чтобы быть эффективной, социальная инженерия не обязана быть высокотехнологичной. Телефонное мошенничество и старые добрые кражи оставленных без присмотра ноутбуков, флешек и мобильных устройств тоже отлично работают.

Однако, хоть старомодные преступления могут вполне соответствовать целям преступников, помните: они становятся изощреннее и самосовершенствуются с помощью технологий, которые делают социальную инженерию все более эффективной. Искусственный интеллект (ИИ), который так облегчает нам жизнь (вспомним хотя бы, как поисковик сам заканчивает за нас слово или фразу, стоит нам только начать вводить их), является новейшим оружием как в арсенале преступников, так и на страже кибербезопасности. ИИ предлагает злоумышленникам еще большую точность в проведении их фишинговых кампаний. Они смогут еще более метко нацеливаться на ничего не подозревающих жертв. Кроме того, они могут использовать ИИ для создания персонализированных сообщений в огромных объемах.

Новый тип социальной инженерии, который становится результатом подобной деятельности, сочетает в себе прицельную эффективность адресного фишинга с масштабами традиционного. Иными словами, в будущем определить фишинговое сообщение будет только сложнее. Онлайн-мир все больше походит на бал-маскарад со всей магией чуда и изумления, которые обещает интернет. Но с каждым часом вечеринка становится все более «многолюдной»: ее переполняют угрозы вроде фишинга, прикрывающиеся причудливыми масками. Ваша бдительность в осознании этой угрозы должна также возрастать со временем.

Поскольку преступники становятся все более подкованными, компании вкладывают в кибербезопасность гораздо больше, чем когда-либо. Но средства защиты приносят пользу лишь в том случае, если их применяют постоянно и регулярно обновляют. Вы можете считать, что ответственность за это в наибольшей степени лежит на директоре по ИБ и его отделе. И будете правы — до определенного момента. **Сотрудники в равной степени несут ответственность за**

обновления на своих ноутбуках, мобильных и других персональных устройствах.

Если ИТ-отдел в рабочие часы запускает обновление, временно снижающее вашу производительность, пожалуйста, не спешите жаловаться. Помните: кибербезопасность не подчиняется традиционным правилам ИТ, согласно которым исправления ПО могут происходить в нерабочее время. Если преступник атакует вашу организацию с помощью новейшей онлайн-напасти, ваша команда, отвечающая за кибербезопасность, не может позволить себе роскошь сидеть и ждать подходящего времени, чтобы запустить обновление защиты устройств. Время — самое желанное оружие для преступника. И оно точно не на стороне вашей компании. Лишь немного понимания и готовность принять эти обновления — вот все, что нужно вашим специалистам по кибербезопасности, выполняющим свою работу и защищающим вас от угроз.

Наконец, в том, что касается кибербезопасности, ничто не заменит строгую гигиену. Порой самые эффективные меры — те, которые проще всего принять. Наверно, нет лучшего тому подтверждения, чем пример из здравоохранения. В XIX веке венгерский врач Игнац Земмельвейс попытался разгадать одну загадку. Он хотел узнать, почему так много женщин умирали от послеродовой лихорадки. Так, он заметил, что в палатах, где работали только врачи-мужчины, уровень смертности был значительно выше по сравнению с теми, где работали только женщины-акушерки. После множества экспериментов, в том числе изменения позы роженицы и даже просьбы, адресованной священникам, не проходить мимо выживших, выражая почтение недавно почившим матерям (чтобы эти священники действительно не запугали других рожениц до смертельной лихорадки одним своим присутствием!), Земмельвейс нашел ответ.

Выяснилось, что врачи-мужчины проводили вскрытия, а акушерки — нет. После вскрытия тот же врач мог принять роды, в процессе занеся в организм матери трупные частицы. Земмельвейс настоял на том, чтобы эти мужчины-врачи помимо привычного мыла и воды мыли руки и инструменты раствором хлора, полностью удаляя с них трупные частицы. Он понятия не имел, что хлор — дезинфицирующее средство. Доктор лишь знал: хлор весьма эффективен для устранения неприятного запаха, остающегося вместе с частицами трупа на руках врачей и их инструментах. Хотя до открытия микробов прошло еще несколько десятилетий, новый протокол Земмельвейса все же возымел действие. В результате уровень смертности от родильной лихорадки в отделении, где работали только врачи-мужчины, снизился. К счастью для нас,

случайное открытие венгерского врача проложило путь к снижению смертности в медицине.

Даже сегодня мытье рук остается одним из наиболее действенных инструментов достижения общественного здоровья — от предотвращения инфекций в ходе операции до защиты от гриппа. Конечно, тут требуется дисциплина. Но зато всего за несколько секунд (если вы зашли в туалет) или минут (если вы профессиональный хирург) вы эффективно защитите себя от множества бактериальных и вирусных врагов из нашего окружения.

Последовав примеру специалистов из области здравоохранения, сотрудники могут практиковать здравую гигиену и в том, чтобы защитить свои компании от самых разных угроз. Вы когда-нибудь позволяли веб-сайту автоматически сохранять пароли или использовали свой смартфон или ноутбук для их хранения? Не нужно этого делать. Тут достаточно будет и одного примера: сотрудница компании использовала личное мобильное устройство для хранения всех своих паролей, в том числе и пароля для ее почтового аккаунта O365. Киберпреступник взломал ее мобильное устройство и украл учетные данные O365. Скомпрометированные таким образом данные были использованы, чтобы получить доступ к аккаунту O365, и хакер стал рассылать руководителям и другим коллегам из ее адресной книги фишинговые письма, которые выглядели как не вызывающие сомнений сообщения от этой сотрудницы. Кражу учетных данных организации обнаружить особенно сложно. В конце концов, доступ сотрудника к аккаунту выглядел вполне законным. И только когда бдительные получатели электронной рассылки забили тревогу, угроза была обнаружена и сдержана.

Я понимаю, что придумывать пароли непросто. В нашем мозге не заложена способность запоминать сотни паролей для разных устройств, сайтов и приложений. Хуже того, надлежащая гигиена в сфере кибербезопасности требует, чтобы пароли менялись регулярно, что еще затрудняет возможность их запомнить.

Существуют такие инструменты, как генераторы паролей, которые помогут вам создать и восстановить сложный пароль. Но если вы не хотите пользоваться подобным инструментом, можете помочь своей памяти, прибегнув к мнемоническому трюку. Так, я выбрала строку из детской песенки «Джек и Джилл идут на горку» (Jack and Jill went up the hill to fetch a pail of water), взяла первые буквы каждого слова (JaJwuthtfapow), использовала символы и комбинацию прописных и строчных букв (J@Jwuthtf@pow) и для верности добавила цифры (J@Jwuth2f@pow). Если верить сайту HowSecureIsMyPassword.net,

чтобы взломать пароль, который я только что придумала, компьютеру понадобится порядка трех миллионов лет.

Управление паролями необходимо для надежной кибергигиены. К сожалению, практикуется оно не так часто, как следовало бы. Не далее как в 2018 году в одном штате количество правительственных чиновников, использовавших пароль «Пароль123», составляло порядка 1500 человек [30]. Хм, как еще облегчить работу хакеру?

Кроме того, о своей физической безопасности следует заботиться не меньше, чем о сетевой. Как я уже говорила в предыдущей главе, миры физической и кибербезопасности все больше сближаются. Киберпреступники не просто нацеливаются в своих атаках на физическую инфраструктуру (включая электросети и производственные мощности): скомпрометированные устройства сотрудников открывают для преступников путь к системам компании.

Одна из самых значительных атак национального масштаба, Stuxnet, была осуществлена через скомпрометированное USB-устройство. Оно позволило правительству США получить доступ к ядерным центрифугам и приостановить ядерную программу Ирана. Как я не устаю повторять, кибератака необязательно должна полагаться на технологии следующего поколения, чтобы быть эффективной.

Вы не трудитесь на ядерной установке? Велика вероятность, что у вас как минимум есть компьютер, который вы используете для работы. Если вы похожи на 25% сотрудников компаний в США, то, уходя домой в конце дня, вы оставляете его включенным и не заблокированным [31]. Это все равно что не вымыть руки после посещения туалета!

И, наконец, для доступа к конфиденциальным данным или их передачи используйте только VPN-сеть вашей компании. Публичные сети Wi-Fi — это настоящее золотое дно для предприимчивых преступников. Кибергигиена здесь находится на крайне низком уровне — и даже профессионалы отрасли не являются исключением! В 2019 году в ходе крупнейшего отраслевого мероприятия, RSA, в котором ежегодно участвуют более 40 000 профессионалов сферы кибербезопасности, некто @Grifter801, назвавшийся хакером, написал в Twitter, что примерно за 26 часов с начала шоу собрал более 33 500 незашифрованных паролей [32]. Притягательность публичного Wi-Fi — мощная сила, устоять перед которой не могут даже самые подготовленные профессионалы в области кибербезопасности.

***

Это прямо-таки нечестно. Ваша компания не только обречена все время защищаться от киберпреступников, но и делать это должна с почти

идеальной четкостью. Тем, кто атакует, достаточно всего одного попадания, чтобы нанести значительный, если не непоправимый, ущерб. Никакие инвестиции в кибертехнологии не смогут сравниться по силе с союзом, состоящим из упрямых преступников и бездеятельных (если не невежественных) сотрудников, вставших в этой битве на сторону первых.

Но есть и хорошие новости. Протокол кибербезопасности, объединяющий всю мощь технологий, инструментов и работающих в гармонии людей, может обеспечить впечатляющую защиту от преступников. Это не значит, что те не будут набирать очки. По сути, дело здесь вовсе не в том, была ли взломана ваша компания, а в том, знают ли в ней об этом. Взломы неизбежны, но их последствия не обязаны быть катастрофическими. Когда на стороне компании встает мощная армия из образованных, бдительных и решительных сотрудников, готовых способствовать ее успешной защите, борьба с противником становится гораздо эффективнее.

Глава 4

Остановите конвейер

Кибербезопасность рассматривается как важнейшая защитная мера для нашего бизнеса. Если принять во внимание, что мы делаем и что предоставляем потребителям — воду, — то если наши системы будут скомпрометированы и если клиенты потеряют веру в нашу способность обеспечивать их хорошей, чистой, безопасной питьевой водой, это будет катастрофа.

Генеральный директор коммунального предприятия

Шел 2017 год. Мы наблюдали за началом расследования предполагаемого вмешательства русских в президентские выборы в США. Мы стали свидетелями подъема движения #МеТоо и последующего падения магнатов индустрии развлечений и бизнеса, раздавленных его тяжестью. Мы понесли катастрофические потери из-за гнева матери-природы, обрушившей на нас одни из самых разрушительных ураганов в новейшей истории, в том числе Харви, Ирму и Марию.

Среди всей этой кутерьмы, которая, казалось, стала синонимом всего 2017 года, мы потеряли светило, чей вклад в бизнес надолго останется с нами в обозримом будущем. 30 декабря тихо и без особого шума в СМИ скончался Тацуро Тоёда, сын основателя японской автомобильной компании Toyota. Ему было 88 лет.

Вам наверняка знаком японский автогигант Toyota. Но вы, возможно, не представляете, какое глубокое влияние один из его

прародителей, Тоёда-сан, оказал на то, как мы с вами сегодня ведем бизнес.

Чтобы понять, сколь велико было влияние Тоёды, мы должны вернуться в другую эпоху — в начало 1980-х, — когда он принял бразды правления первым американским заводом своей компании. В те времена на рынке доминировали американские автопроизводители. General Motors (GM) была бесспорно крупнейшей в мире автомобильной компанией. Но при всех их успехах была у них и проблема: национальные руководящие принципы по выбросам принуждали автомобильные компании производить небольшие, экономичные машины, а GM исторически испытывала с этим трудности. В то же время на автомобильном рынке США в целом наметилась тревожная тенденция: японские производители стали стремительно захватывать свою долю — и так быстро, что Конгресс пригрозил ограничить автомобильный импорт.

Это странное сочетание реальных и потенциальных предписаний со стороны правительства США — тех, что заставляли GM производить небольшие экономичные автомобили, и тех, что угрожали ограничить импорт продукции Toyota, — породило самый невероятный из возможных союзов. Toyota и GM, ярые конкуренты за рынок, превратились в своего рода партнеров. Две компании открыли совместный завод во Фримонте, штат Калифорния, где раньше располагался производственный объект GM.

Каждый из конкурентов извлек пользу из интересного соглашения. Toyota должна была сконструировать для GM качественный экономичный небольшой автомобиль, который наконец принесет прибыль. В процессе GM могла получить доступ к принципам производства автомобилей Toyota — буквально заглянуть за закрытые двери и узнать, что за «секретный соус» есть в арсенале у конкурента. Toyota, в свою очередь, должна была научиться производить автомобили в Соединенных Штатах, тем самым снизив риск будущих ограничений на импорт.

А теперь два слова о бывшем заводе GM во Фримонте. Если само «партнерство» между двумя соперниками не показалось вам достаточно странным, то уж выбор места для открытия предприятия походил на причуду. Завод GM во Фримонте был сущей катастрофой. Брюс Ли, в то время возглавлявший западное крыло профсоюза работников автомобильной промышленности, называл местных сотрудников «худшей рабочей силой во всей автомобильной индустрии США» [33]. Об их выходках была наслышана вся отрасль: от рекордных прогулов и непристойных действий на территории завода до саботирования производства ради возможности получить сверхурочные за починку

автомобилей. Если считать поведение показателем, то эти люди точно ненавидели свою работу и компанию.

Возможно, вы не увидите ничего странного в решении создать совместное предприятие на базе завода с такой дурной историей. В конце концов, зачем вместе с водой выплескивать и ребенка? Сам завод мог быть совершенно приемлемым. Но рабочую силу необходимо было менять — и срочно.

Однако GM и Toyota не стали этого делать. Они наняли 85% бывших работников завода во Фримонте (которых один из лидеров их собственного профсоюза назвал худшими в Америке!) для выпуска прибыльного и высококачественного экономичного автомобиля, чего GM не могла добиться на лучших своих предприятиях в США.

Возможно, еще более удивителен тот факт, что они отправили некоторых из бывших сотрудников завода во Фримонте в Японию — обучаться тому, как там собирают машины. Первый автомобиль, желтый Chevrolet Nova, сошел с конвейера в декабре 1984 года. Почти тогда же завод во Фримонте вышел на ту же скорость производства автомобилей и такой же низкий показатель дефектов на 100 единиц продукции, как и японские предприятия.

Что именно позволило Toyota произвести для американцев первый качественный маленький автомобиль руками практически той же рабочей силы, которая была настолько ниже среднего под руководством GM? Это был даже не секретный соус, а, скорее, секретный ингредиент: постоянное совершенствование.

GM переняла свою философию у Генри Форда. Заводы были четко структурированы, разделение труда являлось стандартом, а во главе угла стояла производительность. Если бы нам нужно было выразить культуру компании в форме слогана-наклейки на бампер, это было бы просто «Конвейер не должен останавливаться». По сути, эти четыре слова вмещали главное правило бывшего завода GM. Сборочный конвейер не должен был останавливаться несмотря ни на что.

Интересное требование, с учетом того, что в некоторые дни работников приходило так мало, что конвейер даже невозможно было запустить. Чтобы заполнить пустоту, GM приходилось приводить людей с улицы. И когда конвейер наконец запускался, он уже не останавливался.

Билли Хаггерти занимался монтажом капотов и крыльев. Рик Мадрид собирал грузовики Chevy. Вместе с Брюсом Ли они дали интервью радиостанции NPR, благодаря которому мы с вами можем заглянуть на бывший завод GM во Фримонте и узнать, насколько строго там соблюдалось золотое правило.

Хаггерти: *Производство никогда не останавливалось, конвейер не должен останавливаться.*
Мадрид: *Конвейер просто не останавливается. Я видел, как один парень сорвался и упал, но даже тогда конвейер не остановили.*
Ли: *Видишь проблему, останавливаешь конвейер — ты уволен [34].*
С дефектами разбирались уже постфактум. Для GM количество было важнее качества.

Toyota же построила свою философию на постоянном совершенствовании. Работникам не просто позволялось останавливать конвейер: их поощряли к этому. Шнуры системы андон находились в пределах досягаемости каждого работника на линии. («Андон» с японского переводится как «бумажный фонарь». Рабочие могли давать визуальный сигнал: зеленый — если на линии все хорошо; желтый — если качество продукции под угрозой; красный — если качество упало настолько, что конвейер следует остановить.)

В Toyota не просто собирали автомобили: там выстраивали процесс, в котором приветствовались интересные идеи от работников любого уровня. Процесс, неустанно преследовавший и искоренявший неэффективность в любом ее проявлении. Процесс, заставлявший постоянно повышать требования.

Эта философия «остановки конвейера» позволяла каждому сотруднику завода в некотором смысле руководить производством. Благодаря ей качество стало неотъемлемой частью всеобщей ответственности за проделанную работу. Тоёда поделился японской философией с американскими рабочими. Когда в 2009 году, спустя десятилетия, Автомобильная целевая группа Белого дома проводила оценку GM в связи с банкротством последней, глобальная система производства и поставок GM, созданная по образу и подобию Toyota, была публично признана системой мирового уровня, столь же эффективной, как японский прототип [35]. Поскольку Тоёда был лидером рискованного похода Toyota во Фримонт, GM многим обязана самому покойному учителю.

Однако влияние Тоёды выходит далеко за рамки GM и даже автомобильной промышленности. Одновременно с процветанием завода во Фримонте в 1980-е во многих отраслях получили распространение принципы Общего управления качеством (ОУК): новым лицом управления стало постоянное совершенствование, а целью — качество.

ОУК со временем уступило место другим концепциям, таким как ISO 9000, «шесть сигм» и «бережливое производство». Хоть стандарты и названия могли измениться, главенствующий принцип остался прежним. Качество больше не рассматривалось как некий *приятный бонус*; оно было необходимо для долгосрочного процветания компании.

Стремление к безопасности занимает то же положение, которое занимало качество, пока все мы не подхватили лихорадку ОУК. Разрабатывая продукты и процессы, мы склонны думать о безопасности как о проблеме завтрашнего дня; как о чем-то, чем мы займемся после того, как продукт сойдет с конвейера. Мы все исправим постфактум. Во многих отношениях безопасность — второстепенная задача. И такой ход мыслей нужно изменить, если мы хотим сделать безопасность неотъемлемой частью всего, что предлагаем. В противном случае результаты могут быть катастрофическими.

Интернет терроризма

Шел 2016 год. Может, вы и не заметили, но 21 октября того года вспыхнула война. Продлилась она всего день, но навсегда вошла в анналы кибербезопасности. Именно тогда неприступная оборона интернета была прорвана мародерами, стремившимися посеять хаос невиданных ранее масштабов. В этот день был сломан интернет.

События 21 октября 2016 года доказывают, что реальность порой бывает куда более странной, чем вымысел. Удивительно было не то, что хакеры положили глаз на компанию, которой хотели навредить. Такими заголовками в нашем цифровом мире уже никого не удивишь. Что было уникального в этой атаке, так это компания, попавшая под прицел хакеров: Dyn.

Может, вы и не слышали о компании Dyn в 2016-м, но наверняка пользовались предлагаемыми ею сервисами: Twitter, Netflix, Spotify, Etsy — и это лишь некоторые из них. Помимо прочего, Dyn была провайдером системы доменных имен (DNS). Если вы вводили адрес сайта одного из ее популярных сервисов, Dyn сопоставляла его с соответствующим IP-адресом.

В тот роковой октябрьский день хакеры вывели Dyn из строя с помощью распределенной атаки типа «отказ в обслуживании» (DDoS). DDoS-атаки — излюбленная тактика хакеров: они направляют на веб-сайт избыточное количество запросов и обрушивают его. Интернет состоит из множества путей и пунктов назначения, почти как разветвленная система автомагистралей. И хотя DDoS-атаки — из числа наиболее популярных видов хакерских угроз, два заметных отличия сделали атаку на Dyn совершенно особенной.

Во-первых, большинство DDoS-атак нацелены на конкретную компанию. На самом деле, в определенных отраслях есть компании, в большей степени подверженные подобным вредоносным атакам, нежели остальные. Возьмем, к примеру, онлайн-игры, являющиеся одной из излюбленных мишеней для DDoS-атак. Если вы геймер, то

наверняка знаете, почему. Во многих онлайн-играх для достижения победы от игрока требуется быстрая реакция. Если хакер сможет перегрузить виртуальные магистрали, связывающие игроков с их общей онлайн-действительностью, время реакции замедляется до полной остановки, и вы уже не можете, к примеру, выстрелить в своего оппонента, не дав ему прицелиться в вас. Помимо онлайн-игр, которым DDoS-атаки наносят исключительный вред, они могут вызвать хаос в любой компании с цифровым присутствием. Наводнив веб-сайт мусорным трафиком, хакеры могут лишить доступа настоящих посетителей.

Однако атака на Dyn стояла особняком. Она уничтожила несколько сайтов одним ударом. Перегрузив DNS-сервис Dyn — метафорический эквивалент системы почтовых адресов в сети, — хакеры заблокировали доступ к целому ряду популярных сайтов. Целый регион США в одночасье лишился доступа к самым востребованным веб-сервисам: опорная сеть интернета дала сбой. Если представить себе присутствие нашей страны в интернете как ночной вид из космоса, то в тот роковой октябрьский день все Восточное побережье просто исчезло. Считайте, десятки миллионов людей и цифровую инфраструктуру, на которую они полагались, поглотила тьма. Хакеры успешно стерли цифровое существование одного из самых мощных коридоров власти на нашей планете.

Атака на Dyn была уникальна и в другом. Для выполнения DDoS-атаки требуется огромный размах. Типичный веб-сайт не будет заблокирован, если несколько сотен или даже тысяч мотивированных хакеров будут одновременно посылать на него запросы. Чтобы нанести сокрушительный удар, потребуются миллионы попыток.

И вот в игру вступает еще один термин кибербезопасности, вошедший в лексикон, — ботнет. Выражаясь языком неспециалистов, ботнет состоит из сети устройств, управляемых хакером. Образованная таким образом армия зомби находится под контролем одного или нескольких злоумышленников, которые могут приказать роботам совершить любое количество действий, в том числе запустить DDoS-атаку через наводнение сайта запросами. Как же эти ботнеты подпадают под власть своих злых повелителей? Все дело во вредоносном ПО, устанавливаемом на компьютере, когда пользователи заходят на зараженный сайт или загружают зараженное сообщение. Зачастую они даже не подозревают, что их устройство было захвачено.

Вы задаетесь вопросом, что такого особенного было в DDoS-атаке на Dyn? Использованный при атаке ботнет не был армией компьютеров или даже просто мобильных устройств, которые ожидаешь увидеть в легионе зомби, ведомом хакером. Вместо этого киберпреступники

взломали обычные бытовые устройства. Среди солдат ботнета, ударивших по Dyn, были радионяни, камеры наблюдения и цифровые видеорегистраторы. Чтобы взять под контроль эти подключенные устройства, хакеры использовали слабые заводские пароли. Ни одному пользователю даже не пришлось загружать вредоносное ПО, не подозревая об этом. В данном случае потребители ничего не сделали для того, чтобы их устройства были скомпрометированы. Но они не подумали сменить стандартные пароли на своих устройствах (если предположить, что среднестатистический пользователь вообще знает, как это сделать).

В тот момент, когда рухнула сеть Dyn, интернет вещей превратился в интернет терроризма. И, чтобы вы уж точно не поверили, будто эта атака была случайностью, примите во внимание еще один пугающий факт: ботнет, который лишил Dyn жизнеспособности, активно набирал участников для своей следующей атаки через несколько месяцев после инцидента. В мире, где мы постоянно на связи, в распоряжении хакеров оказываются миллиарды подключенных устройств, просто ожидающих следующей команды от своего нового предводителя.

DDoS-атака на Dyn открыла нам глаза на новую реалию: цели атак стали их орудиями. Теперь нам нужно защищаться от того, что мы защищали раньше. Точно так же, как данными можно манипулировать, чтобы обмануть нас, эти безобидные подключенные устройства, облегчающие нам жизнь и дома, и на работе, можно направить против нас, нанеся ущерб цифровой инфраструктуре, от которой зависим и мы, и они. Киберугрозы сегодня настолько распространены, что их целью может стать каждое подключенное устройство, каждый бит информации, которые мы воспринимаем как должное.

История с Dyn доказала, что изобретательные хакеры могут использовать для своих новых атак любые подключенные устройства или сервисы. Когда преступники проникли в дома через самые обычные бытовые приборы, кибербезопасность оказалась в числе главных вопросов при разработке продуктов.

Возьмем в качестве примера подключенные автомобили. В 2017 году Toyota, Intel и другие компании сформировали консорциум AECC (Automotive Edge Computing Consortium). Группа подсчитала, что объем данных между транспортными средствами и облаком достигнет уровня 10 экзабайт в месяц примерно к 2025 году, предположительно превысив базовый уровень 2017 года в 10 000 раз. Это в два раза больше, чем объем всех слов, сказанных людьми с начала времен [36].

Возможность вооружить интернет вещей, чтобы ослабить сеть, — это одно. Возможность вооружить восемь миллионов автономных автомобилей, которые, как ожидается, к 2025 году будут ездить по

дорогам [37], делает интернет терроризма еще более опасным. Эти подключенные транспортные средства будут зависеть от точных, поступающих в реальном времени данных, необходимых автомобилям для анализа окрестностей и соответствующей навигации. Они будут полагаться на ежемесячные 10 экзабайт данных, передаваемых между ними и облаком, — данных, которые станут настоящим сокровищем для хакеров, заинтересованных в прибыли меньше, чем в терроре.

Если вы считаете, что вашей компании не о чем беспокоиться, так как она не занимается ни опорными сетями интернета, ни подключенными автомобилями, хакеры будут только благодарны за ваше безразличие в этом вопросе. Однако пример Dyn показывает, что ваша компания может просто попасть под перекрестный огонь. Dyn не была целью атаки: ею были интернет-сервисы, поддерживаемые компанией.

Если и это не заставляет вас иначе посмотреть на дивный новый мир, в котором мы оказались, подумайте вот о чем: сколько ваших сотрудников время от времени работают из дома? В 2016 году, когда произошла атака на Dyn, в среднестатистическом доме, по данным Intel, было по десять подключенных устройств. Тогда же в компании спрогнозировали, что к 2020 году эта цифра вырастет до 50 подключенных устройств на одну семью [38]. Если оставить их незащищенными, эти устройства могут позволить хакерам скомпрометировать ваших сотрудников, пока те работают из дома, и, возможно, проникнуть в вашу компанию. Теперь зона корпоративной сети простирается до домов сотрудников.

Границы размываются. Дом и работа накладываются друг на друга. Продукты и сервисы, которыми мы пользуемся как потребители, мы используем и как работники. Интернет вещей — лишь один из примеров того, как кибербезопасность распространяется дальше, чем кажется на первый взгляд. Как и любой сотрудник, ответственный за разработку продукта или услуги, вы — ключ к тому, *чтобы остановить конвейер*, как только заметите угрозу кибербезопасности.

В данном случае от вас зависит не только компания, где вы работаете, а каждый пользователь, прямо или косвенно затронутый вашим творением.

