Охрана предприятия

№5 (63), 2018

Оглавление

Опасные почтовые отправления

Книжное обозрение

Creating Katrina, Rebuilding Resilience: Lessons from New Orleans on Vulnerability and Resiliency

Руководитель корпоративной службы безопасности в 2023 году

На вопросы журнала Security Management (July, 2018) отвечает Скотт Клососки, Партнер консалтинговой компании Future Point of View.

Как изменится роль руководителя корпоративной службы безопасности через пять лет?

В 2023 году глава корпоративной СБ полностью возьмет на себя задачи и функции управления физическими, электронными и кибер системами охраны. Как правило, он/она будет напрямую докладывать о результатах работы СБ совету директоров, первым лицам. Руководители СБ будут отвечать за такие вещи как, например, предотвращение кражи информации инсайдерами, борьба с попытками компрометации внутренних сетей, защита от дронов….Они будут глубоко вовлечены и иметь убедительный голос в системе управления рисками. Другая функция будет заключаться в обеспечении безопасности топ-менеджеров и их семей, используя, в частности, методы разведки в ходе подготовки командировок и отпускных путешествий. Разведка предполагает глубокий мониторинг социальных сетей на предмет выявления потенциальных угроз.

Как будет выглядеть система подотчетности в службе безопасности в 2023 году?

У руководителя СБ будут заместители по кибербезопасности, физической охране, электронным системам охраны. Речь идет о специалистах, хорошо разбирающихся и ответственных за три разные сферы безопасности: собственно компания и ее персонал, СКУД и видеонаблюдение, кибербезопасность. Потребуется более тесное взаимодействие между СБ и отделом кадров, так как человеческий фактор (инсайдерство, в первую очередь) в вопросах безопасности будет возрастать. Нельзя обеспечить надежную охрану предприятия, если руководитель СБ не контролирует все вопросы, так или иначе связанные с безопасностью.

Какова будет динамика взаимного сотрудничества СБ и других подразделений компании?

Чтобы успешно делать свою работу, руководитель СБ обязан развивать тесные

рабочие отношения с отделами кадров, информационных технологий, операционными направлениями компании. Он/она должен участвовать в решении вопросов, связанных с анализом рисков, включая сферу страхования рисков. Его участие в заседаниях совета директоров, совещаниях на уровне отдельных подразделений (по всей структуре компании) необходимо для своевременного обнаружения новых потенциальных угроз и выстраивания систем защиты. Отсиживаться за кулисами, в тени будет невозможно. Их работа должна быть на виду у всех в организации. Руководители СБ станут важнейшим элементом и фактором стратегии компании.

Можно ли эти оценки относить к вопросам безопасности малых предприятий? Как им справляться с новыми угрозами?

На эти вопросы в реальности есть только один ответ: аутсорсинг. Малый бизнес не располагает достаточными ресурсами, чтобы содержать дорогостоящую службу безопасности. Здесь требуется уменьшенная версия охраны. Наилучший путь – воспользоваться услугами местных охранных предприятий, имеющих опыт работы с небольшими организациями. Охранные предприятия способны выстроить приемлемые процессы и системы безопасности, доступные по деньгам для небогатых клиентов.

Видеонаблюдение в жилом небоскребе

Высотный жилой комплекс The Bowie – один из самых престижных в городе Остин (штат Техас). Он построен в 2015 году. Львиная доля средств, вложенных на безопасность, приходится на видеонаблюдение. Первый вопрос, который задал себе Тимоти Колган, заняв должность генерального менеджера The Bowie: «может ли он управлять видеонаблюдением при помощи своего мобильного дивайса?» Ответ был отрицательным.

Между тем, именно видеонаблюдение с самыми современными технологиями Тимоти считает наиболее важным инструментом обеспечения безопасности в высотке, где 2 этажа из 36 отданы под коммерческую аренду. «С точки зрения управления рисками в небоскребе, - говорит он в интервью журналу Security Management (July, 2014), - возможно, самое ценное, что есть у вас, это возможность отсмотреть записи видеокамер. Особенно, если вам надо написать отчет об инциденте. Когда что-то нехорошее случается, скажем, в лифте или в бассейне, видеозапись просто не имеет цены!».

Президент компании Eagle Eye Network Кен Фрэнсис, владелец квартиры в высотке, предложил генеральному менеджеру использовать камеры с программой VMS (video measuring system – измерительная система на базе видеоустройства). Компания Eagle Eye Network выпускает камеры, позволяющие управлять видеонаблюдением как в облачных исчислениях, так и в обычном, «земном» режиме. На Тимоти Колгана произвело впечатление, что предложенная компанией система не только предусматривает возможность управления с мобильного дивайса, но и обладает технологией распознавания лиц с высоким качеством изображения деталей, а также сенсорами движения.

Камеры VMS были приобретены и установлены в ряде внутренних помещений небоскреба, в частности, в бассейне, подземном паркинге, парке для выгула собак (на

10 этаже). Они с одинаковой эффективностью могут управляться как с обычного настольного компьютера, так и с помощью разных приложений к мобильным смартфонам. Одним-двумя кликами камеры включаются и выключаются, ведут запись, сохраняют или передают записи на монитор охраны.

Колган использует мобильное приложение в течение всего рабочего дня и даже во внерабочее