W.I.S.D.O.M. для разработчика продуктов

Разработчики — первая линия обороны при внедрении требований кибербезопасности в каждый продукт или услугу, которые предлагает компания. В том, что касается разумных принципов разработки продукта и чек-листов (недостатка которых на рынке не наблюдается),

нет необходимости изобретать велосипед. Объединяя принципы киберзащиты с проверенными временем методиками, разработчики играют важнейшую роль в укреплении кибербезопасности своих компаний — и даже своих пользователей.

Первое, что вам следует учесть: на начальных этапах разработки крайне необходимо участие клиента. Многие компании активно просят пользователей давать обратную связь через количественные исследования, индивидуальные опросы, консультативные советы клиентов и/или другие методы. Простой, но действенный способ убедиться, что о кибербезопасности думают не в последнюю очередь, — это **прямо спрашивать клиентов об их требованиях на этом этапе разработки.**

Предположим, вы занимаетесь производством неких подключенных домашних устройств (вроде тех, которые в составе армии роботов уничтожили Dyn). Важный этап разработки — определение момента, когда потребители с наибольшей вероятностью изменят установленный по умолчанию заводской пароль. Более того: если в этот момент устранить промедление со стороны потребителя, например, заложить в интуитивно понятном приложении требование сменить пароль при установке подключенного устройства, вы тут же устраните ключевую уязвимость безопасности.

Теперь давайте представим, что вы занимаетесь разработкой ПО, и что потребители — не ваша целевая аудитория: вы ведете дела с бизнесом. Применяется тот же принцип. В данном случае, точно определив, как именно клиент будет использовать ваше приложение, вы сможете избежать необходимости исправлять ошибки в будущем. Будут ли ваши клиенты полагаться на облачное хранение или оно запрещено к использованию для данных, от которых зависит ваше приложение? Или, наоборот, вы создали продукт для работы в брандмауэре, а ваш клиент предпочитает модели «ПО как услуга»? Эти и многие другие уточняющие вопросы на этапе разработки критически важны для внедрения безопасности в самые основы вашего продукта.

Раз мы заговорили о разработках ПО, то вот еще один немаловажный пункт. Убедитесь, что безопасность является составляющей любого вашего продукта с минимально необходимым функционалом. Когда Эрик Рис [[1]], автор «Бизнеса с нуля», популяризовал такой продукт, он уловил цель любого стартапа: запустить новый продукт, который позволит команде разработчиков с наименьшими усилиями собрать максимум информации о том, как клиенты его используют. Этот процесс прекрасно подходит для облачных приложений, практически не требующих стартового капитала (поскольку многие используют общедоступную облачную

инфраструктуру, предлагаемую AWS, Azure и Google). По сути, все это позволяет быстро реагировать, выполнять итерации в разработке продукта и постоянно поддерживать обратную связь с клиентами.

Дело вот в чем: нельзя заострять внимание только на слове «минимально», игнорируя идущее за ним «необходимый». **Безопасность должна быть именно встроена, а не приляпана,** и неважно, предназначен продукт только для первопроходцев или для масс-маркета. Безопасность *обязана* быть одним из требований к минимально необходимому функционалу вашего продукта.

Кроме того, при разработке продукта задумайтесь, каким образом, где и как долго ваша компания будет использовать данные клиентов. А если к этому вас нужно подталкивать, то существуют правила, которые заставят вашу компанию заботиться о подобных вопросах. Здесь я говорю не об обязательных требованиях регулирующих органов, а об этических стандартах вашей компании. И по тому, что для вас перевесит в этом тесте — требования закона или этики, — можно будет во многом судить о вашей организации.

Так, в первой главе я рассказывала о том, как хакер изуродовал страницу McAfee в популярной соцсети. Хоть в нашем случае и не были затронуты данные клиентов, этот случай поможет мне обрисовать картину и объяснить, что я имею в виду. Поскольку никакие данные не были украдены, а системы McAfee — скомпрометированы, компания вообще не обязана была сообщать о взломе и тем более делать это через СМИ.

Однако McAfee придерживается более высоких стандартов, чем требования закона. Страницы наших сотрудников в соцсетях были изуродованы точно так же, как и страница компании: у всех появилось та же картинка, которую хакер разместил в профиле McAfee. Она несколько часов отображалось на личных страницах каждого, в чьем профиле была указана McAfee. *Есть корпоративные ценности, которых мы четко придерживаемся: открытость и прозрачность*. Хоть с точки зрения закона ничто не обязывало нас сообщать о взломе, ценности компании требовали от нас большего.

Итак, на следующий день после взлома мы опубликовали в интранете статью, где признавались в произошедшем всем сотрудникам. Мы понимали, что рискуем: история, не получившая особого внимания со стороны СМИ (так как произошла она в тихое пасхальное воскресенье), могла полыхнуть утром в понедельник, если хоть один сотрудник отправил бы ее в газеты. К счастью, этого не произошло. В конце концов, мы должны были пойти на этот риск, если

хотели поддержать ценности компании, перевесившие законные требования.

Во-первых, **при разработке любого нового продукта или услуги четко и осознанно определяйте свои требования** в том, что касается данных — придерживаясь самых высоких из них, будь то законодательные нормы или этические стандарты. Приведу еще один пример. На сегодняшний день единственным американским регулятором, выпустившим четкие указания касательно предоставления информации об атаках вымогателей, является Министерство здравоохранения и социальных служб (такой пример нормативных указаний можно расценивать как прогресс, особенно принимая во внимание, что система здравоохранения часто оказывается мишенью программ-вымогателей; однако исключительность такого регулирования также свидетельствует о том, что ситуация с вымогательством, вероятно, намного хуже, чем показывают отчеты по отрасли). Если ваша компания так же ценит прозрачность в отношениях с клиентами и требует раскрытия информации об атаке программ-вымогателей, то вы, вероятно, будете иначе смотреть на готовность рисковать при хранении данных клиентов, даже если закон в этом отношении позволяет вам больше (то есть до тех пор, пока США и другие страны не поддержат инициативу ЕС и не пересмотрят рекомендации, связанные с конфиденциальностью данных пользователей).

Во-вторых, **установите ответственность за обеспечение безопасности на каждом этапе жизненного цикла вашего продукта.** Как ваш товар или услуга будут обновляться для защиты от угроз нового типа? Какой отдел отвечает за непрерывное обслуживание и исправления, а кто — за отработку инцидентов после взлома? Как будут распределены бюджеты? Суть вы уже уловили: четко распределите в компании «плавательные дорожки» и обозначьте, где и когда должны выделяться ресурсы и приниматься решения по вопросам безопасности.

Внедрить продукт может быть не столь сложно по сравнению с тем, чтобы обеспечить его обслуживание. Только после того как первые потребители опробуют ваше творение, неизбежные проблемы с поддержкой, масштабируемостью и — да — безопасностью проявят свою отвратительную сущность. К тому времени ваше сказочное ощущение триумфа от выпуска продукта окажется лишь далеким воспоминанием. Установив контроль над всем этим еще до того, как ваш продукт попадет к первому потребителю или пользователю, вы сэкономите время и снизите будущие риски.

Это ничем не отличается от дисциплины, которую вы, вероятно, уже применяете, рассматривая другие ключевые проблемы жизненного цикла продукта. Только лишь запланировать действия при выявлении проблем с поддержкой и масштабируемостью будет недостаточно. Самый высокопоставленный функциональный лидер каждого подразделения компании (например, службы поддержки, разработки ПО или маркетинга) должен также засвидетельствовать, что требования безопасности в рамках его функции в достаточной мере встроены в продукт до того, как он будет представлен на рынке.

Наконец, вы должны **останавливать конвейер,** если на какой-либо стадии выпуска продукта обнаружите недостаточность или отсутствие безопасности. Еще важнее — активно прививать эту философию *каждому* сотруднику, прямо или косвенно вовлеченному в процесс разработки. Выполнять это требование нелегко, поскольку в бизнесе время — деньги. Еще сложнее компаниям, сотрудники которых не сосредоточены в одной точке (как на том заводе во Фримонте с более чем заметными маркерами — универсальными указателями красного, желтого и зеленого цвета, которые немедленно и однозначно показывали сотрудникам качества продукции). У многих компаний нет ни шнура, ни кнопки, с помощью которых сотрудники могли бы сразу же остановить конвейер. А в такой отрасли, как разработка ПО, и вовсе нет линии производства как таковой.

На самом деле, если мы с вами схожи, то вы работаете в организации с гибридной и растянутой в пространстве схемой расположения объектов и удаленных сотрудников. А значит, вам придется проявить изобретательность в использовании имеющихся у вас в распоряжении виртуальных инструментов, чтобы поддерживать связь, когда сотрудник остановит конвейер. Компании привыкли с помпой обставлять успешный запуск продукта, и это вполне естественно. Не теряя праздничного настроя по поводу выпуска продукта, попробуйте точно так же воспринимать как должное, когда сотрудник останавливает конвейер из-за выявления уязвимости.

Сотрудники замечают, когда в компании их ценят и признают. Это та часть культуры, которая всегда на виду и которая ясно дает понять, что важно (и неважно) для высшего руководства. Если сотрудник останавливает конвейер, найдите способ отблагодарить его. Публично отметьте его с помощью любого средства коммуникации, используемого в вашей компании (здесь вам смогут помочь сотрудники отдела персонала и маркетинга). Ваша задача — показать сотрудникам, что о безопасности вы заботитесь столь же тщательно, как и о качестве продукции. Когда они сами увидят, что вы изменили свою систему поощрения и признания, вы заметите, как все больше ответственных

сотрудников будет высказываться, если безопасность окажется под угрозой. А вы спасете свою компанию от возможных будущих финансовых и репутационных потерь или утраты интеллектуальной собственности.

***

Компании далеко ушли от беспечного, бессистемного подхода к качеству продукта. Опытные покупатели легко могут проверить качество продуктов, прежде чем принимать решение, о котором могут впоследствии пожалеть. Сегодня фирмы знают цену качества. Они измеряют его в удовлетворенности клиентов, показателях их лояльности и процентах сохранения клиентской базы. С его помощью они борются за награды «выбор потребителей» и видят его ценность в финансовых результатах.

Кибербезопасность — качество нашего поколения, но к сожалению, она недооценивается или просто не измеряется. Один мой хороший друг частенько повторяет: «Что заложено в кости, покажет себя и во плоти». Компания, в «скелете» которой заложена прочная кибербезопасность, может процветать благодаря снижению риска и финансовых потерь, большему доверию клиентов и, конечно, более высокому качеству продуктов, изначально разработанным с учетом требований кибербезопасности. Разработчики играют важнейшую роль во внедрении киберзащиты во все, чем мы пользуемся, — как те, кто мечтает о продуктах завтрашнего дня и будет создавать их.

Глава 5

Заполняя пробел

Думаю, самая большая сложность — привлечь и удержать лучшие кадры, обеспечить постоянное инвестирование приоритетных программ кибербезопасности и процессов, требующих улучшения. В общем и целом вы не можете повлиять на то, что происходит за пределами организации, не можете остановить зло. Вы должны просто подготовиться реагировать на него, и самая большая угроза здесь — бездействие. Оно нанесет ущерб. Но до тех пор, пока у вас есть эффективная программа безопасности, пока вы можете сохранять нужные кадры и работать над устранением имеющихся у вас пробелов и дыр, с вами все будет в порядке.

Директор по ИБ компании, предоставляющей медицинские услуги

У всех крупных офисов McAfee по всему миру есть общая фишка. Это не обычные бонусы современных компаний вроде тренажерных залов

или дружелюбных собак на рабочих местах (хотя все это у нас тоже есть). Это… стена.

Поскольку стены — популярная сейчас тема для обсуждения, позвольте мне пояснить. Как и у многих других компаний, у McAfee есть видение, миссия и ценности. Видение отражает наше отношение к отрасли и миру. Миссия определяет стратегию. Наша компания действует в соответствии со своими ценностями. Эти основы культуры, вероятно, не слишком отличаются от тех, которых придерживается и ваш работодатель.

Но что отличает нас от многих компаний, так это наличие обязательства. И в то время как видение, миссия и ценности отражают наши амбиции, мышление и поведение, обязательство говорит о нашем призвании.

Мы посвящаем себя защите мира от киберугроз. Не тех, которые угрожают только нашим компьютерам, но существующим во всех сферах нашего онлайн-мира.

Мы не остановимся в стремлении защитить безопасность наших семей, сообществ и государств.

Эти предложения можно увидеть на стенах крупных офисов McAfee во всем мире. А рядом с ними — подписи тысяч сотрудников компании, которые добровольно взяли на себя это обязательство. Коллеги из других подразделений, включая тех, кто работает удаленно, вероятно, поставили под этим обязательством электронную подпись при присоединении к нашей компании.

Это обязательство — квинтэссенция того, почему мы в McAfee делаем то, что делаем. Мы занимаемся кибербезопасностью. Поэтому вполне естественно, что она — источник жизненной силы нашей компании. Но даже мы не застрахованы от потенциальных нападений врагов. Ни одна компания не застрахована.

Но как вашей организации, деятельность которой, вероятно, не связана с кибербезопасностью, встроить ее в свою культуру? Я не вижу в вашем будущем стен с обязательствами и подписями преданных делу сотрудников, однако есть множество областей, на которых ваша компания может сосредоточиться, чтобы сделать безопасность значимым компонентом своей культуры.

Скорее всего, здоровая доза кибербезопасности пойдет вашей компании на пользу. Без сомнения, если все больше компаний будут принимать культуру безопасности, чаша весов в битве между хорошими и плохими парнями может склониться в пользу первых.

Поскольку наши HR-специалисты — настоящие эксперты в сфере здоровья организации и борьбы за поддержание ее культуры, я посвящаю эту главу им. Хотя они не несут исключительной

ответственности за корпоративную культуру, они оказывают на нее большее влияние, чем кто бы то ни был (кроме, пожалуй, генерального директора). Они вдохновляют нас, создавая среду, которая помогает привлечь и удержать исключительно талантливых сотрудников. Я лично наблюдала здесь, в McAfee, как влияние дальновидного руководителя отдела персонала распространялось гораздо дальше его профессиональной зоны ответственности. И HR-специалисты как участники борьбы за кибербезопасность делают гораздо больше, чем могут себе представить.

Когда слишком хорошо — это плохо

Большая часть моей карьеры до вступления в ряды борцов за кибербезопасность была связана с телекоммуникациями. Я была свидетелем безумного скачка цен на доткомы в конце 1990-х. Помню, как почти все мои знакомые собирались основать собственный дотком-стартап или присоединиться к одному из существующих. Казалось, все были обречены на успех. Помню, как те из нас, кому в то время посчастливилось работать в отрасли, шутили, что мы были частью новой золотой лихорадки. Я оказалась в нужном месте в нужное время. Мне поступало больше предложений о работе, чем я успевала отклонить. Жизнь была прекрасна.

А потом перестала быть таковой. Крах интернет-компаний на рубеже веков разрушил мечты и карьеры. Уровень безработицы резко взлетел. Многим моим друзьям пришлось тогда нелегко: они обменивали акции, которые не стоили и бумаги, на которой были напечатаны, на «розовые листы» извещений об увольнении, стоившие и того меньше.

Потребовалось несколько лет и несколько этапов сокращения сотрудников, чтобы впавшая в состояние хаоса телекоммуникационная отрасль медленно, но пришла в равновесие. И практически нулевой уровень безработицы в данной сфере на заре тысячелетия теперь напоминает тем из нас, кто пережил все это и обзавелся «шрамами», что «слишком хорошо» может быть очень плохо.

Перенесемся вперед почти на 15 лет, когда я пришла в McAfee и индустрию кибербезопасности. Конечно, я знала, в какой сфере работает компания, и ее призвание было мне близко. Я хотела, чтобы 60+ часов в неделю, которые я отдавала своей карьере, были вложены во что-то значимое. Спасение жизней казалось мне хорошим делом.

Настолько хорошим, что вскоре я поняла: мы не можем нанимать нужных людей достаточно быстро. Глобальная нехватка талантов в отрасли вернула меня в те дни, когда безработица в ней практически

отсутствовала. Хотя кандидатов на должности в сфере кибербезопасности привлекала гарантия постоянной занятости, последствия нулевого уровня безработицы оказались даже хуже тех, с которыми мы столкнулись годы назад.

Причина в том, что сейчас на карту было поставлено гораздо больше. Тогда, в 90-е, во время последнего бума доткомов закрытие вакансий вряд ли было вопросом жизни и смерти. Некоторым стартапам, возможно, было труднее привлечь к работе талантливых специалистов, но давайте будем реалистами. Что на самом деле было на кону?

Возможно, нам нужно было подождать несколько лет, чтобы потенциал интернета догнал собственный хайп, чтобы воплотилась в жизнь экономика приложений, которую сегодня мы знаем и любим. В сфере службы доставки продуктов и зоотоваров было несколько фальстартов. К счастью, существовало и множество жизнеспособных вариантов — даже в то время, когда мы ждали, пока электронная коммерция сможет доставить что угодно за пару дней (если не часов). Бум доткомов и последовавший за ним спад для большинства из нас теперь — лишь отдаленные воспоминания. Мы выжили, чтобы рассказать эту историю.

Кибербезопасность — дело другое. На карту поставлены не только пропускная способность сети или классные приложения, а намного больше. Здесь речь о национальной безопасности. О компаниях, которые должны защищать интеллектуальную собственность, финансы, репутацию и многое другое. И именно в это время нам трудно заполнить рабочие места теми, кто будет нас защищать.

В отличие от телекоммуникационной отрасли, эту нехватку талантов вряд ли удастся решить за счет упадка сферы. Вряд ли случится резкий рост безработицы, при котором на рынке окажется избыток талантливых профессионалов в области кибербезопасности. В ряды наших врагов вступают все новые злоумышленники. Пока не будет недостатка в киберпреступниках, не будет и избытка профессионалов в области кибербезопасности.

Такова уж наша природа. Поставщики кибербезопасности переманивают друг у друга талантливых сотрудников: им проще заплатить больше тому, кто уже получил образование в отрасли, чем пытаться выбрать из практически обнулившегося списка кандидатов на рынке. Частные предприятия «ходят» по одному и тому же замкнутому кругу талантов. А государственному сектору, как правило, наиболее нуждающемуся в защите (это наша национальная безопасность!), остается соперничать на этом высоко конкурентном рынке, обладая самыми низкими возможностями оплаты труда.

Спрос на профессионалов в области кибербезопасности намного превышает предложение. И этот разрыв затрагивает всех нас.

Что еще хуже, наблюдается недостаток разнообразия в нанимаемых кадрах. Женщины и представители меньшинств занимают здесь крайне мало должностей. Даже если вы не из тех, кто выступает за разнообразие в коллективе, эта проблема выходит за рамки политических или идеологических принципов. Неутешительная реальность такова, что на рынке труда не хватает квалифицированных кадров, и для решения этой проблемы хороши *все* средства. Отсеивание кандидата по гендеру или принадлежности к меньшинствам работает против всех нас, значительно сокращая список доступных нам талантов в области кибербезопасности.

Так было не всегда

Весьма заманчиво определить проблему как слишком сложную, чтобы ее решить. Проще отложить дело в сторону и забыть о нем, чем немедленно начать разбираться с нехваткой специалистов в области кибербезопасности. Особенно если учесть, с чем мы сталкиваемся.

- В течение ближайших лет количество вакансий в сфере кибербезопасности во всем мире вырастет до нескольких миллионов.
- По данным источника, женщины занимают от 11 до 20% от общего числа сотрудников сферы кибербезопасности [39]. Даже если принимать во внимание бóльшую цифру, она все равно гораздо меньше показателя по рынку, где женщины составляют половину рабочей силы.
- По представителям меньшинств статистика еще хуже. Среди профессионалов сферы кибербезопасности их всего 5% [40] — против практически трети сотрудников в целом по Америке.

Возможно, проблема не решаема? Может быть, женщины и меньшинства просто не хотят работать в сфере кибербезопасности? Или они не созданы для подобной работы? Возможно ли, что индустрия кибербезопасности обречена на отсутствие разнообразия и присущих ему преимуществ?

Нет, если ее судьбу определяет происхождение: ведь первым программистом была женщина. Создание первой в истории компьютерной программы, вычислившей алгоритм последовательности Бернулли, которая, среди прочего, объясняет, почему самолет может летать, приписывают Аде Лавлейс.

В эпоху мейнфреймов, начавшуюся в 1940-х годах, машины также программировали женщины. Мужчины же больше интересовались

созданием гигантских компьютеров, оставив скрупулезную работу по программированию коллегам-женщинам.

Во время Второй мировой войны женщины составляли 75% участников операции в особняке Блетчли-парк [41], благодаря которой удалось взломать код немецкой «Энигмы».

После войны женщины оставались основной силой в сфере кодирования в частном секторе. Именно женщина, Грейс Хоппер, создала первый компилятор, который переводил англоязычный код в биты и байты, понятные компьютеру.

Когда в 1950–60-х годах количество рабочих мест в сфере программирования резко увеличилось, женщины стали основной рабочей силой. В сфере царила меритократия: все было основано исключительно на способностях и достижениях. Компании часто выбирали программистов по результатам вступительного теста, обычно включавшего распознавание образов. У женщин и мужчин были равные шансы.

Что изменилось?

Хотя, возможно, более важный вопрос — что *не* изменилось? Женщины не потеряли в одночасье способность применять свои таланты к математике и естественным наукам в работе. А компании не решили вдруг, что мужчины лучше подходят для работы программистами.

История учит нас тому, что иногда технологии могут препятствовать прогрессу в одной области, чтобы ускорить его в другой. При появлении первых домашних персональных компьютеров в 1984 году мы вряд ли могли представить, какое влияние они окажут на нашу жизнь спустя десятилетия. С одной стороны, они сделали возможной нынешнюю эпоху цифровых технологий. С другой — непреднамеренно лишили женщин и представителей меньшинств возможности работать в сфере программирования, в том числе — в области кибербезопасности, где так необходимы специалисты [42].

Когда на рынке появились персональные компьютеры, позволить их себе, как и многие новые технологии, могли лишь состоятельные люди. Это ставило в невыгодное положение семьи из числа меньшинств, чей доход был в среднем ниже.

Университеты наводнили абитуриенты, желающие построить карьеру в области программирования — на активном рынке с блестящими перспективами, ставшем таковым во многом благодаря появлению персональных компьютеров. Возникла экономическая гонка спроса и предложения. Университеты не могли удовлетворить запросы всех желающих, включая женщин и представителей меньшинств. Они стали усложнять учебную программу, особенно во время решающего

первого года — чтобы отсеивать кандидатов без явных способностей (обычно путем повышения темпа обучения, что сказывалось на успеваемости студентов).

С ускоренной учебной программой лучше справлялись те, кто уже умел «стучать по клавиатуре» и мог погрузиться в изучение внутренней работы компьютера. Иными словами, владельцы домашних ПК — белые мужчины.

А что же женщины из этих семей? С чего бы маленькой девочке интересоваться имеющимся в семье компьютером меньше, чем ее брату?

Вспомните середину и конец 1980-х годов, когда подростковая культура хлынула на большой экран Голливуда. Вы вспомните такие классические поп-ленты, как «Месть полудурков», «Ох уж эта наука!» и «Военные игры». Кто главные герои этих кассовых хитов? Сформированный Голливудом стереотип симпатичного ботаника — точнее, белого ботаника.

Компьютеры и управляющие ими языки программирования были отданы в ведение парней [43]. Мы, девочки-подростки того времени, перестали представлять себя в этой профессии, созданной, казалось, исключительно для мужчин. Есть поговорка, которая поражает меня как женщину: «Если она не может видеть ее, она не может быть ею». А женский архетип, который в свое время дал жару в программировании — благодаря Аде Лавлейс, Грейс Хоппер и женщинам из Блетчли-Парка, — вычеркнули практически из всех блокбастеров, прославлявших в то время компьютерную технику.

Этот краткий исторический экскурс я провела не для того, чтобы кого-то обвинить. На самом деле я благодарна за то, что у меня есть компьютер, с помощью которого я могу писать эту книгу. Я очень рада, что у нас есть талантливые программисты — и мужчины, и женщины, — воплотившие в жизнь многие инновации, которыми мы сегодня наслаждаемся. Я поклонница фильмов 1980-х, сделавших компьютеры частью нашей поп-культуры. И я нисколько не умаляю заслуг бесчисленных новаторов — и мужчин, и женщин, — прокладывавших путь в будущее, которое мы в итоге завоевали.

Я просто хочу увеличить количество квалифицированных кадров в области киберзащиты, потому что нехватка специалистов — еще одна опасность для нас; еще одна угроза нашей цифровой свободе. Без них мы, безусловно, не сможем обойтись.

Те, кто не извлекает уроков из истории, обречены повторять ее. Мы можем многое почерпнуть из прошлого, чтобы изменить траекторию нашего движения в будущем и подняться выше нулевого уровня безработицы в сфере кибербезопасности (я понимаю, это странное

стремление, но надеюсь, ясно, что небольшой избыток рабочей силы гораздо лучше бесконечной нехватки талантов). Как рекрутеры организаций, специалисты по персоналу оказывают значительную помощь своим компаниям и индустрии кибербезопасности в целом, заполняя этот пробел.

W.I.S.D.O.M. для специалистов по персоналу

Нам нужно принять два факта. Во-первых, нам отчаянно не хватает специалистов в области кибербезопасности и в ближайшее время ситуация не изменится. Во-вторых, поскольку нам не хватает кандидатов для закрытия вакансий, каждому сотруднику необходимо «взяться за оружие» для вступления в битву и вносить максимальный вклад в укрепление защиты своей компании.

Две стороны одной медали — набор сотрудников и зачисление их в команду — становятся для HR-специалистов призывом к оружию. Они могут помочь организациям **расширить возможности для привлечения талантливых специалистов в сфере кибербезопасности**. Это не тот случай, когда можно позволить предрассудкам победить. Для борьбы нам нужны все силы — мужчины и женщины, представители меньшинств, искусство и наука. До этого момента наша отрасль была настолько сосредоточена на STEM-подходе (наука, технология, инженерия и математика), что мы забыли о STEAM-подходе (наука, технология, инженерия, искусство и математика). Кибербезопасность — это не только техническая, но и психологическая борьба (битва может вестись на обоих фронтах). Она требует и «мягких», и «жестких» навыков. В ней тренируется и креативность, и способность решать проблемы.

Пересмотрите собственные объявления о вакансиях в сфере кибербезопасности и сформируйте такой баланс навыков, который расширит рынок соискателей. Это не повлияет на их квалификацию (ведь речь идет не о снижении требований). Обратитесь к истории женщин в этой индустрии — к тем временам, когда сложные математические расчеты проводились человеческими умами, а не машинами, — и вы поймете, что женщины способны справляться с этой работой не хуже мужчин. Возможно, в своих объявлениях вы обнаружите ту же предвзятость, которая была присуща университетам, ограничивавшим разнообразие студентов в 1980-х годах. Если найдете, *искорените* ее безжалостно.

Но это еще не все. То же самое потребуется делать на протяжении всего процесса найма, в том числе и на интервью. К сожалению, обычные, казалось бы, вопросы на собеседовании также часто являются

источником неосознанных предрассудков. Например, распространенные поведенческие вопросы (вроде «Не могли бы вы рассказать о том времени, когда…?») заставляют естественным образом отдавать предпочтение кандидатам с большим опытом. Хотя рассказ соискателя может и не иметь отношения к сегодняшним вызовам. Фактически, исследования показывают, что такие вопросы предсказывают успех человека всего на 12% лучше, чем подброшенная монета [44].

Вместо этого предложите кандидату решить задачу. Можете попросить его рассказать, как он планирует адаптироваться к вашей компании и ее культуре после выхода на работу. Можете ознакомить его с текущей схемой выстраивания процессов и предложить внести предложения по улучшению. Вам ведь важно увидеть, как думает кандидат, а не просто выслушать истории из его прошлого.

Чтобы выявить наиболее квалифицированного кандидата, подключите к собеседованию несколько интервьюеров. Это еще одна ситуация, когда перебор хорошего может нанести вред. Например, в Google практикуют «Правило четырех» — успешно работающую модель проведения четырех интервью с кандидатами на должность. Инструмент может предсказать вероятность успеха человека в Google с вероятностью 86% [45]. Больше встреч — излишество. Меньше — недостаточно.

Неважно, сколько интервью с кандидатом потребуется вашей компании, но сделайте так, чтобы хотя бы одним из проводящих собеседование руководителей была женщина или представитель меньшинства. Мужчины и женщины по-разному отвечают на вопросы. Наличие и тех, и других в принимающей команде позволит учесть все особенности.

Еще один интересный урок от Google — вопрос, по ответу на который в компании оценивают мужчин и женщин: «Как вы оценили бы себя как программиста по шкале от 1 до 5?» Данные свидетельствуют о том, что наиболее успешные соискатели-мужчины оценивали себя на 4. По мнению Google, мужчины склонны переоценивать собственные опыт и квалификацию. А какова оценка, с наибольшей вероятностью предсказывающая успех кандидатов-женщин? Абсолютная 5 — в Google считают, что женщины более сдержанны и скромны [46]. (Конечно, теперь Google придется придумывать другие предсказывающие успех вопросы для собеседований, ведь их секрет раскрыт!)

Именно поэтому McAfee практикует групповые собеседования для большинства должностей. В числе интервьюеров всегда присутствует или женщина, или представитель меньшинства — чтобы сразу обозначить разнообразие, к которому мы стремимся.

Наконец, избавьтесь от предрассудков, заставляющих вашу компанию искать профессионалов только с опытом работы в сфере кибербезопасности. Их на рынке недостаточно. Мы не можем непрестанно переманивать друг у друга талантливых сотрудников, до бесконечности повышая их заработную плату. Поэтому избавьтесь от вопросов, которые настраивают вашу компанию против кандидатов с различной квалификацией. Например, просьба рассказать о последних интересных инновациях в сфере кибербезопасности поставит в невыгодное положение тех, у кого меньше практического опыта (как наглядно показывает нам история ПК). Убедитесь, что ваши вопросы квалифицированным кандидатам соответствуют STEAM-подходу.

Я пришла в McAfee, не имея ни малейшего опыта в области кибербезопасности. Через полгода я стала соавтором книги, посвященной этой теме. Я не преуменьшаю сложность отрасли. Я говорю лишь, что опытом можно делиться. Ищите кандидатов с техническими навыками в других областях. Вы легко найдете сферы, например, телекоммуникации, которые не страдают от нулевого уровня безработицы. Технология допускает приливы и отливы сотрудников на различных рынках труда. Откройте двери компании для квалифицированных кадров со смежной специализацией вне зависимости от того, есть ли у них опыт в области кибербезопасности.

Кроме того, вы можете использовать различные инструменты для встраивания кибербезопасности в повседневную работу сотрудников, не перегружая их. Обратитесь **к ценностям вашей компании** — тем стандартам поведения и принципам, приверженности которым вы ожидаете от сотрудников, — и **определите, в какую из них вы можете добавить одно слово, чтобы существенно изменить ее значение: *безопасность***.

Например, исследуя моего предыдущего работодателя, Verizon, я обнаружила, что на момент написания этой книги на сайте компании было размещено впечатляющее кредо. Давайте посмотрим, как вставка всего одного слова может сделать текст глубже без ущерба для первоначального смысла (выделено мной, для усиления акцентов):

У нас есть работа, потому что клиенты ценят качество наших услуг связи.

*Мы обеспечиваем высочайшее качество обслуживания клиентов с помощью наших продуктов и действий. Все, что мы делаем, строится на надежных системах, сети и процессах. Качество, надежность и **безопасность** поставляемой нами продукции имеют первостепенное значение. Клиенты платят нам за предоставление услуг, на которые могут положиться.*

Одно слово может изменить масштаб, не меняя цели. Теперь это не игра в киберлотерею. Но есть ценности и принципы, которым безопасность просто не подходит. Не пытайтесь вставить квадратный предмет в круглое отверстие. Вот отличный пример от Verizon:
Мы знаем, что командная работа позволяет нам лучше и быстрее обслуживать клиентов.
Мы приветствуем разнообразие и личное развитие не только потому, что это правильно, но и потому, что это разумный подход к бизнесу. Нами движет не эго, а достижения. Мы выполняем свои обязательства друг перед другом и перед клиентами. Наше слово — гарант. Мы уважаем и доверяем друг другу, общаемся открыто, прямо и откровенно, поскольку любой другой способ — пустая трата времени. Мы высказываем свое мнение и конструктивно выражаем несогласие, а затем вместе действуем по общему плану. Любой из нас может поделиться мнением или идеей, а также выслушать и оценить чужое чужую точку зрения, независимо от должности того, кто ее озвучивает. Идеи живут и умирают, будучи оцененными по достоинству, а не исходя из того, где были придуманы.
Мне нравится этот отрывок из кредо Verizon. Но, как я ни старалась, не смогла органично встроить слово «безопасность» в эту красивую формулировку.

Это нормально. Хоть вы не впишете безопасность в большинство ценностей компании, в которых ей не место, вам, скорее всего, удастся найти хотя бы одну, где это возможно. Если ваши ценности — это не просто красивый текст на обороте бейджей сотрудников, то вы начнете закладывать безопасность в основу своей компании, искореняя поведение, противоречащее ей, — и внедряя соответствующее.

Затем оцените собственные **программы поощрения и признания успеха**, чтобы найти в них место для достижений в области кибербезопасности. С первыми все просто и ясно. Проявите немного любви к вашей команде, отвечающей за кибербезопасность. Как я уже писала во второй главе, она слишком долго оставалась в тени. Выведите ее на свет.

Как? Предоставьте своему директору по ИБ возможность высказываться на собраниях компании. Ему не нужно присутствовать на каждом мероприятии, но вы можете рассказать о достижениях его команды более широкому кругу сотрудников, чтобы они оценили масштабность атак и важность обеспечения кибербезопасности. Помимо вовлечения в борьбу большего числа новобранцев, важно признавать заслуги вашей команды по кибербезопасности, что может снизить высокую текучесть кадров (из-за нулевого уровня безработицы).

Затем включите тему кибербезопасности в программы поощрений сотрудников. В предыдущей главе я упоминала о том, как важно остановить производство нового продукта или услуги, если их безопасность не обеспечена должным образом. Используйте внутренние платформы компании, чтобы публично выносить благодарность сотрудникам — и не только из сферы кибербезопасности — за открытое высказывание обоснованных опасений по поводу безопасности продуктов и услуг, выходящих на рынок.

А теперь пора обратиться к проблеме, которую каждый замечает, но все боятся озвучить. До настоящего момента мы говорили о сотрудниках как о людях с добрыми намерениями, которые в плане кибербезопасности стремятся действовать во благо своих компаний, но, возможно, не обладают достаточными знаниями. Во многом это соответствует действительности.

Но среди ваших коллег есть и те, кто не хочет поступать правильно. И они не просто апатично наблюдают за битвой за кибербезопасность. Они — злонамеренные инсайдеры, стремящиеся причинить вашей организации вред и/или получить личную прибыль за ее счет. Согласно отчету Verizon, вредоносные инсайдеры осуществляют более 10% всех взломов [47].

Вредоносные инсайдеры — самые коварные враги компаний. Во-первых, организации не желают навязывать сотрудникам контроль со стороны «Большого брата» — и на то есть веские причины. Несмотря на озабоченность конфиденциальностью собственных данных, работодатели не хотят относиться к каждому сотруднику как к потенциальному злоумышленнику, отдавая предпочтение культуре, в которой доверие существует по умолчанию, а не заслуживается с течением времени.

Тем не менее, плохие парни, работающие в вашей компании, — это реальность. И как организации распознать внутреннюю угрозу? У команды, занимающейся кибербезопасностью, есть технологии для выявления аномального поведения. Но сами по себе они — гораздо более слабая защита, чем сочетание технологий и людей, работающих вместе. И вот тут специалисты по персоналу могут помочь в создании средств контроля за сотрудниками для выявления злоумышленников.

Во-первых, совместно с директором по ИБ определите, кто из работников имеет наиболее полный доступ к самым ценным активам компании. У вашего руководителя по информационной безопасности уже должна быть классификация рисков для самой ценной собственности вашей организации — интеллектуального наследия, производственных мощностей, конфиденциальных баз данных и так далее. Определите круг сотрудников с привилегированным доступом к

этим активам. Вместе с менеджером по найму и вашей службой безопасности выясните, какой уровень требуется этим коллегам для эффективного выполнения работы. Периодически пересматривайте список: возможно, изменения в деятельности коллег позволят вам ограничить их права доступа.

Во время проверки эффективности создайте список сотрудников, которые потенциально могут уйти из компании, и сравните их имена с теми, у кого есть привилегированный доступ, убедившись, что юридическая служба соблюдает требования по конфиденциальности сотрудников. Регулярно устанавливая и контролируя права доступа, вы защищаете свою компанию от тех, кому они больше не нужны (или, возможно, никогда и не требовались).

Обратите внимание: гигиена доступа защищает вашу компанию не только от внутренних злоумышленников, но и от внешних. Если бы McAfee соблюдала ее, мы бы вовремя лишили сотрудницу агентства (по сути, «внешнего инсайдера» нашей команды) административного доступа к нашей странице в социальных сетях и предотвратили бы взлом, описанный в первой главе.

Выделите в ваших программах поощрения и признания сотрудников место информаторам. Это выходит за рамки государственных программ, которые защищают и стимулируют подобных людей. Разработайте конфиденциальную программу, с помощью которой сотрудники смогут сообщать о подозрительном поведении. Ясно, что это сверхмера, поскольку вы не хотите создать в компании культуру недоверия. Но если вы позволите коллегам высказаться о том, что им не нравится, вы задействуете одно из самых мощных орудий — ваш собственный штат — для выявления сотрудников-мошенников.

Показательный пример: некоторое время назад McAfee перенаправила потоки инвестиций, чтобы они более точно отвечали потребностям наших клиентов и рынка. Такие решения никогда не даются компании легко, особенно в подобных случаях — когда действия затрагивают сотрудников.

Менеджер из моей команды переслал мне письмо с просьбой о помощи. Одного из сотрудников, на котором отразились наши действия, подслушали во время подозрительного телефонного разговора. В нем он заявил, что теперь, когда их «распустили», они уж точно могут рассказать, над чем McAfee работала в последние месяцы. (Надо упомянуть, что этот сотрудник знал о готовившемся к выпуску продукте).

Услышав это, обеспокоенный коллега решил, что лучше всего рассказать обо всем менеджеру в электронном письме. Благодаря этому мы смогли вмешаться, напомнив уходящему сотруднику о требованиях

конфиденциальности (при этом не раскрывая имени разоблачителя). И мы смогли принять другие решения для внесения изменений в первоначальный график запуска упомянутого продукта.

Поскольку уходящий сотрудник не использовал системы компании для передачи или эксфильтрации информации, эта угроза могла ускользнуть от внимания отдела кибербезопасности McAfee. Лишь один сотрудник слышал телефонный разговор, и в его обязанности не входило сообщать о нем. Но человек это сделал. И я искренне благодарна за его заботу о компании. **Найдите для добросовестных сотрудников конфиденциальный, безопасный способ подать вам сигнал, когда они видят что-то сомнительное. И вознаграждайте их за это соответствующим образом.**

Наконец, определите, какие ключевые показатели эффективности (KPI) вашей компании связаны с кибербезопасностью. **У каждого члена руководства должен быть как минимум один KPI по кибербезопасности.**

Это не должно вызвать сложности. В конце концов, эта книга демонстрирует, как кибербезопасность пронизывает множество функциональных областей компании, и каждый сотрудник может сыграть в ней свою роль. Найдите несколько примеров и внедрите хотя бы один значимый KPI по кибербезопасности для каждого директора. Он передаст соответствующие указания в области кибербезопасности тем, кто за них отвечает. Они, в свою очередь, распределят ответственность между участниками своих команд. За счет такого «эффекта водопада» кибербезопасность в конечном итоге пропитает каждую функцию вашей компании на всех уровнях.

***

Эта книга посвящена формированию культуры кибербезопасности на всех уровнях организации. Культуру нельзя подавить. Она распространяется повсеместно и органично. Лучшее, что может сделать менеджмент, — обеспечить оптимальную почву для процветания великой культуры. А это значит, что сотрудники должны помнить о видении, миссии и ценностях, ведущих вашу компанию вперед. Это требует подбора подходящих специалистов, соответствующих ценностям компании и стремящихся к взаимному успеху. И это влечет за собой наличие программ поощрения и признания и четко согласованных показателей, которые гарантируют общее движение в едином направлении.

Как самые рьяные приверженцы корпоративной культуры, специалисты по персоналу должны сыграть значительную роль в

высаживании семян кибербезопасности. За вами — главная партия в решении проблемы нехватки специалистов в отрасли кибербезопасности, не говоря уже о вашей компании. Устраняя бессознательную предвзятость, ограничивающую нашу коллективную способность находить и привлекать исключительно квалифицированные кадры, и создавая атмосферу, в которой каждый сотрудник станет участником битвы, HR-специалист может закрыть пробел в кибербезопасности для всех нас.

Глава 6

Удача благоволит подготовленным

У нас есть программа, которая запускается, если на нас совершают кибератаку. Так что нам не нужно выходить на свет и сообщать что-то прессе до того, как мы полностью поймем, что случилось, откуда пришла угроза и что мы планируем с ней делать. Мы еще не заходили так далеко. Все зависит от масштаба утечки данных и серьезности проблемы.

Директор по маркетингу и продажам туристической компании

Друг моего друга знает одного парня, который по работе отправился в Лас-Вегас. Как-то вечером он отправился в бар и выпил несколько коктейлей с дружелюбным незнакомцем. На следующее утро он проснулся от мучительной боли в пояснице в ванной, полной льда. Он заметил рядом телефон и записку, в которой говорилось: «Позвони в службу спасения. Тебе удалили почку хирургическим путем». Он выжил и может лично рассказывать эту историю, но теперь у него на одну почку меньше. Будьте осторожны: существует подпольный рынок, на котором продают органы ничего не подозревавших деловых путешественников и туристов.

Возможно, вы слышали подобные истории от друзей ваших друзей. Но их события могли происходить не в Лас-Вегасе, а в Европе. Или в Южной Америке. Кто же знал, что черный рынок органов столь обширен?

На самом деле он, конечно, не таков. Этот современный миф зародился в поздние 1990-е, и хотя сегодня его абсурдность заставляет нас закатывать глаза, помню, какая дрожь пробрала меня (до самых почек!), когда я услышала об этом ужасе впервые. И я была не одинока.

30 января 1997 года, после того, как полицейское управление Нового Орлеана завалило заявками от не в меру осторожных путешественников, собиравшихся посетить город в Марди Гра [[2]], стражи порядка опубликовали следующее заявление:

«За последние шесть месяцев полицейское управление получило от корпораций и компаний Соединенных Штатов множество запросов с предупреждениями путешественников о хорошо организованной преступной группировке, действующей в Новом Орлеане. В этих запросах утверждается, что группа злоумышленников напаивает путешественников алкоголем до потери сознания, а затем вырезает у них почки.
После тщательного расследования управление полиции Нового Орлеана установило, что все подозрения ***АБСОЛЮТНО БЕСПОЧВЕННЫ И БЕЗОСНОВАТЕЛЬНЫ.*** *Сведения, тиражируемые в интернете, являются* ***ЛОЖНЫМИ*** *и могут нарушать уголовное законодательство в отношении распространения ошибочной и вводящей в заблуждение информации» [48].*
Меня очаровывают городские легенды. Как маркетолог, я являюсь одним из их рассказчиков. Городские легенды — это уникальные истории, искры которых быстро превращаются в пламя. И как оказалось, у самых успешных из них есть отличительные характеристики.

У них, как правило, есть мораль, например: «Остерегайтесь незнакомцев, предлагающих вам алкоголь в баре». Они опираются на злободневные социальные страхи. И обычно они приходят от «друзей друзей». Иными словами, источник или достоверность таких историй отследить невозможно, и, распространяя их, люди будут наполнять их все новыми подробностями.

Меня поражает сходство между успешной городской легендой и информацией о взломе, попавшей в заголовки газет. Подобно первым, новости о втором распространяются быстро. Детали взлома — кто и как его произвел — обычно появляются медленно, заставляя людей заполнять пробелы собственными предположениями, как это делают «друзья друзей» в фольклорных сказках.

У взломов и современных мифов есть еще кое-что общее: они обращаются к очень могущественной эмоции — страху. В чем же его сила? Он напрямую связан с нашим инстинктом самосохранения. Страх и гнев — «горячие» эмоции — мы переживаем очень интенсивно. Человеческое тело тысячелетиями училось тому, чтобы быстро реагировать на подобное — и сохранять нам жизнь. И напротив: чтобы ощутить «холодные» эмоции — радость или любовь, например — нам требуется больше времени, поскольку выживание здесь и сейчас зависит от того, насколько сильно мы сможем приглушить эти чувства [49].

Фактически единственное заметное отличие городских легенд от взломов заключается в том, что последние реальны. Восстановить

контроль над нарративами вашей компании, сохраняя прозрачность и честность на протяжении всего этого процесса, — как минимум непростая задача для маркетологов и специалистов по связям с общественностью. Поле PR-битвы усеивает огромное количество примеров того, как компании неправильно выстраивали коммуникацию после взлома.

Как главные хранители репутации бренда, мои коллеги из маркетинга и внешних коммуникаций в случае следующего взлома должны быть готовы отреагировать на него (и быстро!).

Взлом!

В 2014 году, уходя с поста генерального директора The Home Depot, Фрэнк Блейк оставлял после себя семилетнее наследие высоких бизнес-показателей и культуры отзывчивого руководства. Как и многие другие первые лица, за время пребывания в должности Блейк сталкивался с разными серьезными испытаниями. В 2007 году, когда он взял бразды правления в свои руки, жилищный кризис только разгорался. Падала не только стоимость акций, но и моральный дух команды: ее перестала устраивать сформировавшаяся на тот момент вертикальная структура организации.

Приступив к работе, Блейк взялся за основы. Он приостановил открытие новых магазинов, а вместо них начал открывать склады, перемещая товары ближе к существующим торговым точкам. Он сосредоточился на прибыльности и мерчандайзинге. Он закрыл убыточные подразделения и каналы.

В то же время он привнес южное очарование в культуру гигантского ритейла. По воскресеньям Блейк от руки писал сотни именных благодарственных записок достойным сотрудникам — знак внимания, который он перенял от тогдашнего вице-президента Джорджа Буша, когда работал заместителем его советника.

Несколько лет усиленного внимания полностью преобразили The Home Depot. За время руководства Блейка — с 2007 года по август 2014-го — стоимость акций компании возросла вдвое.

И вот, всего через 12 дней после объявления о своем будущем уходе с поста генерального директора Блейк взял заслуженный выходной в День труда и, будучи трудоголиком, в то воскресенье писал рукописные благодарственные письма. Как он любил повторять: «Вы получаете то, чего заслуживаете. Вы получаете то, что прославляете» [50].

Но выходной продлился недолго. Следующим утром Блейку позвонил главный советник его компании. Похоже, произошел взлом их компьютерных систем.

Блейк еще не знал всех подробностей, но понимал: финансовое благополучие и репутация его компании находились под угрозой. В последние несколько месяцев своей работы Блейк столкнулся с кризисом, который не только ставил под угрозу его компанию, но и запятнал безупречную репутацию генерального директора.

Мы знаем, как закончилась эта история: были украдены данные 56 миллионов дебетовых и кредитных карт The Home Depot. Но уникальной эту историю делает не сам взлом, а реакция компании. Критики и лидеры мнений сходятся в одном: пример компании может многому нас научить.

На фоне того, что рассказы о громких взломах регулярно попадали в новости, The Home Depot удалось выделиться — в хорошем смысле. Блейк не стал скрывать информацию: он взял на себя ответственность.

Он не затаился до тех пор, пока не выяснил все подробности. И не переложил проблему на преемника — чтобы уже он выплывал или тонул. (Любой из этих вариантов мог бы выбрать кто-то с более слабым характером).

Вместо этого Блейк принял самое неожиданное решение. Он публично сообщил о взломе еще до того, как его компания полностью разобралась, что происходит. Он принес извинения за инцидент прежде, чем окончательно выяснил, кто виновен. Он сообщил всем клиентам, что ответственность за любые мошеннические платежи будет лежать на его компании, и предложил провести бесплатный кредитный мониторинг до того, как узнал полный размер ущерба.

И хотя компания не была избавлена от коллективного иска, она избежала потенциально гигантских штрафных убытков — во многом благодаря сплоченности Блейка и его команды руководителей. Как пояснил судья в своем решении:

«Настоящими злодеями в этом деле были хакеры, похитившие данные. После обнаружения утечки не было сокрытия: The Home Depot сделала все, чтобы исправить ситуацию, и отреагировала как добропорядочный гражданин. Нет никаких оснований полагать, что организации необходимо изменить линию поведения или что она заслуживает этого. Пакет возмещающих льгот, добровольно предложенный The Home Depot клиентам, превосходит размер прибыли от коллективных исков» [51].

В итоге пока другие компании, пострадавшие от взломов в то время, общественность высмеивала за неумело выстроенные коммуникативные стратегии, The Home Depot хвалили за честность.

А как же безупречное наследие Блейка? Удивительно, но эта ситуация только сыграла в его пользу. В конце концов, как часто компания *открыто обращается* к общественности после взлома?

Хакерам не удалось испортить репутацию The Home Depot. Согласно корпоративным исследованиям потребительского мнения, во время пребывания Блейка у руля компании около 44% пользователей готовы были уверенно рекомендовать ее услуги другим людям [52].

The Home Depot не позволила взлому сломить себя. Компания контролировала свою коммуникацию, не оставляя «друзьям друзей» шансов додумать детали. Они сыграли на расширении возможностей, а не на страхе.

Готовясь к битве

Хотя реакция The Home Depot легендарна, сам взлом — история не уникальная. За то время, пока вы читаете эту главу, в мире было потеряно или украдено более 30 000 записей данных. Согласно индексу критичности утечек данных (Breach Level Index), каждую секунду взламываются 72 записи.

Время никогда не бывает на стороне тех, кому приходится реагировать на кризис. Но после взлома оно работает против вашей компании сразу на двух фронтах. Во-первых, для обнаружения нарушения необходимо время, которое в отрасли называют «длиной клика». Согласно данным Ponemon Institute, в 2018 году средняя «длина клика» составляла 197 дней, то есть киберпреступникам удавалось, не обнаруживая себя, рыться в системах взломанной компании более шести месяцев [53]. (А после ей требовалось в среднем еще 69 дней для устранения нарушения [54]).

Во-вторых, необходимо время для уведомления всех заинтересованных лиц. Компаниям, как правило, трудно справиться с этой задачей, так как расследования кибератак редко проходят легко. Международная ассоциация профессионалов в области конфиденциальности провела в 2016–2017 годах исследование нарушений в области кибербезопасности за 18 месяцев. Она обнаружила, что среднее время с момента обнаружения нарушения до уведомления о нем составляет 29 дней [55]. Для сравнения: Общий регламент по защите данных требует уведомления в течение 72 часов.

Планка, несомненно, высока. Но если мы, рассказчики, усвоили хотя бы что-то за всю свою карьеру, то вот эта истина: удача благоволит подготовленным.

За десятилетия было проведено множество исследований эффективности коммуникаций в кризисных ситуациях. Выяснилось, что лучше всего работают два общих подхода [56]. Как будто Блейк и его команда взяли и разыграли сценарий, над которым ученые работали десятилетиями:

1. *Успешные компании выступают с заявлениями рано и часто*. При появлении плохих новостей ваша компания предстает перед судом общественного мнения. Неудивительно, что первый принцип эффективных коммуникаций в кризисных ситуациях исходит от тех, кто защищает других в суде. Понятие «украденной славы» зародилось в юридической сфере и означает раскрытие своих ошибок до того, как это сделает кто-то другой (в настоящем суде подсудимый признает свою вину до вынесения обвинения; в суде общественного мнения — компания рассказывает о том, что с ней произошло, до того, как это сделают СМИ). Считается, что «украденная слава» срабатывает, поскольку если вы первым озвучите плохую новость о себе, это повысит к вам доверие и сделает откровение менее изобличающим. Ваша аудитория определит серьезность проступка, основываясь на том, кто о нем сообщил — вы или кто-то другой. В частности, люди с большей вероятностью сочтут ваше преступление менее серьезным, если вы смело о нем расскажете [57]. Прозрачность крайне высоко ценится в суде и обществе.

   Наконец, стоит быть напористым. Лучше регулярно информировать заинтересованные стороны о проблеме, чем сохранять молчание в надежде, что она просто исчезнет. И хотя агрессивный подход к коммуникациям изначально провоцировал более резкое падение стоимости акций и репутации организаций, переживавших кризис, но и первое, и второе восстанавливались у них гораздо быстрее, чем у компаний, выбравших пассивность [58].

2. *Успешные компании сосредотачивают внимание на жертвах, а не на себе*. Это сложнее, чем может показаться, поскольку требует от компании сочувствия к другим сторонам. Так как организации часто неохотно проявляют социальную благосклонность (например, публично приносят извинения из-за связанных с этим потенциальных юридических проблем), они могут не пройти «тест с лакмусовой бумажкой», обнаруживающий настоящую жертву. Обратите внимание: ориентироваться на жертву необходимо, но этого не всегда достаточно для выстраивания эффективной коммуникации в кризисных ситуациях. Если понесшие ущерб стороны полагают, что компания могла сделать больше для предотвращения кризиса, или в целом низко оценивают репутацию компании, может потребоваться нечто большее — например, выплаты компенсаций [59].
3. Многие компании в своей коммуникационной стратегии отказываются фокусироваться на жертвах и вместо этого бегут от ответственности. С этим все ясно. Замалчивание проблемы, в возникновении которой повинна организация, влечет за собой двойной удар. Мало того, что отрицание и поначалу — слабая стратегия, так еще и позже, когда тайное становится явным, возникает *новый* кризис. Единственная ситуация, при которой молчание эффективно, — когда *доподлинно известно*, что компания не является виновницей кризиса [60].

   Несмотря на то что молчанием стоит пользоваться избирательно, коммуникаторам все равно стоит принимать его во внимание. В частности в случаях, когда компания не несет прямой ответственности за взлом. Например,

ваш клиент использовал один и тот же пароль на нескольких сервисах, в том числе на предоставляемом вашей компанией. Допустим, хакеры взломали один из этих сервисов, и пароль вашего клиента был продан в даркнет. Да, ваша компания не несет за это ответственности, но как бы вы поступили в данной ситуации, винить в возникновении которой стоит кого-то другого?

Взлом «в соучастии» — это одно. А вот усиление защиты данных — совсем другое. Как становится понятно, киберпреступники уже работают не над тем, чтобы *взять* то, что им нужно, а над тем, чтобы *подделать* это. Возможно, больше всего плохим парням нужна ваша репутация. А может, хакеры желают взломать ваши корпоративные почтовые серверы и раскрыть конфиденциальные или другие частные электронные письма сотрудников, не предназначенные для широкой аудитории.

Но зачем же останавливаться на достигнутом? Злоумышленники начинают манипулировать умами своих жертв точно так же, как раньше манипулировали их денежными средствами. Возможно, когда «утечка» обнаружится, они пустят в дело еще и поддельные электронные письма. Если прибавить к ним подлинные, фейковые сообщения будет очень трудно идентифицировать и еще сложнее — объяснить. Эксперты по коммуникациям должны заранее продумать, как эффективно опровергнуть вину своей компании в фальсификации электронных писем (или других документов), которые ставят под сомнение репутацию бренда, — чтобы их компания не сыграла главную роль в новой городской легенде, созданной ее врагами.

Кибератаки — относительно новое явление для специалистов по коммуникациям, но кризисы — нет. Мы можем извлечь мудрость из проведенных исследований и применить ее в собственном плане действий.

W.I.S.D.O.M. для маркетолога / специалиста по коммуникациям

Если удача благоволит подготовленным, вам нужно разработать план действий задолго до взлома. В противном случае время сыграет не на вашей стороне. Когда будут утекать драгоценные минуты, вам меньше всего нужно, чтобы руководители компании поддавались «горячим» эмоциям — страху и гневу, которые могут затмить рациональное мышление.

Составьте многогранный коммуникационный план с явным участием руководства. Думайте при этом как руководитель по ИБ. Он должен предоставить совету директоров информацию о риске для активов. В этом упражнении не все активы равноценны. Вы должны сделать то же, что и ваша компания, в зависимости от типа и масштабов атаки. Не все атаки равноценны.

Совместно с вашим директором по ИБ выявите угрозы, с которыми ваша компания сталкивается чаще всего, — взломы веб-страниц,

программы-вымогатели, компрометация данных клиентов и сотрудников и т.д. После этого очень четко определите принципы реагирования на каждый из случаев.

- Вы уведомите общественность, даже если этого не требует закон?
- Что, если ваша компания не несет ответственности за атаку? Как это повлияет на тон и содержание вашей коммуникации?
- Когда бы вы уведомили людей? Учтите: чем раньше вы это сделаете, тем проще будет формировать общественное мнение. Результаты исследований кризисных коммуникаций показывают, что лучше всего выбрать время в пределах одного часа после инцидента.
- Кого бы вы уведомили?
- Что бы вы сообщили, если бы не обладали полной информацией (что более чем вероятно в случае взлома)?
- Что вы готовы предложить клиентам в качестве компенсации или знака сочувствия жертве (например, бесплатная защита личных данных или покрытие убытков от взлома кредитной карты)?

Попросите вашего генерального директора и высшее руководство принять участие в этом упражнении и согласовать принципы, определяющие, как, когда и о чем вы будете сообщать в зависимости от серьезности атаки.

На выполнение этого упражнения уйдут недели, если не месяцы. И поскольку велика вероятность того, что ваша компания уже взломана и просто еще не знает об этом, составление согласованного плана является вашим главным приоритетом.

Разработайте шаблоны сообщений для каждого сценария из вашего плана. Привлеките к работе юристов, чтобы каждое слово в них было взвешенным. Создайте электронные письма, веб-страницы, посты для блогов, пресс-релизы, скрипты телефонных разговоров, заявления для СМИ и другие материалы, оставляя поля для деталей — их вы заполните, когда произойдет атака. Разработайте сайты (внутренние и внешние), которые можно будет быстро запустить, чтобы оперативно сообщать на них последнюю информацию.

В своих сообщениях следует проявить сдержанность в инструкциях и тоне. Во время кризиса клиенты хотят знать, что компания заботится об их интересах, что ситуация под контролем. К сожалению, взломы редко когда дают компании возможность проявить гибкость и в том, и в другом.

Чтобы продемонстрировать, что ваша компания контролирует ситуацию, придерживайтесь в своих шаблонах следующей схемы:

- Кто пострадал?

- Какие данные и/или системы были утеряны, украдены и/или иным образом скомпрометированы?
- В течение какого периода система была взломана?
- Какие меры предосторожности необходимо предпринять заинтересованным сторонам?
- Какие действия ваша компания предпринимает для устранения проблемы и снижения риска ее повторения?

Даже если ваша компания еще не владеет всей информацией, своевременное и точное сообщение известных подробностей позволит вам перехватить инициативу.

В тональности сообщений проявите сочувствие, защищая при этом свои законные интересы — вот зачем к составлению плана на ранней стадии нужно привлечь юристов. Попросите их проверить все ваши шаблоны, и тогда в случае взлома вы будете на шаг ближе к окончательному согласованию заполненных документов.

Мы уже обсудили, как важно проявить сочувствие. Эффективность этого принципа ведения кризисных коммуникаций подтверждается и в мире утечки данных. Ponemon Institute опросил потребителей, прекративших сотрудничество с компаниями после утечки данных в 2014 году. На вопрос, что эти компании могли сделать для сохранения отношений, большее количество респондентов высказалось за искренние извинения (43%), чем за бесплатные услуги по обнаружению краж данных и кредитному мониторингу (41%) [61].

Подберите подходящие слова. Сочувствие невозможно выразить через технический жаргон или юридические фразы. Потребители почуют фальшь в извинениях за километр. Другое исследование Ponemon Institute, проведенное в 2012 году, показало, что примерно треть потребителей была недовольна объемом и излишней «бюрократичностью» полученных после взлома сообщений [62].

Разработайте пошаговый план мер для каждого сценария атаки. Валюта кибербезопасности — время. Составляйте планы соответствующе: распишите свои действия до минуты. Скорее всего, у вас не будет полной информации сразу после сообщения о взломе вашей компании.

К счастью, ваш план коммуникаций поможет понять, что и когда могут раскрыть ваши руководители. Прописывать вы его будете, пока время еще не поджимает, а значит, найдете более убедительные аргументы, доказывающие, что своевременная и частая коммуникация приносит пользу (вспомните безупречный пример The Home Depot), даже если известны еще не все факты.

В вашем поминутном расписании должно быть указано, кто отвечает за распространение сообщений и/или указаний среди

ключевых заинтересованных сторон на каждом этапе выполнения плана. Более 60% потребителей утверждают, что их удовлетворенность реакцией взломанной компании значительно повысится, если организация уведомит их немедленно [63].

Подключите к действиям сотрудников, вне зависимости от того, были ли взломаны их данные. Во время кризисов ваш штат (возможно, даже больше, чем клиенты) нуждается в уверенности в том, что их работодатель все контролирует. Сотрудники — лучшие амбассадоры бренда компании. Если вы держите их в неведении относительно деталей ситуации, они не смогут помочь вам распространить нужное сообщение и вы снова превратитесь в потенциальную жертву «друзей друзей». Активно вовлекайте сотрудников, чтобы заручиться их поддержкой и усмирить любые беспокойства. Что касается способов, подумайте, как выйти за рамки групповой электронной рассылки и объявлений в интранете. Проведите хотя бы одно общее собрание, чтобы объяснить ситуацию. Организуйте ежедневные «горячие» конференции (скажем, на 30 минут), в рамках которых будете рассказывать коллегам о последних событиях и отвечать на любые вопросы.

Практикуйтесь, практикуйтесь и еще раз практикуйтесь. Руководители по ИБ проводят «учения», имитируя атаки на свою организацию, чтобы выявить уязвимости и укрепить защиту. Директора по маркетингу должны практиковать свои антикризисные учения, чтобы проверить эффективность реагирования своей команды в соответствии с планом. Эксперты по антикризисному управлению рекомендуют делать это не реже раза в год, чтобы укрепить «мышечную память» компании.

В рамках практических занятий смоделируйте выступления представителей вашей компании перед СМИ. Вам потребуется несколько подготовленных людей, которые будут взаимодействовать с прессой в случае взлома. Убедитесь, что они владеют темой и способны отвечать на вопросы, сохраняя контроль над ситуацией. Практика поможет довести их навыки до совершенства.

Пересмотрите общий план действий в кризисной ситуации и результаты тренировок команды, чтобы убедиться в неизменности ваших главных принципов коммуникации. Найдите время проанализировать действия других компаний за период, прошедший с ваших последних «учений», чтобы учесть передовой опыт и улучшить свой план.

***

Майя Энджелоу однажды сказала: «Люди забудут ваши слова, люди забудут ваши поступки, но они никогда не забудут чувства, которые вы у них вызвали». Мы до сих пор вспоминаем о непреходящем наследии Фрэнка Блейка в области кибербезопасности, потому что его быстрые действия и гибкая реакция заставили всех нас (и пострадавших, и нет) почувствовать себя лучше, видя, что компании все еще могут поступать правильно. Своими действиями Блейк показал, что его компания заботится о клиентах. И это чувство сохранялось еще долго после его ухода с поста генерального директора.

Когда происходит взлом, удача благоволит подготовленным. Ваша компания не сможет предотвратить все атаки. Настойчивым киберпреступникам достаточно преуспеть всего один раз. И командам по маркетингу и коммуникациям необходимо молниеносно нанести ответный удар — по скоординированному, тщательно продуманному плану, который вовлечет все заинтересованные стороны, будет содержать четкие инструкции и искреннее сочувствие. Клиенты и сотрудники будут оценивать вашу компанию по ее реакции. Когда дым рассеется, они могут не вспомнить все, что вы сказали или сделали, но они наверняка не забудут, как чувствовали себя после ваших слов и действий.

Мои товарищи по маркетингу и коммуникациям, вы стоите между хакерами и репутацией своего бренда. К счастью, вы можете многое предпринять, чтобы быть во всеоружии.

Глава 7

Интересные компаньоны

По мере погружения в онлайн-среду вы становитесь все более уязвимыми. У нас есть очень надежная политика использования услуг сторонних подрядчиков и сеть мониторинга онлайн-отношений. Фактически это одна из зон моей ответственности. В нашей компании над этим работает целый отдел. У нас есть специальные опросники и разные компании-партнеры, которые время от времени проводят аудиты и оценку некоторых из наших ключевых поставщиков услуг — чтобы убедиться, что они поддерживают соответствующий уровень безопасности. Мы требуем, чтобы проверки безопасности данных наших сторонних подрядчиков проводились ежегодно. Это довольно надежный подход.

Финансовый директор компании финансовых услуг

Если вы финансовый директор компании, скорее всего, у вас есть кое-что общее с большинством хакеров — здоровая жажда прибыли. Многие враги будут солидарны с философией, которой вы, вероятно, дорожите: деньги — всему голова.

Индустрия кибербезопасности очень зря создала стереотипное представление о хакере как о парне в толстовке с капюшоном, уткнувшемся в монитор. Образ родился в 1980-х годах — именно тогда Голливуд подарил лицо хакерскому сообществу. Темная фигура одинокого волка за клавиатурой никак не соотносится с изощренными синдикатами киберпреступников, явно жаждущих прибыли.

Джонатан Лустхауз никогда не предполагал, что станет заниматься изучением киберпреступников. Его страстью было исследование религиозного насилия. Но тема его диссертации не подходила для изучения в Оксфордском университете, и Лустхаузу пришлось искать новый круг интересов.

Совершенно неожиданно для себя он нашел вдохновение в лекциях известного автора книг о киберпреступности, который в то время, когда у Лустхауза как раз истекал срок выбора новой темы, читал лекции в Оксфорде. После почти 250 интервью с агентами правоохранительных органов, специалистами по безопасности и бывшими киберпреступниками Лустхауз стал авторитетным специалистом. В своей книге Industry of anonymity: Inside the business of cybercrime [[3]](*«Индустрия анонимности: внутри бизнеса киберпреступности»)* он раскрыл настоящую изнанку этой индустрии с оборотом в $600 млрд64.

Он обнаружил, что подпольный рынок имеет много общего с рынками финансовыми, которые поддерживают здоровый и легальный бизнес и промышленность. Лустхауз обратил внимание на узкую специализацию киберпреступников. Среди них крайне мало мастеров на все руки. Напротив, как выяснил Лустхауз, большую экономическую выгоду им приносит инвестирование в торговлю данными, а в более узких сферах они склонны полагаться на других. Те из них, кто более подкован технически, создают проблемы для онлайн-среды. Другие хорошо продают, поэтому идут на подпольные рынки — чтобы там продвигать ценные предложения. Третьи сильны в организации. Они осуществляют послепродажную поддержку покупателей, которым нужна помощь в доставке «орудия» к намеченной цели (или целям).

Разделение обязанностей, принятое в самых продвинутых компаниях мира, также активно работает на даркнет. Но как киберпреступники с узкой специализацией могут доверять друг другу в плане оплаты услуг? Точно так же, как онлайн-покупатели научились доверять законным онлайн-компаниям. Они полагаются на место,

которое другие злоумышленники занимают в рейтинге опыта. Они используют форумы обратной связи, чтобы обмениваться информацией о неудачном сотрудничестве (видимо, у воров действительно есть честь).

Эти механизмы обратной связи увеличивают масштаб киберпреступности. Каждый злоумышленник может тратить меньше времени на проверку квалификации и надежности потенциальных партнеров и больше — на оттачивание своего преступного мастерства.

Рынок киберпреступлений не только имитирует законный бизнес, но и симулирует правила законного управления. Лустхауз обнаружил злоумышленников, использующих условное депонирование — удерживание средств (если не товаров) при проведении сделок доверенной третьей стороной до тех пор, пока все их условия не будут выполнены. Существует даже арбитражный суд, где каждая сторона может инициировать спор перед высокопоставленным членом сообщества, назначенным для вынесения решения. В некоторых случаях «судья» может запретить нарушителю доступ на рынок.

McAfee провела собственное исследование [65] огромного рынка киберпреступности, скрывающегося в недрах интернета. Благодаря тому, что правоохранительные органы уничтожили некоторые известные торговые площадки даркнета, киберпреступники прокачали предпринимательские навыки. Отдельные продавцы подменяют официальные маркетплейсы (которые, как правило, находятся под пристальным наблюдением органов правопорядка) собственными веб-сайтами, чтобы торговать на них своими товарами и/или услугами в даркнете. Дерзкие веб-дизайнеры становятся соучастниками преступлений: они создают скрытые торговые площадки для начинающих продавцов. Да, даже в даркнете есть слои, которые позволяют пользователям уходить еще глубже — за пределы досягаемости радаров.

Открытие «копий» — только один из путей, по которому можно пойти. Существует множество подпольных форумов, посвященных теме киберпреступности, помогающих хакерам оттачивать мастерство. Наибольшей популярностью там пользуются обсуждения утечек пользовательских данных, распространенные уязвимости, а также «сайты-свалки», на которых можно найти множество актуальных данных украденных кредитных карт.

Это — лицо киберпреступности. Этот сложный лабиринт запутанных сервисов, покупателей, продавцов и «регулирующих органов» — вот чему противостоит наша компания. Противодействовать может и ваша организация. Это нечестная игра. В даркнете нет закона Сарбейнса — Оксли (SOX). Нет Общего регламента

по защите данных, регулирующего конфиденциальность и использование информации. Нет никаких стандартов соответствия, продиктованных множеством руководящих органов. Хакеры могут кодировать в 2 часа ночи и взламывать своих жертв в 4 часа утра. Они не обязаны использовать обременительные окна тестирования, чтобы гарантировать соблюдение контроля качества.

В отличие от ваших конкурентов, которые руководствуются теми же правилами, положениями и общими бизнес-идеалами, что и ваша компания, противники не соблюдают никаких законов (кроме принятых в их сообществе). В отличие от конкурентов, стремящихся занять долю рынка, злоумышленники хотят цапнуть все, до чего могут дотянуться.

Вероятно, вам хорошо известно, что вы имеете дело с отлично скоординированным противником. Но чтобы понять, что такое кибербезопасность, давайте обратимся к тому, как финансовый отдел обычно распределяет бюджеты между отделами. Это происходит на основе сравнительных данных. И хотя вы можете найти статьи расходов на кибербезопасность, они могут ввести в заблуждение, так как настоящие критерии затрат на эту область диктуют злоумышленники. Если вы не знаете, сколько они вкладывают в исследования и разработки своих продуктов, как вы можете точно оценить необходимый бюджет на кибербезопасность?

Если нет данных сравнительного анализа, бюджеты распределяются по рентабельности инвестиций (ROI). Опять же, это непросто для профессионалов в области кибербезопасности. Как директору по ИБ доказать, что отсутствие видимых результатов — это успех? Даже если попытаться, разве финансовые руководители не оспорили бы истинность этого утверждения? Представьте следующий разговор финансового директора и руководителя по ИБ:

— Зачем нам покупать этот новый виджет безопасности?

— Потому что мы наблюдаем рекордное количество атак на компанию в этой области.

— Но какова рентабельность этих затрат?

— Что ж, есть вероятность, что нас взломают, если мы ничего не предпримем.

— То есть вы можете гарантировать, что если мы купим эту технологию, нас не взломают?

— Не совсем. Все немного сложнее.

— Давайте не будем усложнять. Какова рентабельность инвестиций?

Видите — диалог пошел по кругу. Если не считать попытки шокировать и запугать людей запутанными показателями

кибербезопасности, у директора по ИБ нет шансов ответить на вопрос: «Какова рентабельность инвестиций?».

Дело не в том, что руководители по ИБ уклоняются от ответа или не понимают концепции рентабельности инвестиций. Чтобы понять, почему на этот вопрос невозможно ответить, давайте рассмотрим несколько атак.

Чем больше все меняется…

В мае 2017 года вопросы кибербезопасности вышли на первые полосы практически всех интернет-СМИ и попали в новости по всему миру. Те, кто раньше не встречался с вирусами-вымогателями, теперь узнали о них по одному названию — WannaCry. Беспрецедентная по масштабу и скорости атака за первые несколько дней заразила более 200 000 компьютеров по всему миру, в результате чего были закрыты больницы, университеты и банки [66]. WannaCry удерживала компьютерные файлы каждой жертвы с целью получения выкупа в размере до $300 в биткойнах. Каков предполагаемый ущерб от WannaCry? Миллиарды долларов во всем мире.

Но было бы несправедливо называть WannaCry классической программой-вымогателем. Несомненно, шантаж был очевидным способом сыграть на уязвимости жертв, которым угрожала безвозвратная потеря файлов. Но именно способ «заражения» — использование свойств «червя» — делало WannaCry настолько незаметным. Не вдаваясь в технические подробности, можно сказать, что ключевое различие между «традиционными» программами-вымогателями и WannaCry заключается в том, что последняя не требует вмешательства человека. Вот почему она распространилась так быстро — не полагаясь на то, что ничего не подозревающие люди проглотят наживку. Вместо этого она использовала уже существовавшие уязвимости популярной операционной системы.

Собственный анализ WannaCry, проведенный McAfee, показал, что программу вообще нельзя квалифицировать как вымогатель. Авторы разработки вложили в нее довольно грубые возможности монетизации. Они не связали жертвы с их платежами в биткойнах, что сделало расшифровку файлов чрезвычайно сложной. Так чем же на самом деле была WannaCry? Программой-вымогателем? «Червем»? И тем и другим.

В 2018 году хакерская изобретательность снова проявилась во всей красе с выпуском Zyklon. Он представлял собой полнофункциональный пакет угроз для предприимчивых преступников: позволял красть пароли, запускать DDoS-атаки, добывать криптовалюту и многое

другое. Чем на самом деле являлся Zyklon? Криптоджекингом? DDoS? Кейлоггером? Всем вышеперечисленным.

Как показывают примеры WannaCry и Zyklon, хакеры не только сотрудничают по текущим вопросам, но и вместе создают новые «смеси» конвергентных угроз. Они объединяют старые разновидности (например, «черви») с новыми (например, программы-вымогатели). В ходе анализа подпольных форумов, проведенного McAfee, мы увидели, что киберпреступники обсуждают и те и другие. Результатом становятся изощренные угрозы, способные распространяться намного быстрее, чем раньше.

Вернемся к разговору между финансовым директором и руководителем по ИБ. Когда последний обращается к первому по вопросу дополнительного финансирования, обычно он опирается на эту реальность. Даже в середине финансового периода, уже после выделения определенного бюджета, директор по ИБ может затребовать больше средств. WannaCry не дожидалась окончания квартала, чтобы нанести ущерб. Преступников не волнует ваш бюджетный цикл.

Но если не рентабельность инвестиций является подходящим показателем для кибербезопасности, то что тогда? Управление рисками. Профессионалы сферы занимаются именно этим. Несомненно, они обладают техническими знаниями и множеством продуктов, используемых для защиты компаний от синдикатов высокоорганизованной преступности. Но если отбросить технический жаргон, все сведется к одной конкретной бизнес-цели — снижению рисков компании.

Как известно финансовым директорам, управление рисками и связанные с ним показатели в корне отличаются от более традиционных показателей рентабельности инвестиций. Я живу в Северном Техасе, в регионе, заслужившем печальное прозвище «Аллея торнадо». По сей день я испытываю перед торнадо страх. Во всем виноваты учебные сирены, которые включают для проверки в полдень первой среды каждого месяца — страшный саундтрек для фильма о войне. А может, все дело в Дороти и ее спровоцированном торнадо путешествии в страну Оз, мысль о котором пугала меня в детстве. В любом случае, я боюсь торнадо: я верила, что каждую весну в Северном Техасе они представляют угрозу для моего мирного существования. Это продолжалось, пока я не узнала, насколько безосновательны мои опасения. В прошлом году в Даллас переехал главный технический директор McAfee. Нервные коллеги, старожилы Техаса вроде меня, сразу же рассказали ему, как действовать в случае торнадо. Однако, в отличие от меня, он решил не поддаваться панике, а провести собственное исследование. И обнаружил, что за 69 лет наблюдений в

моем округе был только один торнадо уровня F3 или выше (это ураганы, способные нанести серьезный ущерб).

А теперь вернемся к управлению рисками. Проверяет ли финансовая группа рентабельность вложений в знаки-указатели, ведущие к убежищам от торнадо на территории вашего офиса, если он расположен на Аллее торнадо? Скорее всего, нет. Если вы изучите риски, которые повлечет за собой снятие этих знаков, скорее всего, они будут минимальными (опираясь на исследование нашего технического директора, предполагающего, что смертельный торнадо действительно крайне маловероятен).

Но даже если за 69 лет пройдет только один разрушительный ураган, риск все равно есть. В этом случае отказ от указателей ради экономии нескольких долларов может в итоге оказаться очень дорогостоящим решением.

С кибербезопасностью дела обстоят так же. Хотя руководители по ИБ ежедневно устраняют множество угроз (которые, вероятно, не вызовут катастрофического ущерба, но тем не менее могут повлиять на бизнес), они также должны учитывать потенциальный катастрофический (хотя и гораздо менее вероятный) риск от крупномасштабной атаки, которая на время может вывести компанию из строя. Они ходят по этому «канату» каждую минуту каждого дня.

Если финансовые директора смогут общаться с руководителями по ИБ несколько иначе, то они помогут построить мост от кибербезопасности к управлению рисками. Давайте снова представим их диалог:

— Зачем нам покупать этот новый виджет безопасности? Что мы пытаемся обезопасить?

— Он защитит наши активы, которые мы определили как стратегический ресурс компании.

— Но как узнать, что актив в опасности?

— Нам известно об уязвимости, которую могут использовать злоумышленники.

— Чем мы рискуем, если ничего не предпримем?

— Учитывая, что это актив с высокой степенью риска, последствия взлома будут означать [нарушение в работе компании, штрафы до X миллионов долларов, негативные отзывы клиентов, связанные с безопасностью, отключение критических систем или сайтов и т.д.].

— Давайте еще раз подробно обсудим последствия. Расскажите, какие последствия взлом будет иметь для нашей [финансовой, юридической, интеллектуальной собственности и/или репутации].

Задавать те же вопросы бывает полезно и в других бизнес-ситуациях, определяемых проверенной метрикой рентабельности

инвестиций. Большинство компаний, стремящихся увеличить прибыль, работают над собственным ростом. Это влечет за собой необходимость выхода на новые рынки, расширения ассортимента продукции, повышения производительности за счет новых технологий и т.д. Многие из этих бизнес-процессов соответствуют требованиям рентабельности инвестиций. Но как часто их исследуют на предмет влияния на риски компании, в частности, на наличие уязвимостей, которые могут использовать злоумышленники?

Финансовые руководители могут помочь своим организациям, задавая следующие вопросы о рисках всякий раз, когда у них на столе появляется новое бизнес-предложение:

- Как новые [рынки, внутренние технологии, продукты и т.д.] повлияют на уязвимости компании?
- Как это влияет на степень риска для стратегических активов компании?
- [Предполагая, что риск увеличивается] Какие дополнительные инвестиции (разовые и регулярные) требуются для сведения рисков к минимуму? Включены ли эти вложения в анализ рентабельности инвестиций?

Задавая эти вопросы коллегам, не связанным с кибербезопасностью, финансовые руководители и их команды могут гарантировать, что кибербезопасность — одна из приоритетных задач для стратегического роста их компаний.

…тем дольше остается неизменным

Днем они скрываются — и кормятся ночью. Они ищут кровавой пищи, чтобы выжить, вгрызаясь в свою жертву, пока та спит — поскольку ненавидят движение. Они быстро передвигаются, преодолевая три-четыре фута [[4]] в минуту, что в масштабе можно сравнить со скоростью бега среднего взрослого. Да, постельные клопы возрождаются по всему миру [67].

Эти крохотные хищники были почти побеждены после Второй мировой войны благодаря тщательной домашней гигиене и промышленной дезинсекции. В последние годы они вернулись. Оказывается, в царстве насекомых появился штамм постельных клопов, обладающий высокой устойчивостью к агрессивным пестицидам. Добавьте к этому путешественников по всему миру — невольных переносчиков этих мерзких «автостопщиков» — и вы получите эпидемию клопов, которая снова захлестнет мир.

Вот почему искоренить постельных клопов так сложно. У вас может быть самый чистый дом в мире. Вы можете неукоснительно дезинфицировать постельное белье, пижамы и любую другую одежду,

которая касается вашего спального места. Но если вам доведется заехать в отель или полететь в самолете, зараженном паразитами, достаточно будет, чтобы всего один назойливый клоп прицепился к вашему багажу и добрался до вашего жилья.

Проблема усугубляется, если вы живете в многоквартирном доме. Тут нужен только сосед через стену с более низкими стандартами гигиены — и вот у вас уже появляются нежелательные жильцы (да, эти решительные паразиты могут перемещаться сквозь стены, используя в качестве маршрутов пустоты, водопроводные трубы и электрическую проводку).

У постельных клопов такая слава, что большинство не хотят верить в собственное соседство с этими кровососами. К тому времени, как люди признают наличие проблемы, их дома уже полностью заражены. Если вам довелось переночевать в отеле или разделить стену с нечистоплотным соседом, ну, вы понимаете…

Постельные клопы — грустное напоминание о том, насколько мы зависим друг от друга. Суть не в том, чтобы обращаться за помощью к соседям, а в том, чтобы доверять их знаниям об окружающем пространстве (исследование показало, что почти 50% людей, чьи постели были заражены клопами, даже не подозревали об этом [68]) и вовремя обращаться за профессиональной помощью.

Какая прекрасная аллегория кибербезопасности. Компании не работают на островах сами по себе, а действуют в очень сложных экосистемах. Несмотря на то, что организация может практиковать разумную гигиену кибербезопасности, она должна быть уверена, что ее «соседи» — любая третья сторона, с которой она ведет бизнес и с системами которой связана, — делают то же самое. В противном случае она остается уязвимой для коварных хищников, вламывающихся в систему через «заднюю дверь». (Между прочим, взломы могут происходить и вне обширных сетей. Вспомните правила кибербезопасности и гигиены, описанные в главе 3. Все, что требуется, — это неосторожный партнер, оставивший USB-накопитель или незапароленный ноутбук с конфиденциальными файлами вашей компании без присмотра — и ваша организация под угрозой).

Десятилетия без клопов напоминают нам о том, что забытое старое снова может стать новым. Чем больше все меняется, тем дольше остается неизменным. И вот мы снова жалуемся на клопов, несмотря на все успехи в борьбе с ними.

Хотя перемены — единственная константа бизнеса, многие финансовые руководители могут быть уверены в одном: они управляют закупками своих компаний. Поскольку это в основном остается

финансовой функцией, родство финансового директора с руководителем по ИБ скоро станет намного ближе.

Подобно тому, как постельные клопы напоминают нам о том, насколько мы зависим от взаимной бдительности, связи со сторонними организациями являются дополнительными уязвимостями, которые хакеры могут использовать для нанесения вреда нашим компаниям. Рассмотрим следующие постулаты от Ponemon [69], которые отражают отрезвляющую реальность:

- 59% организаций подтверждают, что столкнулись со взломом по вине третьих лиц.
- Только 29% заявили, что узнали о взломе от самих третьих лиц.
- 76% утверждают, что количество инцидентов в сфере кибербезопасности с участием поставщиков растет, но только 46% согласны с тем, что управление рисками во взаимоотношениях с аутсорсинговыми партнерами является приоритетной задачей.
- 57% не знают, достаточны ли меры защиты поставщиков их организаций для предотвращения взлома.

Но есть и плюс: эти показатели можно улучшить. Стороннее управление безопасностью для многих организаций — понятие новое. Как показывают приведенные выше цифры, это очень важно. Ответственность за обеспечение достаточной проверки сторонних организаций на уровень кибербезопасности несут руководители финансовых служб в процессе закупки. Здесь ваш директор по ИБ поможет вам задать правильные вопросы.

Конечно, высшая степень доверия третьей стороне — это передача на аутсорсинг работы подразделения или ее части. В 2016 году компания Deloitte провела глобальное исследование, посвященное жизненному циклу аутсорсинга и его ключевым тенденциям. Сколько основных функций было передано на аутсорс? 72% организаций передают на аутсорсинг хотя бы часть функций ИТ-подразделений, а 31% планируют это сделать [70].

Когда-то передача кибербезопасности на аутсорсинг казалась абсурдной идеей. Но похоже, что эта сфера идет по стопам своих предков в области ИТ, поскольку сейчас доступ третьих сторон к защите наиболее ценных цифровых активов организации становится все более приемлемым. Конечно, глобальная нехватка специалистов по кибербезопасности только подливает масла в огонь. Вместо того чтобы яростно сражаться за профессионалов области, которых просто нет на рынке, компании предпочитают нанимать третьих лиц с необходимым опытом, чтобы хотя бы увеличить внутренние кадровые возможности.

В частности, функции Центра обеспечения безопасности, которые с наибольшей вероятностью могут быть переданы на аутсорсинг, включают тестирование проникновения (этим занимаются 75% внешних организаций), сбор и передачу разведданных об угрозах (54%) и цифровую экспертизу и проверку вредоносных программ (51%) [71].

У передачи одной или нескольких функций кибербезопасности сторонним подрядчикам есть свои плюсы. Как и в большинстве подобных случаев, компании стремятся сэкономить деньги и минимизировать первоначальные затраты, нанимая третьих лиц с необходимым пакетом услуг в сфере кибербезопасности. Организации также могут снизить риск устаревания технологий, заключив с подрядчиками соглашения о своевременном обновлении ПО. И наконец, так как подрядчики специализируются на кибербезопасности, они могут сосредоточиться на этой ключевой компетенции, позволяя своим клиентам сосредоточиться на своих.

Как и большинство тем в этой книге, эта окрашена в несколько оттенков серого. В то время как передача части функций кибербезопасности на аутсорсинг идеально подходит многим компаниям (особенно тем, у которых действуют жесткие кадровые ограничения), кибербезопасность чем-то похожа на благотворительность — она начинается дома. Передача полной ответственности за свою кибербезопасность третьей стороне — действительно рискованное дело. Своим опытом в сфере киберзащиты подрядчик компенсирует нехватку понимания уникальной среды вашей компании. Из-за этого он может пропустить в вашей среде аномалии, которые легко обнаружит специальная внутренняя группа. Поскольку поставщик услуг поддерживает нескольких клиентов (что также дает преимущество, поскольку он учитывает тенденции более широких рынков), он может уделять меньше времени потребностям вашей компании. И все это может привести к неоптимизированной политике кибербезопасности, если ваша компания полностью передает «ключи» стороннему подрядчику.

Это еще одна область, в которой финансовые руководители и их команды должны оказывать значительное влияние. Сам по себе наем внешних сотрудников — это неплохо, но для получения положительных результатов необходимо тщательно продумывать условия взаимоотношений с надежным подрядчиком. Ни одна компания не позаботится о кибербезопасности вашей организации больше, чем ваша собственная. Но это не означает отказа от кибербезопасности. Это взаимное партнерство, позволяющее использовать ключевые компетенции и дополнительный персонал для получения максимальной выгоды.

W.I.S.D.O.M для профессионалов сферы финансов

Как основные распределители ресурсов и бюджета организации, финансовые специалисты могут многое предложить культуре кибербезопасности, в частности, **помочь руководителям ИТ и их командам говорить на языке бизнеса**. Это требует отказа от формулировок, которые не соответствуют кибербезопасности — например, «окупаемость инвестиций». После того как финансовые директора избавят руководителей по ИТ от необходимости давать ответы на невозможные вопросы, команды смогут вместе определять ценность инвестиций в кибербезопасность.

Цель — максимально эффективно снизить риск. Есть ряд вопросов, которые позволят директорам по ИБ и финансовым руководителям общаться на новом уровне, например:

- Какие активы подвержены риску?
- Какова стратегическая ценность актива(-ов)?
- Каков текущий уровень уязвимости актива(-ов)?
- Каковы будут последствия взлома (финансовый ущерб, уязвимость интеллектуальной собственности, репутационные риски)?

Чтобы кибербезопасность не стала второстепенным вопросом, финансовым директорам следует обратиться к другим руководителям с просьбой предоставить информацию по следующим вопросам:

- Как новые [рынки, внутренние технологии, продукты и т.д.] повлияют на уязвимости компании?
- Как это влияет на степень риска для ключевых стратегических активов компании?
- [В случае, если риск увеличивается] Какие дополнительные инвестиции (разовые и регулярные) требуются для сведения рисков к минимуму? Включены ли эти вложения в анализ рентабельности инвестиций?

Чтобы обеспечить максимально эффективное расходование ресурсов, будет справедливо попросить директора по ИБ предоставить вам следующую информацию:

- Какой процент инвестиций в кибербезопасность был потрачен на «полочное» ПО?
- Есть ли планы его запуска?
- Когда проводился последний аудит, позволяющий убедиться, что продукты безопасности настроены правильно? Каковы его результаты?
- Когда проводился последний тест на проникновение? Каковы его результаты?
- Когда проводился последний тренинг по кибербезопасности для всех сотрудников? Каковы его результаты?

Отвечая за закупки, **финансовые руководители и их команды минимизируют вред, связанный со взломами «в соучастии» через третьи стороны.** Начните со всеобъемлющей проверки сторонних организаций (по данным Ponemon, это делают только 34% организаций [72]). Затем проведите аудит средств защиты и методов кибербезопасности. Плохая новость в том, что это может потребовать времени и усилий. Хорошая — те же проверочные вопросы можно использовать для определения уровня квалификации любой новой компании, желающей поставлять вам услуги.

Вопросы коснутся нескольких областей и помогут оценить состояние кибербезопасности нового партнера. Они охватят следующие темы:

- Изучение того, как третья сторона оценивает и обновляет права доступа сотрудников.
- Понимание процесса обеспечения бесперебойного функционирования и частоты его тестирования.
- Поиск компанией инструкций по управлению изменениями для новых пользователей и/или нового ПО для ее систем.
- Разъяснение того, как будут использоваться, защищаться и удаляться в надлежащее время (при расторжении контракта и/или в соответствии со стандартами compliance) любые данные, передаваемые между вашей и сторонней компаниями.
- Знание того, как компания шифрует данные в различных состояниях (в состоянии покоя, при использовании, при передаче).
- Оценка того, как сторонняя компания снабжает своих сотрудников информацией о кибербезопасности и учит их соблюдать кибергигиену.

Рассмотрите вариант привлечения третьей стороны для ежегодной проверки методов обеспечения безопасности ваших наиболее важных поставщиков. Это отличный первый шаг. Но для гарантии того, что их меры безопасности не ослабеют после включения вас в список клиентов, потребуется еще больше усердия.

Наконец, с осторожностью разрешайте третьим сторонам рассказывать что-либо о своей компании. Обычно партнеры выпускают пресс-релизы, объявляя о новых контрактах. Также нормально видеть на веб-сайтах организаций логотипы их клиентов, поставщиков и/или партнеров. Я маркетолог, поэтому знаю, о чем говорю. Использование мощи экосистемы для увеличения ценности бренда, как правило, хорошо для всех сторон.

Однако будьте осмотрительны. Любая третья сторона, желающая рассказывать о своих отношениях с вами, сообщает хакерам о наличии «задней двери», через которую они могут проникнуть в вашу организацию. Это показывает киберпаразитам, как проникнуть в

систему, используя «соседа за стенкой». Если у вас есть хоть малейшие опасения, что одна из третьих сторон, желающая опубликовать информацию о связи с вашей компанией, не придерживается требуемых вами стандартов кибербезопасности, **не позволяйте ей это делать.**

Это лишь часть длинного контрольного списка, позволяющего убедиться, что ваши партнеры так же дисциплинированно защищают вашу организацию от угроз, как и вы. Но если они серьезно настроены заработать на вашем бизнесе, разве они не должны также стремиться защищать его?

***

На первый взгляд может показаться, что миры финансов и кибербезопасности не пересекаются. Но более глубокий анализ показывает, что общего у них гораздо больше, чем вы могли думать. По своей сути киберпреступность — крупный бизнес, и это финансовый директор может понять. В свою очередь, кибербезопасность связана с управлением рисками — еще одной концепцией, хорошо знакомой финансистам. С помощью коллег из сферы финансов руководители по ИБ могут более свободно заговорить на языке совета директоров. В свою очередь, они могут помочь тем, кто занимается закупками, говорить на языке кибербезопасности при проверке третьих сторон. Когда две функции объединяются, радуя своими сходствами и заставляя забыть о различиях, это делает их сильнее. В конце концов, дажеплохие парни уже оценили важность взаимодействия. Не пора ли финансовым директорам и руководителям по ИБ сделать то же самое?

Глава 8

Мистер/миссис Целлофан (реприза)

Огромной проблемой для любой компании является то, что пользователи их товаров и услуг, люди из бизнеса, могут просто купить все, что им нужно. Они понятия не имеют, что делают, а в сущности им вообще все равно. Они видят комплект ПО и говорят: «О, вот что мне нужно. Это поможет мне в работе». О вопросах безопасности они даже не задумываются. И во многих случаях они просто загружают и используют данный продукт, что является серьезным риском с точки зрения кибербезопасности. Однако остановить их невозможно.

Технический директор производственной компании

Эймосу повезло. Может, он и женился на обманщице-убийце, но в конце концов она получила по заслугам и провела остаток своих дней в тюрьме. Что же Эймос? Он благополучно женился второй раз. У него

прекрасная семья. Он нашел свое счастье и реализовался в карьере. Пусть на пути его все равно поджидали жизненные испытания, из каждого он выходил лишь сильнее, мудрее и увереннее в себе. Он больше не собирался мириться с тем, чтобы другие члены общества смотрели сквозь него и проходили мимо, не замечая его.

***

Такие же фанаты «Чикаго», как и я, прекрасно знают, что окончание этой повести об Эймосе я выдумала. Самое большее, на что он мог надеяться в мюзикле, — это короткий момент, когда на него ненадолго обратил внимание жуликоватый адвокат его жены, после чего Эймос покинул сцену — и историю.

Но в моем воображении он остался. В своей версии концовки истории Эймоса я переписываю его будущее. Почему бы ему не прожить прекрасную жизнь? У меня Эймос превращает свою трагедию в триумф и исправляет судьбу. Он понимает, что заслуживает намного большего, как бы его ни оценивали другие. И он заставляет всех признать собственную ценность, отказываясь тихо уходить в тень.

Я хочу, чтобы директора по ИБ точно так же переписали свое будущее. Для этого им придется выучить язык, на котором говорит совет директоров. Им нужно будет ослабить бразды правления, чтобы получить больше контроля над своим окружением. И им придется взяться за оружие, став в своих компаниях теми, кто задаст курс на культуру кибербезопасности.

Одна картина вместо тысячи слов

В своей книге «Правила мозга» Джон Медина утверждает: «Мы видим не глазами. Мы видим мозгом» [73]. Он ссылается на интересное исследование, в котором знатокам вин давали белое вино, смешанное с красным красителем без вкуса и запаха. Конечно, испытуемые понятия не имели о манипуляциях, которые исследователи проводили с белым вином. Целью эксперимента было измерить способность зрения влиять на наше восприятие. Будут ли ценители хороших вин полагаться на все остальные чувства, в том числе вкус и запах, чтобы обнаружить подлог?

Как оказалось, не особенно. Сталкиваясь с поддельным красным, дегустаторы описывали свои ощущения словами, которыми мы обычно описываем настоящее красное вино. Как отмечает в своей книге Медина, «визуальная обработка не просто *помогает* нам в восприятии мира. Она *доминирует* в этом восприятии» [74]. [курсив мой]

Может быть, именно поэтому в мире бизнеса так много визуальных сигналов. У нас есть шкалы оценок, наглядно показывающие

производительность, яркие презентации, раскрывающие информацию, и индикаторы, которые в реальном времени дают нам сведения о множестве показателей эффективности бизнес-процессов.

Когда в 2017 году McAfee отделилась от Intel в качестве независимой компании, наш генеральный директор Крис Янг распорядился оперативно собрать и проанализировать важнейшие показатели, чтобы получить полное представление о положении дел. Я была рада продемонстрировать, что команда маркетинга и коммуникаций делала от имени McAfee. Я была уверена, что у нас есть как минимум интересная история: мы планомерно выстраивали отлаженный процесс, и наши усилия по созданию бренда начали приносить плоды.

Я исправно высылала сводный график своей команды раз в неделю. Крис — очень увлеченный лидер, он внимательно относится к деталям. Так что я регулярно получала от него вопросы о работе команды. Они давали мне понять, какую дополнительную информацию следует включить в отчет на следующей неделе, и эффективный цикл продолжался.

Однако однажды я заметила, что в графике моей команды чего-то не хватает. В нашем случае это были не какие-то показатели или метрики. Это был *сигнал*. Нет ничего удивительного в том, что отчеты могут пострадать из-за слишком большого количества деталей, заглушающих само сообщение. Но в нашем случае все было не так. Мы тщательно скорректировали свои показатели, чтобы исключить вероятность соревнования с самими собой среди смножества отвлекающих факторов.

Вместо этого мы создали слишком много шума, не включив в наши отчеты понятные графики, в которых нуждается важнейшее из чувств — зрение.

Этим откровением я обязана лично Крису. Выяснилось, что он недолюбливает одну из самых популярных диаграмм (в том числе и в отчетах моей команды) — круговую. Сначала я думала, что это просто придирки. Затем я поняла: он не единственный, кто не приемлет эту схему.

Несложный поиск в Google показывает, что многие недолюбливают круговые диаграммы. Некоторые придерживаются мнения, что это Nickelback визуализации данных [75] (приношу извинения ярым фанатам Nickelback, читающим это). Если подобная музыка — это не ваше и вы скорее неравнодушны к героям комиксов, то некоторые критики называют круговую диаграмму Акваменом среди диаграмм: «Зачем вам Аквамен, если есть Супермен, который сделает все, что в его силах, а потом еще немного больше? [76]»

Крис выразился более дипломатично. Круговые диаграммы зачастую содержат слишком много информации, сжатой в крошечные сектора, не показывающие, как менялись данные с течением времени. Круговая диаграмма выполняет всего одну функцию: представляет нечто как часть целого. Другие графики, например столбчатая диаграмма, делают то же самое и при этом показывают изменение тенденции во времени.

Я привела этот пример, чтобы подчеркнуть необходимость директору по ИБ в совершенстве овладеть и другим языком — тем, на котором говорят генеральный директор и совет директоров. Конечно, я не говорю, что директора по ИБ — это те самые Аквамены корпоративной Америки: я всего лишь настаиваю, что они не могут позволить себе оставаться экспертами лишь в одной своей области. Чтобы стать Суперменами и Чудо-женщинами своих компаний, они могут сделать несколько выводов из примера с круговой диаграммой:

- Если зрение — ключевое чувство, то зал, где собирается совет директоров, — это кинотеатр IMAX® 3D. Видеоряд должен говорить сам за себя. Эта книга, конечно, не о том, как правильно презентовать свои достижения. Но то, как подача сообщения влияет на его действенность, изучали еще во времена Аристотеля. Если убедительная подача информации, которая не потеряется в какофонии графики и/или другого невербального «шума», не является вашей сильной стороной, вам следует поднатореть в этом [77].
- Директоров по ИБ на заседании правления можно сравнить с туристами. Говорить на языке «коренных» членов совета директоров — обязанность «приезжего» директора по ИБ.
- Члены совета директоров не только свободно оперируют типичными финансовыми показателями (такими как выручка, прибыль, движение средств и т.д.), но и отлично владеют языком риска. Директора по ИБ обычно говорят на языке атак. Между ними есть связь, но существуют и явные различия, и ответственность за то, чтобы связать между собой два языка, лежит на директоре по ИБ.

Позвольте мне объяснить: у руководителей по ИБ есть несколько решений для изучения угроз. Эти модели исследуют анатомию атаки — критически важная (и непростая) задача для директора по ИБ по оценке того, как и где действуют противники. Если директор по ИБ понимает, как маневрирует злоумышленник в ходе атаки, он сможет защитить свою организацию, прибегнув к соответствующей тактике, технике и процедурам, позволяющим уклониться от удара. Он сможет обнаружить уязвимости, применив одну из схем атак для укрепления кибербезопасности своей компании.

С другой стороны, советы директоров занимаются управлением рисками (например, определяют, что может пойти не так). Они делают это в рамках более широкого обсуждения, включающего корпоративную стратегию (как мы будем создавать ценность?), бизнес-модели (как стратегия трансформируется в

ценность?) и ключевые показатели эффективности (как мы будем измерять свою эффективность?) [78].

Конечно, кибератака на фирму сопряжена с риском, порой весьма значительным. Но обратите внимание: директорам по ИБ предстоит сделать как минимум два шага, чтобы перевести свои слова на язык совета директоров. Во-первых, они должны постепенно переходить от риска к стратегии. Риск вне контекста стратегической важности, создания ценности или корпоративных измерений эквивалентен круговой диаграмме ваших результатов, показывающей совету директоров лишь маленький фрагмент общей картины.

Во-вторых, директора по ИБ должны перевести угрозу на язык риска. Для этого им нужно понять следующие вещи: готово ли правление допустить риск в отношении высокоприоритетных активов; как потенциальная атака повлияет на эту готовность; осознают ли руководители возможные последствия — как финансовые, так и иные.

Планка высоковата? Так оно и есть. Стэнфорд представил отчет, согласно которому большинство компаний не объединяют управление рисками и стратегию. Кроме того, у 50% вообще нет системы управления рисками [79]. Есть ли хорошие новости для директоров по ИБ? Вы станете приятным исключением из этих правил, когда сможете эффективно донести позицию вашей компании в отношении кибербезопасности на языке совета директоров. Директора по ИБ заслуживают права доступа на заседания правления, как я и говорила в главе 2. Однако то, как они готовят и доносят свое сообщение, скорее всего, определит, пригласят ли их снова. Чтобы вас не выставили за дверь вместе с одномерными круговыми диаграммами, выучите язык и стиль зала заседаний высшего руководства.

Отпустить, чтобы удержать

В 2014 году на предприятиях творилось нечто невообразимое. Их охватили массовые восстания; ИТ-отделы бурлили; безопасность попала под перекрестный огонь. И что же оказалось в центре всего этого безумия? Сотрудники из лучших побуждений требовали на работе доступа к тем же технологиям по запросу, к каким привыкли дома. К 2014 году вердикт был вынесен. «Консьюмеризация ИТ» стала не просто трендом: она надолго обосновалась в системе.

В том же году IDG Enterprise изучила влияние этого явления на организации. На тот момент 40% компаний предсказывали, что одержимость внедрением пользовательских технологий на работе негативно повлияет на безопасность [80]. Их опасения были небезосновательны. Подумайте, какая скользкая дорожка: 90% организаций в 2014 году заявили, что их сотрудники используют в работе потребительские или индивидуальные сервисы — и 41% делали это без разрешения ИТ-отдела.

Неудивительно, что указанные организации были настроены действовать. Более половины ввели политику доступа и обмена корпоративными данными на мобильных устройствах и/или через облачные сервисы. Примерно треть компаний вложились в безопасный сервис для обмена данными. Третьи внедрили утвержденные средства совместной работы.

Перенесемся на несколько лет вперед и заглянем в отчет McAfee о внедрении облачных технологий и рисках 2019 года. Вместо того чтобы спрашивать респондентов об их мнении или планах в отношении использования облака (что является важным компонентом тренда на консьюмеризацию ИТ), McAfee проверила, какой процент файлов в облаке на самом деле защищен. (Для этого мы анализируем корпоративную политику для каждого файла. Например, программа определяет степень конфиденциальности файла и с помощью анонимизированных агрегированных данных определяет, соответствует ли ей их использование).

Результаты показали, что неуправляемый поезд консьюмированных ИТ уже давно сошел с пути:

- 21% всех файлов в облаке содержит конфиденциальные данные. Эта цифра выросла только за два последних года на 17%.
- Количество размещенных в облаке файлов, содержащих конфиденциальные данные, также увеличилось — на 53% всего за год.
- Облачные учетные данные 92% всех организаций были украдены для продажи в даркнете.

В дополнение к активной консьюмеризации ИТ в 2014 году наметилась и другая гонка. Разработчики, создавая приложения для своих компаний, все чаще и чаще использовали общедоступную облачную среду.

На этом этапе защита облака стала еще сложнее. Как известно всем директорам по ИБ, их организации больше рискуют при переходе от облачной технологии SaaS (от англ. software-as-a-service — ПО как услуга) к PaaS (platform-as-a-service — платформа как услуга) и IaaS (infrastructure-as-a-service — инфраструктура как услуга). Хоть защита данных во всех трех системах единообразна, по мере перехода компании от одной технологии к другой директора по ИБ берут на себя бóльшую часть ответственности за обеспечение безопасности базовых компонентов инфраструктуры облака.

Так, из того же отчета McAfee 2019 года следовало, что на среднестатистическом предприятии на тот момент работало 14 неверных конфигураций IaaS или PaaS, оставляющих открытой для

доступа облачную инфраструктуру — ту самую, которая должна быть защищена в целях обеспечения безопасности данных предприятия.

Поясню: за эти уязвимости безопасности не отвечают поставщики облачных услуг. Вина лежит на компаниях, которые используют данные сервисы, не понимая, как их должным образом защитить. И вся ответственность в конечном итоге ложится на директора по ИБ.

Столкнувшись с новыми реалиями консьюмеризации ИТ, организации стремились обезопасить себя. Подливали ли они непреднамеренно масла в огонь, или же просто их превзошел джинн, которого они пытались загнать обратно в бутылку, — узнать невозможно. Сформулируем вопрос иначе: сотрудники просто обходили политику, снижавшую их производительность? Или же эта политика помогла ограничить нежелательное поведение только для того, чтобы ее обогнало развитие облака? И то, и другое, вероятнее всего, отчасти верно. Как бы то ни было, исследование McAfee доказывает: организации теряют контроль над безопасностью своих данных, хранящихся в облаке, и быстрее, чем всего пару лет назад.

Я дала каждой заинтересованной стороне в организации руководство к действию, которое позволит им сыграть свою роль в укреплении общей безопасности компании. Но я ни за что не посоветую сотрудникам перестать использовать популярные облачные сервисы, к которым они так привыкли. Такие советы все равно останутся без внимания. Пока корпоративные ИТ-службы не предложат сотрудникам альтернативы, люди продолжат пользоваться тем же, чем и раньше, просто без ведома и уж тем более разрешения ИТ-отдела, что еще больше усложнит задачу (вспомним о почти 2000 облачных сервисов, которые используют сотрудники среднестатистической компании, о чем я упоминала в главе 2: «теневые ИТ» действительно могут отбрасывать длинные тени).

Облачиться в мантию

Несколько месяцев назад наш офис загудел, как потревоженный улей. Кто-то развесил повсюду листовки со словами: «Нам нужна будет лодка побольше». Фанаты «Челюстей» сразу опознали фразу из фильма. Но никаких намеков на смысл этих слов для сухопутных сотрудников McAfee не последовало.

Зазвучали самые дикие домыслы. Мы переезжаем в другой офис? Мы с кем-то объединяемся или приобретаем другую компанию? Парковку расширяют? (Да, припарковаться возле офиса бывает сложновато).

Представьте, каково было наше удивление, когда мы обнаружили виновника всей этой шумихи: им оказался не кто иной, как наше управление ИБ. Расклейка объявлений оказалась первым шагом кампании, призванной освежить в памяти сотрудников требования кибербезопасности. В частности, словосочетание «лодка побольше» касалось фишинга (умно!). Управление ИБ разослало всем фишинговые письма, и ряд сотрудников «клюнули», после чего им указали на ошибку и призвали сообщать обо всех подозрительных письмах команде, отвечающей за безопасность. Сделать это можно было через удобный плагин «сообщить о фишинге» в нашем почтовом приложении, запуск которого также совпал с кампанией.

Наше управление ИБ пошло еще дальше. Каждый из руководителей высшего звена ежемесячно получал отчеты о том, как его команда справлялась с испытанием. Какой процент сотрудников стал жертвой фишинга? Какой процент тех, кто не дал себя обмануть, сообщил о подозрительном письме управлению ИБ?

Кампания набирала обороты, и объявления на стенах сменялись напоминаниями о том, как распознать фишинг и сообщить о нем. Осведомленность о проблеме выросла. Руководители (и я в том числе) использовали отчеты для того, чтобы в конструктивной форме донести до своих команд, что можно улучшить, а что делается хорошо и нуждается только в поддержании.

Я даже поймала себя на том, что настороженно ожидаю фишинговых писем от нашего управления ИБ, готовая немедленно сообщить о них. Как-то утром, собираясь на работу, я открыла почту на телефоне и увидела письмо от нашего генерального директора, Криса. Но я тут же поняла: тут что-то не так. Он просил ответить ему по почте, так как якобы не мог до меня дозвониться.

Выбегая из дома, я подумала: «Наша фишинговая кампания началась так продуманно. Но это поддельное письмо от Криса — *не столь умный ход. Слишком уж просто*».

Добравшись до офиса, я тут же сообщила о фишинге. К своему удивлению, я не увидела стандартного всплывающего окна с сообщением от команды по безопасности, которое поздравляло с успешно пройденной проверкой. «Странно. Нужно сообщить им, что автоответ отключен. Как только увижу нашего директора по ИБ, я скажу ему…»

Но такой возможности не представилось: менее чем через десять минут я получила письмо от нашей службы безопасности. Но вовсе не такое, которого я ожидала: «Вы молодец, что заметили поддельное фишинговое письмо». Оказалось, я сообщила о настоящем фишинге. Наша служба безопасности отследила его за считанные минуты и

прислала перечень обязательных мер, которые следует принять в случае, если я ответила на письмо (чего я не делала).

Такой разносторонней кампании вы скорее будете ожидать от отдела маркетинга или персонала. В первый момент вы даже не подумаете о службе безопасности в таком ключе. Но если ваши директора по ИБ и их команды не облачатся в мантию и не станут проповедовать культуру кибербезопасности, то с чего бы им ожидать, что коллеги обратятся в их веру? Директора по ИБ должны идти им навстречу, если хотят, чтобы культура кибербезопасности в компании укоренилась.

W.I.S.D.O.M. для специалиста по кибербезопасности

В распоряжении директоров по ИБ есть множество ресурсов и передовых методов работы. Мудрость, о которой я поведу речь, не для тех, кто хочет получить углубленный технический совет. Но это не умаляет ее значимости. Предлагаемая установка позволит связать вашу ценность с ценностью бизнеса. Она потребует от директоров по ИБ не только начать с основ, но и выйти за рамки своего подразделения.

Необходимость поддерживать здоровую гигиену кибербезопасности даже не обсуждается. Директора по ИБ должны убедиться, что сотрудники понимают основы кибергигиены и что она находится на первых строках «списка дел» каждого в компании. Это тот случай, когда на здравый смысл не всегда можно положиться. Один из самых серьезных взломов на сегодня произошел из-за известной уязвимости, которая не была исправлена. «Вскрытие» этой атаки показало не менее интересный факт: список рассылки, используемый для уведомления администраторов об уязвимости, не включал тех, кому действительно следовало сообщить об этом. Итак, неисправленная уязвимость привела к взлому. А устаревший список рассылки администраторов ИБ привел к неисправленной уязвимости. И это всего лишь один яркий пример того, насколько внимательно профессионалам по кибербезопасности нужно относиться к мелочам.

Поскольку инфраструктура компании постоянно расширяется как физически, так и виртуально, вам следует провести ревизию всех возможных используемых и неиспользуемых серверов. Примером могут послужить зомби-серверы, которые не использовались уже как минимум полгода, но могут составлять значительную часть инфраструктуры предприятия. До 30% всех виртуальных серверов

пребывают в коматозном состоянии [81]. И раз никто ими не пользуется, вероятнее всего, никто их и не защищает.

Вы не можете защитить то, чего не видите. А ваша команда — исправить то, о чем вы не говорите. Помимо инвентаризации всех активов, пересмотрите план ваших внутренних коммуникаций для своевременного уведомления администраторов об уязвимостях.

Перепроверьте свои защитные программы на предмет «полочного» ПО. Обнаружив подобную защитную технологию, которую компания приобрела, но не установила, выясните, почему так произошло. Это решение вам больше не нужно? Или у организации не было времени на его реализацию? Если так, то проработайте со своей командой план или привлеките профессионалов, предоставляющих такого рода услуги, чтобы не дать вашим драгоценным приобретениям пылиться на полке (оставляя вас незащищенными!).

Важна также конфигурация. Вы можете похвастаться лучшей гигиеной в том, что касается исправления уязвимостей, и оперативностью в установке всех приобретаемых технологий кибербезопасности. Однако если вы неправильно настроили эти продукты, то хакеры легко найдут лазейку. Проводя инвентаризацию статуса исправлений, списков уведомлений и «полочного» ПО, проанализируйте конфигурацию имеющихся продуктов на предмет каких-либо изменений со времени предыдущей проверки (которая могла проводиться еще тогда, когда их только установили у вас в организации).

Кроме того, сделайте резервную копию данных. Хоть это и не защитит вас от разнообразных атак (например, от утечки), те же программы-вымогатели неэффективны в случае, если организация регулярно создает резервные копии своих данных. Обладая надежной системой резервного копирования, можно игнорировать требования программ-вымогателей и восстанавливать все файлы в сравнительно короткие сроки. Так что стоит потратить время и определить активы, без которых вы никак не можете обойтись, а затем решить, как сделать резервную копию данных и систем.

Конечно же, резервное копирование полезно и по другим причинам: например, оно дает возможность восстановить более раннюю конфигурацию или версию документа. Оно незаменимо в случае вепонизации (от англ. weapon) данных, когда хакеры манипулируют ими в жульнических и других целях. Регулярная архивация позволяет организации при необходимости получать более раннюю и точную версию данных.

Регулярно проверяйте систему резервного копирования, чтобы убедиться в сохранности заархивированных данных — да, такой сбой в

резервном копировании не редкость. Для безопасного резервного копирования прибегайте к шифрованию — да, как минимум одна компания была бита за то, что не зашифровала журналы регистрации данных.

Если ваш отдел кибербезопасности напрямую не связан с собратьями по ИТ, поддерживать здоровую кибергигиену будет несравнимо тяжелее. К сожалению, отношения между директорами по ИТ и ИБ порой больше напоминают семейную вражду, нежели закадычную дружбу. Достигнув подросткового возраста, кибербезопасность изо всех сил старалась установить и сохранить независимость, отделившись от ИТ-родителя.

Конфликт во многом возникает из-за противоречащих друг другу целей, стоящих перед командами. ИТ — это поддержание работы критически важных систем и применение технологий для функционирования бизнеса. Кибербезопасность же — это защита активов организации. Порой эти цели идут вразрез друг с другом. Например, директор по ИБ может остановить внедрение технологии, которая подвергает организацию риску, чем может возмутить ИТ-директора, особенно если тот действует согласно актуальному графику развертывания систем.

Споры об идеальных отношениях между директорами по ИТ и ИБ ведутся уже много лет. В 40% компаний директор по ИБ подчиняется ИТ-директору, а не генеральному или финансовому [82]. Некоторые подвергают такое положение вещей критике, в качестве основной проблемы выделяя организационный конфликт. Другие же утверждают, что такая структура статистически приводит к увеличению времени простоя и финансовым потерям из-за инцидентов, связанных с кибербезопасностью [83].

Эти вековые дебаты показывают, что директора по ИБ и ИТ должны сонастраиваться друг с другом по духу, а не только по букве закона. **Это требует от директоров по ИБ вовлекать ИТ-директоров в разработку метрик и целей** независимо от того, отчитывается ли первый перед вторым или оба являются соратниками, сидящими за одним столом. В частности, в начале каждого цикла планирования необходимо разделить и согласовать роли и обязанности по обеспечению надлежащей кибергигиены — в том числе исправления, многофакторную аутентификацию и т.п. Если бюджет общий, руководители должны определить, какая его часть будет направлена на ИТ, а какая — на ИБ. В дополнение к этому, возможно, каждый новый ИТ-проект должен учитывать траты на кибербезопасность для финансирования и защиты новых технологий. Как уже упоминалось, директора по ИТ и ИБ должны установить ключевые показатели

эффективности (KPI) и соглашение о гарантированном уровне обслуживания (SLA), что определит приоритетность тех или иных действий и поможет разрешить возникающие споры.

Одно лишь составление подобного списка — уже непростая задача (оттого соблюдение кибергигиены так сложно осуществить на практике). Регулярно проводите тестирование на возможность проникновения, желательно привлекая к процессу третьих лиц. Компании, оказывающие подобные услуги, помогут вам найти неизвестные уязвимости (в кибергигиене или другого рода защите) раньше, чем это сделают злоумышленники.

Инвестируйте в технологии, которые повышают ценность вашего бизнеса и обесценивают усилия ваших противников. Бизнес переходит на облако. Что еще важнее, сотрудники переходят на облако. Так что, если ваша организация не относится к полностью закрытым (каковыми являются, например, крупные государственные учреждения), скорее всего, вы не сможете ограничить сотрудникам доступ к потенциально опасным приложениям или сервисам.

Как говорится, не можешь победить — присоединяйся. Вместо того чтобы сопротивляться переходу на облако, примите его. В качестве возможного решения обратите внимание на брокеров облачного доступа (CASB). По сути, технологии CASB обеспечивают организациям в сфере безопасности контроль над облачными сервисами, используемыми в их компаниях (утвержденными или нет). Они могут обнаружить ошибки конфигурации безопасности в облачных элементах управления (таких как общедоступное и/или доступное для записи хранилище); могут позволить организациям устанавливать соответствующую политику безопасности в любой облачной среде. Иными словами, они позволяют компаниям обеспечить безопасность популярных облачных сервисов, используемых сотрудниками, а директорам по ИБ — поддерживать программы трансформации своих компаний, оставляя во главе угла обеспечение безопасности.

Теперь два слова о негативном влиянии на ценность вашего противника. Как я уже говорила ранее, в кибербезопасности нет такого понятия, как игра от атаки. Это правда. Защитники по определению не бьют первыми. Но сбить врагов с толку они все же могут.

Искусство обмана на войне восходит к глубокой древности, еще в VI веке до н. э. китайский военный стратег Сунь-цзы посвятил ему целый трактат. В кибербезопасности тщательно замаскированные приманки, кажущиеся скрытыми в вашей инфраструктуре сокровищами, выполняют несколько функций. Во-первых, они дают вам дополнительные возможности отслеживать модели поведения врага. Во-вторых, отвлекают его от настоящих сокровищ, которые вы хотите

защитить. Наконец, они тратят время и ресурсы соперника на погоню по ложному следу. Последний пункт более всего напоминает игру от атаки.

Используйте искусственный интеллект (ИИ) для выявления сложнейших угроз и решения проблемы нехватки кадров — но не забывайте об ограничениях. Это новейшая технология в области кибербезопасности. Безусловно, она обещает киберзащитникам помощь в обнаружении самых изощренных угроз, сочетая в себе масштабы машин с умением людей решать проблемы. Однако будьте бдительны. Искусственный интеллект позволяет ограниченным в средствах директорам по ИБ добиться большего при меньших затратах — но ценой ложных срабатываний. Для определения вероятности угрозы ИИ использует сложную аналитику, а значит, дает лишь вероятность, а не уверенность, что угроза действительно существует. А следовательно, ИИ как минимум время от времени будет ошибаться.

С другой стороны, проверенные временем модели обнаружения угроз, основанные на сигнатурах, о которых я говорила в главе 2, тоже могут ошибаться. Сигнатуры не идентифицированной ранее угрозы «нулевого дня» нет в базе данных. Если вашей организации не повезло стать «нулевым пациентом», этот ложноотрицательный результат может нанести ей реальный вред. ИИ может обнаружить угрозу «нулевого дня», которую пропустил сигнатурный метод обнаружения, но он также фиксирует ложные срабатывания. Идеальной модели обнаружения просто не существует.

Вам может показаться, что ложные срабатывания гораздо менее вредны, чем ложноотрицательный результат проверки. Но все зависит от того, под каким углом рассматривать проблему. Ложные срабатывания отнимают ограниченное время и отвлекают внимание от реальных угроз. Подобно тому, как обманная технология, о которой я говорила ранее, отвлекает злоумышленников, ложные срабатывания серьезно истощают ресурсы специалистов по кибербезопасности.

Исследование, проведенное компанией Ponemon [84], показало, насколько коварными могут быть ложные срабатывания. Среднестатистическая организация каждую неделю получает 17 000 предупреждений об угрозах. Лишь 19% из них требуют действий. В Ponemon пришли к выводу, что в среднем крупная компания тратит $1,3 млн на обнаружение ложных срабатываний — что равносильно почти 21 000 часов потраченного впустую времени.

Сложность этой темы усугубляет новая категория угроз, называемая вредоносным машинным обучением. В этом тоже замешаны злоумышленники, изобретающие новые способы сеять хаос и причинять вред своим жертвам. С помощью вредоносного машинного обучения злоумышленники манипулируют входными данными.

Принцип «мусор на входе — мусор на выходе» применим к сфере кибербезопасности, как и в любой другой области ИТ. Модель машинного обучения хороша ровно настолько, насколько надежны входные данные. Если они ошибочны (или подделаны), точность модели страдает.

На одной из недавних выставок McAfee продемонстрировала, как малейшие изменения в пикселях изображения, незаметные человеческому глазу, сбивают с толку модель машинного обучения и заставляют ее отнести изображение пингвина к категории… сковородок! В реальном мире и пингвины, и сковороды могут быть вполне безобидны. Но представьте, как подобный процесс приводит к тому, что беспилотный автомобиль распознает знак обязательной остановки как знак ограничения скорости — и поймете, сколь опасны могут быть варианты использования машинного обучения.

Враги могут вызвать такую же путаницу в системах классификации вредоносных программ. Вводя небольшую вариативность в высокочувствительные модели машинного обучения, злоумышленники могут дезориентировать и профессионалов в области кибербезопасности. Они могут обрушить целый шквал ложных срабатываний и, возможно, приглушить тем самым их остроту реакции (сходный эффект вызывает срабатывание назойливой пожарной сигнализации в многоквартирных домах [85]). Затем, убедившись, что жертва ослабила оборону, злоумышленники наносят настоящий удар.

ИИ, как и любая технология, есть и в вашем арсенале, и у ваших противников. Но это не значит, что ИИ следует избегать. Нам нужно лучше понимать его возможности и ограничения использования.

Возьмем, к примеру, нехватку талантов. С одной стороны, ИИ позволяет тем, кто стоит на страже кибербезопасности, устранять большее количество угроз, делегируя машинам задачи, которые в противном случае требовали бы вмешательства человека. При этом ИИ также увеличивает количество ложных срабатываний и подвержен воздействию со стороны злоумышленников. Если оставить любую из этих опций без внимания, ИИ отчасти лишит нас прироста производительности, который сам же и создал. Угрозы приобретают самые разные формы. Тем же должна отвечать и защита. Люди должны объединиться с машинами. Кроме того, чтобы повысить эффективность и снизить количество ложных срабатываний, потребуется сочетать различные модели обнаружения угроз — основанные как на ИИ, так и на сигнатурах.

Наконец, **несите в массы культуру кибербезопасности.** Конечно, это потребует усилий. Во-первых, директор по ИБ должен владеть языком совета директоров. В залах заседаний понимают язык риска и

всегда сверяются со стратегией компании. Вместе с руководителями бизнес-подразделений, финансовым и генеральным директором определите наиболее стратегически важные активы компании и расставьте приоритеты. Оцените их текущую уязвимость и последствия взлома того или иного актива. Обозначьте наиболее приоритетные/уязвимые активы, которые нужно защитить в первую очередь. Приходя на совет директоров, пользуйтесь этой схемой как руководством, чтобы понять, как ваша стратегия кибербезопасности соотносится со стратегией компании в целом.

Распространять культуру безопасности нужно не только по вертикали, но и по горизонтали, среди сотрудников организации. Проведите совместно с коллегами из отдела персонала эффективный тренинг, который улучшит понимание сотрудниками своей роли (как это сделал директор по ИБ McAfee в рамках своей фишинговой кампании). Найдите способ сделать кибербезопасность чем-то бóльшим, нежели просто ежегодным тренингом или перечнем вопросов, на которые сотрудники отвечают, приходя на работу в компанию. Наймите в команду эксперта по коммуникациям, который совместно с отделом маркетинга определит роль и набор навыков для соответствующей должности. Пусть ваш специалист по внутренним коммуникациям поработает с сотрудниками отделов маркетинга и персонала над созданием эффективных внутренних кампаний, которые сделают кибербезопасность частью повседневной работы каждого в организации.

***

Директорам по ИБ пора занять свое место за столом высших руководителей. Пора взяться за взращивание культуры кибербезопасности, которая простирается далеко за пределы ИТ. Настало время новых партнерских отношений между ключевыми заинтересованными лицами, а именно отделами персонала и маркетинга, которые повысят осведомленность сотрудников о кибербезопасности и снизят уровень уязвимости системы безопасности. Пора переписать конец истории о директоре по ИБ. Благодаря многим прогрессивным руководителям, уже вставшим на этот путь, остальным действующим лицам не нужно выдумывать финал своей истории. Он уже становится реальностью.

Глава 9

Как выглядит культура безопасности на практике

Думаю, отношение к кибербезопасности у нас в офисе слишком легкомысленное. Если бы кто-то действительно хотел, по-моему, *он легко смог бы добыть конфиденциальную информацию, обманув ничего не подозревающих сотрудников или проникнув в незащищенную сеть компании.*
Респондент этнографического онлайн-исследования McAfee

К написанию этой главы я приступаю в довольно-таки нетипичном месте, которое стало для меня на удивление привычным: на высоте примерно 35 000 футов над землей, сидя в трубе весом более 50 тонн, движущейся со скоростью порядка 450 миль в час. Я возвращаюсь из Тампы в Даллас после выходных, проведенных с семьей. Для меня перелеты стали обычным делом. Я не отношу себя к фрилансерам, работающим «на чемоданах», но все же за год легко преодолеваю больше 100 000 миль — достаточно, чтобы получить «золотой» статус от моей любимой авиакомпании, что делает рутину чуть более терпимой.

Хоть меня и поражает, сколь обыденными стали для меня переезды, я все же из тех, кого можно назвать немного нервным путешественником. Например, я крайне серьезно подхожу к сборам (что бы я ни везла с собой и сколько бы ни длился перелет, все должно помещаться в одобренную авиакомпанией ручную кладь, так как сдачу вещей в багаж я даже не рассматриваю). Перед выездом в аэропорт я несколько раз проверяю документы, кошелек и телефон. (Здоровое опасение: я боюсь, добравшись до стойки регистрации, обнаружить, что забыла один из этих предметов первой необходимости.) Я заранее выезжаю в аэропорт, так как нестись сломя голову через терминалы, задыхаясь, прорываться сквозь толпы пассажиров со своей ручной кладью, чтобы в последнюю минуту успеть на рейс, — не лучшее времяпрепровождение для меня. А затем, уже добравшись до своего выхода, я задаюсь вопросом, полетит ли рейс по расписанию, учитывая, что чаще всего по прилете мне предстоит спешить на встречу.

Подобные тревожные мысли — мой вечный плейлист, который я прокручиваю в голове перед каждой поездкой. Но обратите внимание, какого трека в этом списке нет. При всех моих переживаниях одна вещь на удивление не вызывает у меня беспокойства: я не беспокоюсь о собственной безопасности. Я не задумываюсь о том, правильно ли вообще садиться в 50-тонную трубу, которая с трудом поднимается в воздух. Я в этом не сомневаюсь, как и еще 4 млрд пассажиров по всему миру, ежегодно делающих то же самое [86].

Как все изменилось со времен моего первого полета! Тогда я была 20-летним интерном в INROADS, некоммерческой организации,

которая стала моим стартом в корпоративной Америке. Мы с друзьями и другими интернами летели из Тампы в Атланту. В самолете мне досталось место в самом хвосте, рядом с туалетами. Тогда мне это показалось большой удачей — если бы мне срочно понадобилось посетить уборную, до нее было рукой подать. Очень удобно!

Слушая впервые в жизни инструктаж от бортпроводников, я послушно стала застегивать ремень безопасности. Но он никак не хотел защелкиваться. После нескольких тщетных попыток справиться самой и обращения за помощью к соседу я поняла: мой ремень безопасности неисправен. Помню, как подумала: *«Ну и ладно. Наверно, пристегиваться в общем-то не обязательно, как в школьном автобусе»*. Я даже не стала озвучивать свою проблему. А бортпроводники в свою очередь не проверили, застегнула ли я ремень.

Конечно, теперь, пролетев миллионы миль, я знаю, насколько вопиющим нарушением является сломанный ремень безопасности. Сегодня я не представляю, чтобы позволила себе вырулить на взлетно-посадочную полосу, не говоря уже о том, чтобы подняться в воздух, не защелкнув его на талии, как положено. (Между прочим, авиакомпания, на самолете которой я совершала свой первый перелет, в конце концов прекратила свое существование. Что лежало в основе ее упадка? Серьезные проблемы с безопасностью.)

Теперь я знаю, как выглядит и ощущается безопасность на борту самолета и в аэропорту. И я прекрасно понимаю, какая гигантская инфраструктура обеспечивает мое главное право как пассажира: безопасный перелет. Это не значит, что самолеты не падают. Однако в то же время мне незачем соглашаться на меньшее, чем стандарт безопасности, который неукоснительно соблюдается при перелетах — и, да, исправный ремень несомненно входит в обязательный перечень.

Авиаперелеты неспроста остаются самым безопасным способом передвижения — в сто раз безопаснее поездок на автомобиле [87]. Культура безопасности давно проникла во все области авиационной индустрии и прочно там укоренилась.

В этом утверждении, как вам может показаться, нет ничего необычного, и безопасность априори заложена в саму основу авиаперевозок. В конце концов, индустрия была создана для транспортировки ценных грузов — в данном случае людей, — из одной точки в другую. Вы будете правы лишь отчасти. На самом деле культура безопасности, которую мы считаем само собой разумеющейся, так глубоко проникшая в самые основы авиаперевозок, совершенно отсутствовала на заре развития индустрии.

Вспоминая старые добрые времена первых полетов, мы рисуем себе идиллические картины: спокойное небо, одетых по последней моде

пассажиров, за которыми ухаживают внимательные бортпроводники, роскошные лайнеры с простором для ног и изысканной кухней. Чего не хватает этому ностальгическому образу, так это подлинности в части того, как опасно было в те времена летать самолетами. Уровень смертности пассажиров в среднем в четыре раза превышал сегодняшний [88], и это при всей «культуре безопасности», которая и близко не была безопасной. Вот лишь краткий перечень проблем, которые могли ожидать пассажиров в разные периоды истории коммерческих перевозок:

1. Столкновения в воздухе и аварии при посадках случались гораздо чаще из-за несовершенства технологий, отвечавших за полет или посадку судна в ненастную погоду.
2. Двигатели отваливались так часто, что инциденты даже не фиксировали как несчастные случаи, если самолет удавалось посадить на одном двигателе.
3. Из-за конструкции ремней безопасности и низких потолков сильная турбулентность могла привести не только к опрокинутому обеду, но и к перелому шеи.
4. Кстати, о турбулентности. Она была гораздо более частым явлением на самолетах прошлых лет, не имевших герметичных воздушных кабин, которые позволяют летать на более безопасных и комфортных высотах.
5. Походы в туалет представляли отдельную опасность для пассажиров. Стоило чуть-чуть не удержаться на ногах или споткнуться, и можно было рухнуть на острый край кресла или столика — еще один источник опасности на борту, приводивший к травмам и смертям.
6. Стеклянные перегородки, отделявшие первый класс, выглядели потрясающе. Однако в случае аварии или турбулентности они могли разбиться и покалечить пассажиров.
7. На борту можно было закурить. Пассивное курение было частью атмосферы полета.
8. Если сигареты, неисправная проводка или несанкционированный груз (например, кислородные генераторы — да, случалось и такое) приводили к пожару, пассажирам не приходилось рассчитывать на помощь датчиков дыма или огнетушителей за их отсутствием.
9. Вы забыли дома документы? Ничего страшного. Для посадки на рейс их и не требовали.
10. Даже когда предъявление удостоверения личности стало обязательным, требование, чтобы имена на билете и в документе совпадали, не было введено.
11. Вы проносите с собой на борт оружие? Для вашего удобства бортпроводники могли помочь вам убрать его в отсек над головой [89].
12. На внутренних рейсах не проводили осмотр багажа.
13. На международных рейсах иногда проводили осмотр багажа.
14. Ножи, вязальные спицы, ножницы и бейсбольные биты? Пожалуйста, проносите в салон.
15. Чем дальше, тем веселее: пассажиры могли проходить (и регулярно это делали) со своими близкими до самого выхода на посадку и только там прощались.

16. Посетить кабину пилота было настоящим праздником для счастливого пассажира. Сделав это, вы могли даже заработать собственные «крылья».
17. Во время посещения кабины вы увидели бы пилота, имеющего в шесть раз меньше часов налета [90], чем обязаны иметь те, кто сегодня управляет самолетами.
18. Пилот, скорее всего, был бы сильно утомлен, за что отдельное спасибо минимальным требованиям к обязательному отдыху для работников авиации.
19. Инструкции безопасности, которые мы сегодня воспринимаем как должное? В дни первых полетов они были куда менее строгими. Такие требования, как затемнение салона и поднятие шторок иллюминаторов при взлете и посадке, относительно недавно вошли в перечень требований обеспечения безопасности полета: и то, и другое позволяет пассажирам адаптироваться к условиям окружающей среды в случае катастрофы.
20. А как же Управление транспортной безопасности (TSA), проверяющее ежедневно более двух миллионов пассажиров и членов экипажей? До 2001 года его не существовало.

Это всего лишь двадцать примеров того, как далеко продвинулась безопасность авиаперелетов за прошедшие десятилетия. И я даже вскользь не упомянула о преобразованиях, произошедших в мире после 11 сентября и навсегда изменивших характер коммерческой авиации.

Все эти изменения не произошли в одночасье. Они стали результатом того, что индустрию одолели противники (не только люди, но и обстоятельства), и планку безопасности с течением времени приходилось постоянно повышать. Порой мы ностальгируем по давним, более простым временам, когда проверки безопасности в аэропортах практически не существовало; но многие из нас никогда не познают и террора, который угрожал свободе полетов. Если вы рассуждаете как я, то не сможете представить себе, как садитесь на борт в постоянном страхе, но не перед турбулентностью или ненастной погодой, а перед бандитами, преследующими личные или политические цели.

И все же этот образ, ставший визитной карточкой кассовых боевиков, когда-то был суровой реальностью путешественников времени, названного «Золотым веком воздушного пиратства». В период с 1968 по 1972 год угонщики захватили в американском воздушном пространстве более 130 самолетов, и порой это происходило с частотой от одного до нескольких раз в неделю [91]. «Вирус» воздушного пиратства принимал масштабы эпидемии. СМИ с не меньшим рвением освещали эту мрачную действительность. Опрашивая угонщиков, психиатры выявили у них манию превосходства над другими. Те, кто планировал угнать самолет, очарованные широким освещением в новостях последних авиапроисшествий, думали: «Я и лучше могу; я им всем покажу, как надо» [92]. Зараза распространялась.

Сложно поверить, но в те годы угон самолетов стал настолько рядовым событием, что пассажиры воспринимали его как неотъемлемую часть авиаперелетов. В 1968 году журнал Time в некотором смысле подшутил над эпидемией воздушного пиратства, опубликовав статью под заголовком «Что делать, когда появляется угонщик». В ней журналист сообщал о более чем тысяче американцев, переправленных на Кубу за последние 11 месяцев. В то время как «пилоты на всякий случай брали с собой карты гаванского аэропорта имени Хосе Марти, а стюардессы руководствовались распоряжением не спорить с возможными угонщиками, а просто выполнять их приказы… никто пока и не подумал проинструктировать несчастных пассажиров» [93].

Автор любезно соглашается с некоторыми пунктами, что можно и нельзя делать, если помимо своей воли окажешься пассажиром угнанного самолета: например, не следует проявлять агрессию, паниковать, нажимать на кнопку вызова бортпроводника (чтобы звук не напугал угонщика и не заставил его инстинктивно воспользоваться своим оружием) или звать стюардессу во весь голос. Автор также дает два совета, что делать по прибытии на Кубу: сохранять спокойствие и получить удовольствие от пребывания на острове. В статье вы найдете даже несколько полезных рекомендаций по комфортному размещению на ночлег.

Как же авиакомпании справлялись с постоянной угрозой? Они подчинялись. Если угонщик хотел посадить самолет на Кубе или где бы то ни было, пилот разворачивал судно. Куба была настолько популярным направлением угона самолетов, что во всех кабинах экипажа независимо от предполагаемой точки назначения рейса имелись карты Карибского моря. Кроме того, пилотам выдавали карточки с фразами на испанском, которые должны были помочь им общаться с держащими курс на Кубу авиапиратами: «Мне нужно открыть полетный планшет и свериться с картами» или «У самолета проблемы с техникой, до Кубы нам не добраться» [94]. Если преступник требовал выкуп, авиакомпании платили ему в надежде вернуть деньги после ареста угонщика. Компании упорно отстаивали свои слабые средства контроля безопасности, открыто сопротивляясь таким нововведениям, как металлодетекторы, которые помешали бы угонщикам проносить на борт оружие: авиаперевозчики не хотели подвергать клиентов, оплачивающих их услуги, такому же тщательному досмотру.

Невероятно, но факт: авиакомпании настолько противились идее введения каких-либо ограничений, что в качестве альтернативы металлоискателям и прочим подобным мерам даже рассматривали

возможность построить на юге Флориды макет аэропорта, напоминающий гаванский. Согласно этому плану, пилоты сажали бы самолет в фальшивом аэропорту, где угонщика поджидали бы федеральные агенты.

Идея строительства аэропорта-приманки из-за высокой стоимости была отвергнута в пользу поведенческого профайлинга. Агенты, продававшие билеты, проводили беглый осмотр пассажиров на предмет выявления хотя бы одного из примерно двух десятков поведенческих «маячков», отличавших потенциального угонщика. Но так как удобство пассажиров оставалось для компаний важнее в том числе и безопасности, профайлинг применялся менее чем к 1% путешествующих, что оставляло 99% пассажиров непроверенными.

Авиакомпании не были привержены культуре безопасности, в чем я им так доверяю сегодня. На самом деле, они приняли противников как данность и выработали способы сосуществования с ними. Меры безопасности, столь распространенные в наше время, изначально не соответствовали парадигме оптимального обслуживания авиапассажиров. На тот момент доводы, почему следует подчиняться террористам вместо того, чтобы обеспечивать безопасность воздушного сообщения, казались разумными. Авиаперевозки перестали быть прерогативой одной лишь элиты и стали доступны путешественникам из среднего класса. Даже 15-минутные задержки из-за проверки безопасности могли стать существенным стимулом искать другой способ передвижения. На такой риск сравнительно новая индустрия не могла пойти.

Так и обстояли дела до 10 ноября 1972 года, когда угон самолетов превратился из незначительного неудобства в угрозу национального масштаба. Трое захватчиков угрожали направить самолет на атомный реактор Ок-Риджской национальной лаборатории в штате Теннесси. После этого Федеральное управление гражданской авиации приняло меры, от которых отбивались авиакомпании. Уже в январе следующего года все пассажиры начали проходить досмотр, в том числе проверку металлоискателем и проверку багажа.

Но преступники отличаются решительностью и изобретательностью. Когда введенные в аэропорту проверки усложнили угон самолетов, внимание криминальных умов сфокусировалось на авиационных бомбах. Когда в 1990-х меры для защиты от угроз такого типа были усовершенствованы, террористы превзошли сами себя, устроив атаку 11 сентября 2001 года: с помощью допустимых к проносу на борт ножей они захватили коммерческие авиалайнеры и превратили их в самонаводящиеся ракеты (вспомним неудачную попытку совершить подобное в 1972 году).

Что бы ни происходило, авиационная индустрия отвечала дополнительными мерами безопасности.

- 22 декабря 2001 года: пассажир Ричард Рид пытается устроить взрыв с помощью вещества, спрятанного в обуви. Через пять лет Управление по безопасности на транспорте вводит требование разуваться на досмотре.
- 9 августа 2006 года: раскрыт заговор с целью сбивать самолеты с применением жидких взрывчатых веществ. 26 сентября того же года Управление запрещает пассажирам перевозить в ручной клади жидкости весом более 3,4 унции: допустимая к провозу жидкость должна помещаться в прозрачный пластиковый пакет емкостью в одну кварту (требование 3–1–1).
- 25 декабря 2009 года: Умар Фарук Абдулмуталлаб проносит на борт взрывчатку в своем нижнем белье. Вскоре пассажирам приходится проходить через сомнительный виртуальный стриптиз в зоне досмотра — спасибо машинам обратного рассеяния.

Эта игра в кошки-мышки не закончится. На появление следующей угрозы авиаиндустрия ответит новыми мерами безопасности, призванными нивелировать ее. А пассажиры, хоть и будут раздосадованы неудобствами, тоже согласятся с новой нормой, в основе которой лежит их безопасность.

Вот почему я привожу авиаиндустрию как пример культуры безопасности. Это, конечно, не значит, что сегодня авиакомпании с готовностью принимают все меры контроля, не только обеспечивающие нам бóльшую безопасность, но и приносящие некоторые неудобства. В первые дни, когда представители отрасли и пассажиры рассматривали воздушное пиратство как неприятность, а не как угрозу, сопротивление было достаточно сильно.

Посмотрите на перечень мер, которые должны быть приняты, прежде чем современный самолет получит разрешение на взлет. Если хотя бы один пункт не будет соблюден, пассажиров может ожидать задержка, а то и вовсе отмена рейса:

1. Предполетная проверка включает в себя обход и осмотр критически важных компонентов системы, в том числе сенсоров, датчиков, двигателей и кабелей, например тех, что находятся в шасси.
2. Предполетная проверка также включает внутреннее тестирование важнейших систем, таких как термосигнализаторы, метеорадары и сигнальные огни.
3. Бригада техобслуживания выполняет все необходимые работы в соответствии с графиком. Наименее инвазивная и самая часто проводимая из этих проверок происходит каждые 500 летных часов. Самая масштабная — примерно раз в шесть лет, и обходится она так дорого, что зачастую авиакомпания просто списывает самолет, лишь бы ее не проводить.
4. Обслуживающий персонал проводит доскональную инвентаризацию всего оборудования на борту. Если обнаруживаются какие-либо проблемы,

необходимо определиться, устранить проблему или отложить ее решение. Все зависит от перечня минимального оборудования, которое должно быть исправно для совершения полета. Если самолет не соответствует требованиям, он не полетит.

5. Пилот перепроверяет перечень минимального оборудования и отложенных работ по техобслуживанию, чтобы знать все о техническом состоянии самолета перед взлетом.
6. Наземные операторы проверяют самолет на предмет повреждений, а взлетно-посадочную полосу — на наличие мусора или иных препятствий, которые могут помешать при рулении.
7. Пилоты и бортпроводники собираются вместе для предполетной проверки, обсуждают план полета, прогноз погоды и многие другие вопросы, которые помогут сделать предстоящий перелет более безопасным и комфортным для всех.
8. Диспетчеры готовят план полета, учитывая в числе прочего погодные условия и ограничения аэропорта назначения.
9. Пассажиры вовремя прибывают в аэропорт для прохождения проверки безопасности. Она начинается задолго до дня полета: например, заблаговременно выясняют, не числится ли пассажир в розыске.
10. Пассажиры предъявляют документы установленного образца с фотографией; имя совпадает с данными, указанными в билете.
11. Зарегистрированный багаж всегда проверяется.
12. Пассажиры, не включенные в специальные программы (например, предполетного контроля Управления транспортной безопасности), вынимают из ручной клади ноутбуки и жидкости, соответствующие требованию 3–1–1, снимают обувь и верхнюю одежду.
13. Вся ручная кладь проходит через рентгеновский аппарат (если не подвергается физическому осмотру).
14. Каждый пассажир проходит через рамки металлоискателя, сканеры миллиметрового излучения и/или физический осмотр на предмет наличия контрабанды.

Эти проверки безопасности, включая контрольный досмотр, могут быть еще более жесткими для международных рейсов, прибывающих в США.

Критики поспешат указать на недостатки этих систем оценки безопасности с точки зрения защиты пассажиров. Они будут выделять степень надежности тестов на проникновение, проведенных самим Управлением транспортной безопасности: только в 2017 году через различные лазейки проскользнуло не менее 70% незаконной контрабанды [95]. Ни одна система безопасности не безупречна, и авиаиндустрия не является исключением.

Вместо того чтобы удариться в критику, давайте рассмотрим всю статистику. В частности, изучим важнейший, с чем многие, скорее всего, согласятся, результат — безопасную перевозку пассажиров. По

данному показателю авиационная индустрия все же показала себя более чем достойно.

В 2018 году сайт Aviation Safety Network сообщил: количество несчастных случаев со смертельным исходом на крупных коммерческих рейсах составило 36 на миллион рейсов, что соответствует одному летальному исходу на каждые три миллиона полетов [96].

В некоторых странах, например в США, уровень смертности оказался и того ниже. В период с 2009 по 2018 год американские авиакомпании совершили порядка 100 млн рейсов и перевезли несколько миллиардов пассажиров без единого смертельного исхода [97].

Эти результаты говорят сами за себя. В меня, заядлого путешественника, они вселяют уверенность, что у меня гораздо больше шансов умереть из-за сердечно-сосудистого заболевания, погибнуть в автокатастрофе, от удара молнии или даже от укуса пчелы [98], чем на борту самолета. Я могу беспокоиться из-за взятых на борт вещей или забытых документов, но за свою безопасность я спокойна, так как знаю: авиационная индустрия озаботилась вопросами безопасности. Государственный и частный сектор объединились ради одной цели: обеспечить безопасность пассажиров.

Быть может, ваша компания не занимается спасением жизней. Или ваша индустрия еще не пережила свой эквивалент «Золотого века воздушного пиратства» или метафорическое 11 сентября. Надеюсь, в этом и не будет необходимости: главное, чтобы вы, как и любой сотрудник и член совета директоров, поставили безопасность на положенное ей место.

Чтобы безопасность перешла из самых дальних офисов в зал заседаний совета директоров.
Чтобы каждый сотрудник мог внести свой вклад в защиту компании, где работает.
Чтобы конвейер останавливался, если производимый продукт недостаточно защищен.
Чтобы восполнить дефицит талантов в области кибербезопасности.
Чтобы иметь возможность своевременно и однозначно реагировать на взломы.
Чтобы вплести безопасность в обширную сеть сторонних организаций и третьих лиц.
Чтобы поселить культуру безопасности на каждом рабочем месте.

Гарантируют ли все эти меры, что вашу компанию никогда не взломают? Конечно, нет. Принесут ли они положительные результаты,

которые позволят снизить риск и легче восстановиться после атаки? Несомненно.

При всех моих похвалах в адрес авиационной индустрии, даже она не застрахована от угроз — как со стороны человека, так и иного характера. За несколько дней до моего визита домой в Тампу пришла ужасающая новость о катастрофе лайнера Ethiopian Airlines, унесшей жизни всех 157 человек, которые находились на борту. Моя мама редко путешествует. Зато часто смотрит новости по кабельному телевидению. Она позвонила мне накануне моей к ней поездки.

— Элли, я переживаю из-за твоей поездки сюда. На каком самолете ты летишь?

— Мама, я не знаю. Что ты посмотрела и почему спрашиваешь?

— В новостях сказали, что катастрофа Ethiopian Airlines схожа с другой, произошедшей несколько месяцев назад. Обе случились с самолетами 737 MAX. Ты летишь на таком же?

— Мама, пожалуйста, перестань смотреть новости. Все будет в порядке. У меня гораздо больше шансов погибнуть в автокатастрофе, чем на борту самолета. (И прочее бла-бла-бла о безопасности полетов, так и не пробившее могучую защиту, которую мама выстроила от всего, что могло ослабить ее страхи.)

— Дорогая, мне просто нужно знать, что ты не летишь таким самолетом. А если да, то давай договоримся на другое время.

Однако передоговариваться нам не пришлось. Более того, мне не пришлось проверять, на каком самолете я полечу. Накануне моего вылета Федеральное управление гражданской авиации приостановило полеты всех Boeing-737 MAX 8. Культура безопасности, пронизывающая все аспекты авиаперевозок, которыми я регулярно пользуюсь, снова поставила мою безопасность во главу угла.

Я, возможно, и не предвидела никакой опасности, но зато действия Федерального управления не укрылись от взора моей мамы. В ночь перед вылетом она позвонила уточнить, когда именно я прилетаю.

— Элли, я так рада, что нам не пришлось переносить твою поездку. Слава богу, они отозвали все эти самолеты.

— Да, мам. И правда, слава богу.

И слава авиакомпаниям за то, что показали нам, какой может быть культура безопасности — определенно не идеальной, но несомненно достаточно крепкой, чтобы сдерживать грозных противников и развеивать опасения даже тех из нас, кто больше склонен делать из мухи слона. Включая и мою любящую маму.

Глава 10

Культура безопасности для всех

Некоторые кампании по корпоративному управлению, рискам и compliance «задают тон сверху». Руководители должны рассказывать о различных типах угроз кибербезопасности и о том, как их распознать. Тогда должно быть ясно, какую роль ИТ играют в предотвращении кибератак и какую — все остальные. Сейчас я не знаю, где проходит эта грань. О каких аспектах кибербезопасности мне следует беспокоиться, и что должны предотвращать сотрудники ИТ-отдела?
Респондент этнографического онлайн-исследования McAfee
Заголовок короткой статьи был едва заметен и терялся внизу страницы, рядом с объявлением о предстоящем школьном футбольном матче. Те, кто все же заметил его, возможно, отмахнулись как от очередного пророчества о конце света: «Приближается землетрясение мирового масштаба». Четыре дня спустя произошло землетрясение Лома-Приета силой 6,9 балла, которое унесло жизни 63, нанесло ущерб в миллиарды долларов и сорвало третью игру мировой серии в Кэндлстик-парке [99].

Землетрясения — ужасающие проявления силы природы. Ежедневно по всему миру происходит несколько сотен, хотя большинство из нас их даже не замечает. Их сила относительно невелика — 2 балла и менее. Серьезные землетрясения магнитудой более 7 баллов случаются чаще, чем раз в месяц; более 8 баллов — примерно раз в год. В отличие от их меньших «братьев и сестер», мы замечаем только сильные землетрясения. Даже если нам посчастливится избежать гнева матери-природы, средства массовой информации позаботятся о том, чтобы мы узнали о ее разрушительной силе, наполняя наши экраны кадрами разрушенных зданий и жертв катаклизмов.

Что пугает в землетрясениях, так это их неизбежность. Земля активна. Ее плиты сдвигаются. От этого явления никуда не деться.

При всей своей неизбежности землетрясения совершенно непредсказуемы. Их невозможно спрогнозировать. Это единственное, что отличает землетрясения от других стихийных бедствий — ураганов, торнадо и наводнений, — где научные модели помогают людям избежать смертельного удара.

С землетрясениями это не работает — они бьют без предупреждения. Геологическая служба США (USGS) недвусмысленно заявляет об этом на своем веб-сайте: «Ни Геологическая служба, ни другие ученые никогда не предсказывали серьезных землетрясений. Мы не знаем, как это сделать, и не ожидаем, что удастся понять это в обозримом будущем [100]».

Поэтому, когда геолог Джим Беркланд представил невероятно точное (или чрезвычайно удачное) предсказание землетрясения магнитудой 6,9, которое потрясло калифорнийское побережье еще в 1989 году, те, кто пропустил небольшой заголовок несколькими днями ранее, определенно обратили на него внимание после того, как осела пыль.

При составлении прогнозов Беркланд использовал научные индикаторы, такие как график приливов и положение Луны. При этом предсказание Лома-Приеты было одним из 300, которые он сделал за последние 15 лет.

Еще одна выборка данных, которую Беркланд включил в свое исследование для расчета вероятности землетрясения, — количество пропавших без вести до события питомцев, указанное в местных классификациях домашних животных. Зачем было включать в исследование столь нестандартную метрику? Домашние животные убегают, чувствуя надвигающееся землетрясение [101].

Эта гипотеза не нова. На протяжении веков предсказатели предполагали, что животные обладают шестым чувством и способны ощущать незаметные человеку вибрации или электрические изменения в воздухе.

Наука пока не смогла доказать существование такого шестого чувства. Существует множество исследований, направленных на поиск связи между странным поведением животных и последующим землетрясением. Данные свидетельствуют о том, что животные прячутся, становятся агрессивными или демонстрируют иное необычное поведение, хотя «доказательства» не подкреплены научными экспериментами, которые позволили бы четко связать причину и следствие.

Но данное исследование, похоже, доказывает, что животные действительно могут предчувствовать землетрясения. Нельзя утверждать, что они могут предсказать их, но, видимо, животные ощущают предшествующие сильным сотрясениям легкие толчки, которые людям не распознать.

Хотя до сих пор доподлинно не известно, может ли необычное поведение животных помочь людям спрогнозировать землетрясение, есть по крайней мере некоторые свидетельства того, что животные обладают способностью распознавать малозаметные аномалии в окружающей среде — даже если это нужно лишь для того, чтобы привести их в режим повышенной готовности. Эти несколько мимолетных мгновений решают, выживет зверек или нет.

На мой взгляд, то же самое относится и к организациям, которые мобилизуют силу толпы — пресловутый стадный инстинкт — для того,

чтобы привить и развить шестое чувство в отношении киберугроз, которое у сотрудников, как правило, отсутствует. Это происходит, когда каждый оттачивает навыки в обеспечении кибербезопасности. Что еще важнее, это происходит тогда, когда кибербезопасность настолько неразрывно переплетается с повседневной работой каждого в компании, что коллективное шестое чувство обнаруживает угрозы прежде, чем они успевают нанести непоправимый ущерб.

Давайте распространим культуру безопасности на всю вашу организацию.

Каждый сотрудник и каждый руководитель может поработать над тем, чтобы сделать кибербезопасность неотъемлемой частью рабочего процесса — это введет в борьбу мощь «двенадцатого игрока» и разовьет коллективное шестое чувство для борьбы в цифровой сфере.

В этой главе я приведу все ключевые вопросы и действия каждого сотрудника, менеджера, руководителя и члена совета директоров.

Теперь вы в команде.

W.I.S.D.O.M. для генерального директора / члена совета директоров

- Выделите не менее 90 минут на заседании совета директоров на выступление директора по ИБ, в котором он расскажет о текущем положении с кибербезопасностью в компании.
- Немедленно перераспределите бюджет на активы, которые являются одновременно стратегически важными и наиболее уязвимыми.
- На каждом заседании совета директоров посвящайте не менее 30 минут обсуждению темы кибербезопасности.
- Получите от вашего руководителя по ИБ отчет о статусе учений «красной» команды (также известных как тестирование на проникновение). Настаивайте на регулярном проведении этих учений.
- Рассмотрите возможность ввести в состав совета директоров человека, обладающего опытом в области кибербезопасности.

W.I.S.D.O.M. для сотрудника

- Не поддавайтесь кампаниям социальной инженерии. Обращайте внимание на явные признаки вредоносности электронных писем, такие как адрес отправителя. Не переходите по ссылке из неизвестного источника.
- Будьте активны и немедленно сообщайте о любых подозрительных электронных письмах своей команде по кибербезопасности.
- Следите, чтобы ПО безопасности для ноутбуков, планшетов и других персональных устройств оставались актуальными. Не откладывайте обновление системы безопасности, если оно уже отправлено вашей службой безопасности.

- Соблюдайте строгую кибергигиену: придумывайте надежные пароли, не используйте их повторно, избегайте незашифрованных USB-устройств.

W.I.S.D.O.M. для разработчика продукта

- Узнавайте о требованиях ваших клиентов к кибербезопасности на этапе знакомства с ними.
- Включите безопасность в минимальный пакет требований к продукту.
- Четко и осознанно определяйте свои требования к данным при разработке любого нового продукта или услуги.
- Обеспечьте безопасность на каждом этапе жизненного цикла продукта.
- Остановите производство, если на каком-либо этапе запуска продукта вы обнаружите пробелы в его безопасности. Поощряйте и публично вознаграждайте других сотрудников компании за подобные действия.

W.I.S.D.O.M. для специалистов по персоналу

- Дайте дорогу талантам в области кибербезопасности — мужчинам и женщинам, представителям меньшинств, искусства и науки (STEAM). Просмотрите текущие объявления о вакансиях в сфере кибербезопасности на предмет содержащихся в них ограничений. Вычлените из списка вопросов для интервью такие, которые содержат неосознанную предвзятость, включая вопросы вроде: «Расскажите о периоде, когда…» или «Расскажите о последних новинках в области кибербезопасности». Включите в группу интервьюеров хотя бы одну женщину или представителя меньшинств.
- Найдите ценности компании, в которые вы можете добавить слово «безопасность» (или его производную) без изменения первоначального содержания.
- Поощряйте и вознаграждайте поведение, которое укрепляет защиту вашей компании в области кибербезопасности.
- Вместе с директором по ИБ определите и контролируйте доступ к наиболее ценным активам вашей организации. Найдите конфиденциальный и безопасный способ для сознательных сотрудников сообщать о случаях, когда они видят нечто, напоминающее внутреннюю угрозу. Когда они это сделают, вознаградите их соответствующим образом.
- Убедитесь, что у каждого руководителя есть хотя бы один ключевой показатель эффективности (KPI), связанный с кибербезопасностью.

W.I.S.D.O.M. для маркетолога /специалиста по коммуникациям

- Составьте многогранный коммуникационный план с явным участием руководства. План должен включать ответы на следующие вопросы:

- Вы бы уведомили об инциденте общественность, даже если этого не требует закон?
- Что, если ваша компания не несет ответственности за атаку? Как это изменит тон вашего сообщения? (В качестве примеров рассмотрим варианты использования взлома «в соучастии» и вепонизации данных.)
- Когда бы вы уведомили общественность?
- Кого именно поставили бы в известность?
- Что бы вы сообщили, если бы не владели исчерпывающей информацией?
- Что вы готовы предложить клиентам в качестве компенсации или демонстрации сочувствия (например, бесплатную защиту личных данных или предложение покрыть убытки клиентов в результате взлома кредитной карты)?

- Создайте шаблоны сообщений для каждого сценария, указанного в вашем плане. Оставьте пустыми поля для ответов на следующие вопросы:
- Кто пострадал?
- Какие данные и/или системы были взломаны, украдены и/или скомпрометированы иным образом?
- В течение какого периода происходило вмешательство?
- Какие меры предосторожности необходимо принять заинтересованным сторонам?
- Какие действия ваша компания предпринимает для устранения проблемы и снижения риска ее повторения?

- Разработайте временной график для каждого сценария атаки.
- Убедитесь, что в ваш план включены сотрудники, вне зависимости от того, были ли взломаны их данные.
- Проводите учения по вашему плану не реже одного раза в год.

W.I.S.D.O.M. для финансовых специалистов

- Помогите руководителям по ИБ и их командам говорить на языке бизнеса — об управлении рисками, — задавая следующие вопросы:
- Какие активы подвержены риску?
- Какова стратегическая ценность актива(-ов)?
- Каков текущий уровень уязвимости актива(-ов)?
- Каковы последствия (финансовый ущерб, уязвимость интеллектуальной собственности, репутационные риски) в случае взлома?

- Чтобы гарантировать, что обеспечение кибербезопасности не является второстепенной задачей, финансовые директора должны запрашивать следующие бизнес-кейсы, представленные другими руководителями:
- Какими будут последствия взлома (финансовый ущерб, уязвимость интеллектуальной собственности, репутационные риски)?
- Как это повлияет на степень угрозы стратегическим активам компании?
- [В случае, если угроза растет] Какие дополнительные инвестиции (разовые и регулярные) требуются для сведения рисков к минимуму? Включены ли эти вложения в анализ рентабельности инвестиций?

- Снижайте риски максимально эффективно, задавая директорам по ИБ такие вопросы:

- Какой процент инвестиций в кибербезопасность пошел на «полочное» ПО?
- Есть ли планы внедрения этих продуктов?
- Когда проводился последний аудит, позволяющий убедиться, что продукты безопасности настроены правильно? Каковы были результаты?
- Когда проводился последний тест на проникновение? Каковы его результаты? (Тестирование на проникновение было рассмотрено в главе 2 и относится к проверке эффективности политики кибербезопасности организации — обычно путем оплаты третьей стороне попытки взлома).
- Когда проводился последний тренинг по кибербезопасности для всех сотрудников? Какие были результаты?

- Снижайте риски от найма третьих сторон путем проверки уровня безопасности потенциальных поставщиков:
  - Изучите, как компания оценивает и обновляет права доступа сотрудников.
    - Регулярно ли проводятся проверки прав доступа пользователей, гарантирующих минимально необходимый доступ?
    - Осуществляется ли своевременная деинициализация, отзыв или изменение доступа пользователей к системам, информационным активам и данным организации при любом изменении статуса сотрудников, подрядчиков, клиентов, деловых партнеров или вовлеченных третьих сторон?
  - Узнайте, есть ли у компании понимание процесса обеспечения бесперебойного функционирования, и как часто проводится его тестирование.
    - Есть ли у вас планы обеспечения непрерывности бизнеса и аварийного восстановления на случай плановых и внеплановых отключений, и проверяете ли вы эти планы не реже одного раза в год? Если да, опишите типы проведенных тестов.
    - Регулярно ли вы создаете резервные копии, чтобы с их помощью восстанавливать повреждения данных и сводить потери к минимуму? Регулярно ли проверяется восстановление из этих резервных копий?
  - Узнайте, каковы руководящие принципы контроля изменений компании для новых пользователей и/или нового ПО для их систем.
    - Все ли имена пользователей и пароли по умолчанию были изменены во всех ваших системах?
    - Имеются ли у вас средства контроля для отслеживания и ограничения установки ненадежного программного обеспечения в ваших системах (например, вредоносных программ, отключения автозапуска, выдачи чрезмерных прав доступа)?
  - Выясните, как любые данные, передаваемые между вашей компанией и сторонней организацией, будут использоваться, защищаться и удаляться в надлежащее время (при расторжении контракта и/или в соответствии со стандартами compliance).
    - Имеются ли у вас процедуры, гарантирующие, что производственные данные не будут тиражироваться или использоваться в непроизводственной среде?
    - Надежно ли уничтожаются данные из хранилища, когда в них больше нет необходимости? Тщательно ли вы очищаете нефункциональные жесткие диски перед утилизацией или гарантийным возвратом?

- Обеспечиваете ли вы уничтожение всех конфиденциальных данных в течение 30 дней после расторжения контракта?
  - Узнайте, как компания шифрует данные в различных состояниях (в состоянии покоя, при использовании, при передаче).
- Шифруются ли данные при перемещении между узлами, модулями или виртуальными серверами? Если нет, есть ли возможность добавить эту опцию? Опишите используемое шифрование.
- Зашифрованы ли данные в состоянии покоя (например, если они хранятся в базе данных, на резервном диске и т.д.). Если нет, есть ли возможность добавить эту опцию? Опишите используемое шифрование.
  - Оцените, как сторонняя организация снабжает своих сотрудников информацией о кибербезопасности и учит их соблюдать протокол гигиены.
- Есть ли в вашей компании программа обучения и повышения осведомленности о безопасности?
- Обеспечивает ли организация ежегодное обучение персонала политикам безопасности и осведомленность сотрудников об изменениях или обновлениях этих политик?
- Обучает ли компания сотрудников, имеющих доступ к конфиденциальным данным, правилам обеспечения ИБ в рамках их должностных обязанностей?
- Гарантирует ли компания, что все сотрудники, имеющие доступ к персонально идентифицируемой информации (ПИИ), проходят курс подготовки по вопросам конфиденциальности и были осведомлены о каких-либо конкретных требованиях в отношении конфиденциальности обрабатываемых данных?
- Рассмотрите вариант привлечения третьей стороны для ежегодной проверки методов обеспечения безопасности ваших наиболее важных поставщиков.
- Если у вас есть хоть малейшие опасения, что одна из третьих сторон, желающая опубликовать информацию о связи с вашей компанией, не придерживается требуемых вами стандартов кибербезопасности, не позволяйте ей это делать.

W.I.S.D.O.M. для специалистов по кибербезопасности

- Необходимость надежной кибергигиены не подлежит обсуждению. Постоянно вносите изменения как в физическую, так и виртуальную инфраструктуру. Изучите свой план внутренних коммуникаций для уведомления администраторов об уязвимости, включая периодическую проверку списков рассылки для подтверждения точности. Установите «полочное» ПО. Убедитесь, что защитные элементы представлены в надлежащей конфигурации. Создавайте резервные копии данных (и проверяйте работу резервных систем). Регулярно проводите тестирования на проникновение и информируйте руководителей и членов совета директоров о достигнутом прогрессе.
- Директора по ИТ и ИБ должны согласовывать показатели и цели. Для обеспечения надлежащего уровня кибербезопасности в начале каждого цикла планирования распределите между отделами обязанности, включая установку обновлений, резервное копирование, многофакторную аутентификацию и т.п.

Определите, какая часть бюджета пойдет на ИТ, а какая — на кибербезопасность. Согласуйте ключевые показатели эффективности (KPI) и сформулируйте единое соглашение об уровне предоставления услуги (SLA), чтобы расставить приоритеты и иметь возможность разрешать возникающие споры.

- Инвестируйте в технологии, которые повышают ценность вашего бизнеса и снижают ценность вашего противника.
  - Брокеры безопасного облачного доступа (CASB) помогают защитить надежные (и нет) облачные сервисы.
  - Обманные технологии отвлекают противника и сбивают его с толку.
- Используйте искусственный интеллект для выявления наиболее сложных угроз и решения проблемы нехватки кадров, но помните об ограниченности его возможностей. ИИ дает больше ложных срабатываний. Традиционные технологии позволяют отследить меньше угроз. Однако совместное использование обоих способов обеспечит высокую эффективность с меньшим количеством ложных срабатываний.
- Несите в массы культуру кибербезопасности.
  - Распространяйте знания по вертикали, говоря с советом директоров и руководителями на их языке — языке управления рисками. Сотрудничайте с финансовым отделом, чтобы перевести киберречь в метрики и результаты, которые будут наиболее понятны совету директоров и оценены им.
  - Распространяйте знания по горизонтали, используя коммуникационные кампании, направленные на повышение уровня осведомленности о культуре организации. Наймите специалиста по коммуникациям для работы с отделами кадров и маркетинга: вместе они разработают эффективные кампании, которые сделают кибербезопасность частью повседневной работы. Предоставьте функциональным партнерам эффективные оценочные карты, которые помогут измерить понимание сотрудниками принципов кибербезопасности и соблюдение ими политик компании.

Благодарности

Я узнала, что почти вся наша деятельность по жизни — это командный вид спорта, и написание этой книги не стало исключением. Я благодарю тебя, читатель, за то, что занял свое место в команде тех, кто борется за кибербезопасность. И хочу выразить благодарность еще нескольким людям за неоценимый вклад в создание этой книги:

Стиву Гробману — за блистательное умение переводить сложные концепции в практичные советы. С твоим техническим гением может поспорить только твоя искусная коммуникабельность.

Шатель Линч — за то, что стала пророком в своей области и создала среду для процветания культуры мирового уровня. Ты каждый день показываешь мне, что значит играть на победу.

Марку Мюллеру — за мастерство рассказчика. Для меня большая честь сотрудничать с тобой в создании невероятных запоминающихся моментов.

Крису Чаффину — за бесценные отклики по ходу написания этой книги в том числе и во время собственного отпуска!

Джулии Муччарелли — за несравненный талант в создании прекрасных дизайнов, в том числе и обложки, которая займет почетное место на моей книжной полке.

Моргану Беллу, Гевину Доновану и Кевину Истервуду — за скрупулезное изучение каждой главы на предмет фактической и технической точности.

Джонатану Розеку — за несокрушимое упорство в исследовании множества аспектов столь сложной темы.

Роберту Грину и Адаму Розенблатту — за разработку и проведение блестящего исследования, в ходе которого мы нащупали пульс кибербезопасности на современном рабочем месте.

Майклу Марто — за то, что поделился своей мудростью и связями, которые помогли мне воплотить эту историю в жизнь именно такой, какой я ее изначально задумала.

И последнее по порядку, но, конечно, не по важности: **Крису Янгу** — за то, что вы такой вдохновляющий лидер. Благодарю за то, что посвятили свою карьеру и труд тысяч сотрудников McAfee обеспечению безопасности во всем мире. Ваша страсть не сравнится ни с чьей, ваш талант безграничен, а принципы — непоколебимы.

Об авторе

Эллисон Сэрра нашла свое признание в 18-летнем возрасте, когда случайно и на всю жизнь занялась маркетингом в сфере сложных технологий. Она предлагает практический подход к пониманию слияния важных технологических трендов — в том числе мобильности, облачных технологий, больших данных, безопасности и сотрудничества — и помогает увидеть, куда эти силы могут привести культуры в будущем. Анализируя то, как широкополосная связь разрушает традиционную экономику, как технология влияет на корпоративную культуру и отражает ее, как на стыке виртуального и реального миров рождается новый психотип или как злоумышленники бросают вызов нашей цифровой свободе, на страницах своих книг она исследует пересечение технологии, стимулов и моделей поведения. В 2015 году, движимая желанием встать на сторону добра в битве, которую так важно не проиграть, Эллисон Сэрра пришла в McAfee, где до сих пор успешно сочетает свое призвание — маркетинг — и высокую цель

обучения ничего не подозревающих участников виртуальной битвы, которую слишком многие недооценивают, если и вовсе не игнорируют.

Примечания

Глава 1

[1] Louise Bien, "What Makes Seattle's 12th Man So Special?," SB Nation, January 22, 2015, https://www.sbnation.com/nfl 2015/1/22/7871519/seattle-seahawks-12th-man-super-bowl-patriots./seattle-seahawks-12th-man-super-bowl-patriots.

Глава 2

[2] McAfee, "Cloud Adoption and Risk Report," 2019.

[3] Я делюсь результатами работы многих других, кто разбирается в проблемах кибербезопасности и передовом опыте успешных предприятий. По ходу повествования я буду озвучивать собственные идеи McAfee, но также буду с радостью знакомить вас с многочисленными исследованиями и новым мышлением таких организаций, как Deloitte, Ernst & Young (EY), ESG и другие. В этой битве вы не одиноки, о чем свидетельствует растущее число компетентных аналитиков и консультантов, фокусирующихся на этой теме.

[4] Deloitte, "2014 Board Practices Report — Perspectives from the Boardroom,"https://www2.deloitte.com/content/dam/Deloitte/us/Documents/regulatory/us-2014-board-practices-report-final-9274051-12122014.pdf.

[5] Deloitte, "2016 Board Practices Report — a Transparent Look at the Work of the Board,"https://www2.deloitte.com/content/dam/Deloitte/us/Documents/center-for-board-effectiveness/us-cbe-2016-board-practices-report-a-transparent-look-at-the-work-of-the-board.pdf.

[6] Там же.

[7] Melanie Turek, "Employees Say Smartphones Boost Productivity by 34 Percent: Frost & Sullivan Research," Samsung Insights, August 3, 2016, https://insights.samsung.com/2016/08/03/employees-say-smartphones-boost-productivity-by-34-percent-frost-sullivan-research/.

[8] Nir Nissim, Ran Yahalom, and Yuval Elovici, "USB-Based Attacks," Computers & Security, Elsevier, September 2017, https://www.sciencedirect.com/science/article/pii/S0167404817301578.

[9] Apricorn press release, "Apricorn USB Data Protection Survey: Majority of Enterprise USB Security Is Outdated, Inadequate; Nine Out of 10

Employees Use USB Devices, But Only 20 Percent of Them Are Leveraging Encryption," December 12, 2017, https://markets.businessinsider.com/news/stocks/apricorn-usb-data-protection-survey-majority-of-enterprise-usb-security-is-outdated-inadequate-nine-out-of-10-employees-use-usb-devices-but-only-20-percent-of-them-are-leveraging-encryption-1011079268.

[10] McAfee, "The Economic Impact of Cybercrime — No Slowing Down,"https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf.

[11] Justin Nobel, "The True Story of History's Only Known Meteorite Victim," National Geographic News, February 20, 2013, https://news.nationalgeographic.com/news/2013/02/130220-russia-meteorite-ann-hodges-science-space-hit/.

[12] Cybersecurity Ventures, "Cybersecurity Jobs Report 2018–2021," May 31, 2017, https://cybersecurityventures.com/jobs/.

[13] Там же.

[14] Leslie Scism, "Insurers Creating a Consumer Ratings Service for Cybersecurity Industry," The Wall Street Journal, March 26, 2019, https://www.wsj.com/articles/insurers-creating-a-consumer-ratings-service-for-cybersecurity-industry-11553592600?mod=hp_lista_pos5.

[15] Jon Olstik and Jack Poller, "Automation and Analytics versus the Chaos of Cybersecurity Operations," Enterprise Strategy Group, September 2017.

[16] EY, Global Information Security Survey 2017–18, https://www.ey.com/gl/en/issues/governance-and-reporting/center-for-board-matters/the-cost-of-cybersecurity-on-the-board-agenda-ey.

[17] Там же.

[18] Deloitte, "2016 Board Practices Report."

[19] Там же.

[20] Jon Oltsik, "Why Do CISOs Change Jobs So Frequently?," CSO, January 2, 2018, https://www.csoonline.com/article/3245170/why-do-cisos-change-jobs-so-frequently.html.

Глава 3

[21] McAfee Labs Threats Report, December 2018, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2018.pdf.

[22] Gartner press release, "Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019," August 15, 2018, https://www.gartner.com/en/newsroom/press-releases/2018-08-15-

gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019.

[23] EY Global Information Security Survey, 2018–2019, https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2018-19/$FILE/ey-global-information-security-survey-2018-19.pdf.

[24] Patricia Zengerle, "Millions More Americans Hit by Government Personnel Data Hack," Reuters, July 9, 2015, https://www.reuters.com/article/us-cybersecurity-usa/millions-more-americans-hit-by-government-personnel-data-hack-idUSKCN0PJ2M420150709.

[25] Ponemon, "2018 Cost of a Data Breach Study: Global Overview," July 2018.

[26] Verizon, "2018 Data Breach Investigations Report,"https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf.

[27] Verizon, "2018 Data Breach Investigations Report."

[28] Dante Disparte, "Whaling Wars: A $12 Billion Financial Dragnet Targeting CFOs," Forbes, December 6, 2018, https://www.forbes.com/sites/dantedisparte/2018/12/06/whaling-wars-a-12-billion-financial-dragnet-targeting-cfos/#59a7bc3b7e52.

[29] Verizon, "2018 Data Breach Investigations Report."

[30] Taylor Telford, "1,464 Western Australian Government Officials Used 'Password123' as Their Password. Cool, Cool.," The Washington Post, August 22, 2018, https://www.washingtonpost.com/technology/2018/08/22/western-australian-government-officials-used-password-their-password-cool-cool/?utm_term=.d28180e988e7.

[31] https://www.techrepublic.com/article/over-40-of-reported-security-breaches-are-caused-by-employee-negligence/

[32] https://twitter.com/Grifter801/status/1103007628244869121.

Глава 4

[33] NPR, "The End of the Line for GM-Toyota Joint Venture," March 26, 2010, https://www.npr.org/templates/transcript/transcript.php?storyId=125229157.

[34] Там же.

[35] David Kiley, "Goodbye, NUMMI: How a Plant Changed the Culture of Car-Making," Popular Mechanics, April 2, 2010, https://www.popularmechanics.com/cars/a5514/4350856/.

[36] Verlyn Klinkenborg, "Editorial Observer; Trying to Measure the Amount of Information That Humans Create," The New York Times, November 12, 2003, https://www.nytimes.com/2003/11/12/opinion/editorial-observer-trying-measure-amount-information-that-humans-create.html.

[37] Bret Kenwell, "This Is How Many Autonomous Cars Will Be on the Road in 2025," TheStreet.com, April 23, 2018, https://www.thestreet.com/technology/this-many-autonomous-cars-will-be-on-the-road-in-2025-14564388.

[38] Shilipa Phadnis, "Households Have 10 Connected Devices Now, Will Rise to 50 by 2020," ETCIO.com, August 19, 2016, https://cio.economictimes.indiatimes.com/news/internet-of-things/households-have-10-connected-devices-now-will-rise-to-50-by-2020/53765773.

Глава 5

[39] Steve Morgan, "Women Represent 20 Percent of the Global Cybersecurity Workforce in 2019," Cybersecurity Ventures, March 13, 2019,https://cybersecurityventures.com/women-in-cybersecurity/.

[40] Jane LeClair, "Why There Are So Few Women and Minorities in Cybersecurity," Thomas Edison State University, September 7, 2018, https://blog.tesu.edu/why-there-are-so-few-women-and-minorities-in-cybersecurity.

[41] Bletchley Park Research, https://www.bletchleyparkresearch.co.uk/research-notes/women-codebreakers/.

[42] Clive Thompson, "The Secret History of Women in Coding," The New York Times, February 13, 2019, https://www.nytimes.com/2019/02/13/magazine/women-coding-computer-programming.html.

[43] Там же.

[44] John Sullivan, "7 Rules for Job Interview Questions That Result inGreat Hires," Harvard Business Review, February 10, 2016, https://hbr.org/2016/02/7-rules-for-job-interviewquestions-that-result-in-great-hires.

[45] Shannon Shaper, "How Many Interviews Does It Take to Hire a Googler?" re:Work, April 4, 2017, https://rework.withgoogle.com/blog/google-rule-of-four/.

[46] Shankar Vedantam, and Maggie Penman, "How Google's LaszloBock Is Making Work Better," National Public Radio Hidden BrainPodcast, June 7,

2016, https://www.npr.org/2016/06/07/480976042/how-googles-laszlo-bock-is-making-work-better.

[47] Verizon, "2018 Data Breach Investigations Report,"https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf.

Глава 6

[48] https://web.archive.org/web/19980506013419/; http://mardigrasday.com/police1.html.

[49] Jim Taylor, "Is Our Survival Instinct Failing Us?" Psychology Today, June 12, 2012, https://www.psychologytoday.com/us/blog/the-power-prime/201206/is-our-survival-instinct-failing-us.

[50] Maria Saporta, "UPDATE: Retired Home Depot CEO Frank Blake:'I Really Don't Like Amazon,'" Atlanta Business Chronicle, August 15, 2017, https://www.bizjournals.com/atlanta/news/2017/08/15/retired-home-depot-ceo-frank-blake-i-really-dont.html.

[51] Lozanski v The Home Depot, Inc., 2016 ONSC 5447 (CanLII), <http://canlii.ca/t/gt65j>, retrieved on 2019-03-11.

[52] Jennifer Reingold, "How Home Depot CEO Frank Blake Kept His Legacy from Being Hacked," Fortune, October 29, 2014, http://fortune.com/2014/10/29/home-depot-cybersecurity-reputation-frank-blake/.

[53] Ponemon, "2018 Cost of a Data Breach Study: Global Overview," July 2018.

[54] Там же.

[55] Mahmood Sher-Jan, "From Incident to Discovery to Breach Notification: Average Time Frames,"https://iapp.org/news/a/from-incident-to-discovery-to-breach-notification-average-timeframes/.

[56] W. Timothy Coombs, "State of Crisis Communication: Evidence and the Bleeding Edge," Research Journal of the Institute for Public Relations1, no. 1 (Summer 2014).

[57] Lara Dolnik, Trevor I. Case, and Kipling D. Williams, "Stealing Thunder as a Courtroom Tactic Revisited: Processes and Boundaries," Law and Human Behavior 27, no. 3 (June 2003).

[58] R. Moran, and J. R. Gregory, "Post Crisis: Engage — or Fly Low?" Brunswick Review 6 (2014): 32–34.

[59] W. T. Coombs, "Impact of Past Crises on Current Crisis Communications:Insights from Situational Crisis Communication Theory." Journalof Business Communication 41, no. 3 (2004): 265–289.

[60] W. Timothy Coombs, Sherry Jean Holladay, and An-Sofie Claeys, "Debunking the Myth of Denial's Effectiveness in Crisis Communication:

Context Matters." Journal of Communication Management 20, no. 4 (2016): 381–395, https://doi.org/10.1108/JCOM-06-2016-0042.

[61] Ponemon Institute, "The Aftermath of a Data Breach: Consumer Sentiment," April 2014, https://www.ponemon.org/local/upload/file/Consumer%20Study%20on%20Aftermath%20of%20a%20Breach%20FINAL%202.pdf.

[62] Ponemon Institute, "2012 Consumer Study on Data Breach Notification, June 2012, http://www.experian.com/assets/data-breach/brochures/ponemon-notification-study-2012.pdf.

[63] Lillian Ablon, Paul Heaton, Diana Catherine Lavery, and Sasha Romanosky, Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information. Santa Monica, CA: RAND Corporation,2016. https://www.rand.org/pubs/research_reports/RR1187.html. Also available in print form.

Глава 7

[64] McAfee, "The Economic Impact of Cybercrime — No Slowing Down."

[65] McAfee Labs Threat Report, December 2018, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2018.pdf.

[66] Alfred Ng, "WannaCry Ransomware Loses Its kill Switch, So Watch Out," CNET, May 15, 2017, https://www.cnet.com/news/wannacry-ransomware-patched-updated-virus-kill-switch/.

[67] Sean Rossman, "Bed Bugs Disappeared for 40 Years, Now They're Back with a Vengeance. Here's What to Know," USA Today, June 21, 2017, https://www.usatoday.com/story/news/nation-now/2017/06/21/bed-bugs-disappeared-40-years-now-theyre-back-heres-what-know/399025001/.

[68] Korin Miller, "You Can Have Bed Bugs and Not Know It — Here's What to Look Out For," Self, April 6, 2016, https://www.self.com/story/you-can-have-bed-bugs-not-know-it-heres-what-to-look-out-for.

[69] Ponemon Institute, "Data Risk in the Third-Party Ecosystem — Third Annual Report," November 2018.

[70] Deloitte, "Deloitte's 2016 Global Outsourcing Survey," May 2016, https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/operations/deloitte-nl-s&o-global-outsourcing-survey.pdf.

[71] EY Global Information Security Survey 2018–19, https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2018-19/$FILE/ey-global-information-security-survey-2018-19.pdf.

[72] Ponemon Institute, "Data Risk in the Third-Party Ecosystem — Third Annual Report," November 2018.

Глава 8

[73] John Medina, Brain Rules: 12 Principles for Surviving and Thriving at Work, Home and School (Seattle, WA: Pear Press, 2014).

[74] Там же.

[75] https://twitter.com/WaltHickey/status/345646754089291777.

[76] Walt Hickey, "The Worst Chart in the World," Business Insider, June 17, 2013, https://www.businessinsider.com/pie-charts-are-the-worst-2013-6.

[77] Одна из моих любимых книг о презентациях — «Мастерство презентаций» Джерри Вайссмана (Presenting to Win: The Art of Telling Your Story). Если вы не располагаете временем или бюджетом на прохождение профессионального тренинга, эта книга станет для вас бесценным источником секретов, как рассказать свою историю наиболее эффективно.

[78] David F. Larcker and Brian Tayan, Corporate Governance Research Initiative, "Strategy & Risk Oversight," Stanford Business Corporate Governance Research Initiative, https://www.gsb.stanford.edu/sites/gsb/files/publication-pdf/cgri-quick-guide-06-strategy-risk-oversight.pdf.

[79] Там же.

[80] IDG Enterprise, "2014 Consumerization of IT in the Enterprise,"https://www.scribd.com/presentation/212942014/IDGE-CITE-2014.

[81] Patrick Thibodeau, "A Third of Virtual Servers Are Zombies," Computerworld, May 12, 2017, https://www.computerworld.com/article/3196355/a-third-of-virtual-servers-are-zombies.html.

[82] Jody R. Westby, "Governance of Cybersecurity: 2015 Report," Georgia Tech Information Security Center, October 2, 2015, https://globalcyberrisk.com/wp-content/uploads/2012/08/GTISC-GOVERNANCE-RPT-2015-v15.pdf.

[83] Bob Bragdon, "Maybe It Really Does Matter Who the CISO Reports To," CSO, June 20, 2014, https://www.csoonline.com/article/2365827/maybe-it-really-does-matter-who-the-ciso-reports-to.html.

[84] Rishi Bhargava, "False Positives Have Real Consequences," Light-Reading SecurityNow, June 22, 2017, https://www.securitynow.com/author.asp?section_id=613&doc_id=733939.

[85] G. Proulx, J. C. Latour, and J. W. MacLaurin, "Housing Evacuation of Mixed Abilities Occupants," IRC-IR-661, Internal Report, Institute for Research in Construction, National Research Council of Canada, 1994.

Глава 9

[86] https://www.statista.com/statistics/564717/airline-industry-passenger-traffic-globally/. Поясню: эти статистические данные опираются на количество авиапассажиров в год. А значит, заядлый путешественник вроде меня учитывается в этой статистике по нескольку раз.

[87] Ian Savage, "Comparing the Fatality Risks in United States Transportation across Modes and over Time," Research in Transportation Economics 43 (2013): 9e22.

[88] John Brownlee, "What It Was Really Like to Fly During the Golden Age of Travel," Fast Company, December 5, 2013, https://www.fastcompany.com/3022215/what-it-was-really-like-to-fly-during-the-golden-age-of-travel.

[89] Christopher Balderas, "Welcome to the Future: 20 Ways Air Travel Has Changed Since the 1950's," The Travel, June 28, 2018, https://www.thetravel.com/welcome-to-the-future-20-ways-air-travel-has-changed-since-the-1950s/

[90] Leslie Josephs, "The Last Fatal US Airline Crash Was a Decade Ago. Here's Why Our Skies Are Safer," CNBC, February 13, 2019, https://www.cnbc.com/2019/02/13/colgan-air-crash-10-years-ago-reshaped-us-aviation-safety.html.

[91] Brendan Koerner, "How Hijackers Commandeered over 130 Planes — in 5 Years," Wired, June 18, 2013, https://www.wired.com/2013/06/love-and-terror-in-the-golden-age-of-hijacking/.

[92] Libby Nelson, "The US Once Had More Than 130 Hijackings in 4 Years. Here's Why They Finally Stopped.," Vox, March 29, 2016, https://www.vox.com/2016/3/29/11326472/hijacking-airplanes-egyptair.

[93] "What to Do When the Hijacker Comes," Time, December 6, 1968, http://content.time.com/time/subscriber/article/0,33009,844656,00.html .

[94] Koerner, "How Hijackers Commandeered over 130 Planes."

[95] Summer Meza, "TSA Fails to Spot Weapons More than Half the Time," Newsweek, November 9, 2017, https://www.newsweek.com/tsa-fails-half-time-706568.

[96] David Shepardson, "Fatalities on Commercial Passenger Aircraft Rise in 2018," Reuters, January 1, 2019, https://www.reuters.com/article/us-

airlines-safety-worldwide/fatalities-on-commercial-passenger-aircraft-rise-in-2018-idUSKCN1OW007.

[97] Lea Lane, "Reality Check After the Southwest Airlines Fatality: Shocking Stats on Flying, Health and Safety," Forbes, April 18, 2018, https://www.forbes.com/sites/lealane/2018/04/18/reality-check-after-the-southwest-airlines-fatality-shocking-stats-on-flying-health-and-safety/#1205e3117a46.

[98] Там же.

Глава 10

[99] D. Frances, "Ready for the Big One," Sonoma Index Tribune, January 30, 2014, https://www.sonomanews.com/csp/mediapool/sites/SIT/News/story.csp?cid=3387701&sid=744&fid=181&sba=AAS./News/story.csp?cid=3387701&sid=744&fid=181&sba=AAS.

[100] https://www.usgs.gov/faqs/can-you-predict-earthquakes?qt-news_science_products=0#qt-news_science_products, Accessed March 20, 2019.

[101] "Quake Predictor Suspended from Job," San Marino Tribune (and San Marino News), Thursday, November 23, 1989, page 10.

[1] Рис Э. Бизнес с нуля. Метод Lean Startup для быстрого тестирования идей и выбора бизнес-модели. — М.: Альпина Паблишер, 2015.

[2] Марди Гра (фр. Mardi gras, букв. — «жирный вторник») — вторник перед Пепельной средой и началом католического Великого поста, последний день карнавала. Праздник, который знаменует собой окончание семи «жирных дней» (аналог Всеядной недели). Название распространено в основном во франкоговорящих странах и регионах. Празднуется во многих странах Европы, в США и в других странах. Из городов США самые массовые и пышные празднования проходят в Новом Орлеане.

[3] Lusthaus J. Industry of anonymity: Inside the business of cybercrime. — Cambridge: Harvard univ. press, 2018.

[4] Фут — единица измерения длины в английской системе мер, составляет 30,48 см.

Переводчик *Людмила Смилевска*

Редактор *Мария Приморская*

Руководитель проекта *И. Позина*

Корректоры *Е. Жукова*, *Н. Казакова*

Дизайнер *А. Маркович*
Компьютерная верстка *Б. Руссо*

Сэрра Э.
Кибербезопасность: правила игры: Как руководители и сотрудники влияют на культуру безопасности в компании / Эллисон Сэрра; Пер. с англ. — М.: Альпина ПРО, 2022.

ISBN 978-5-9075-3443-8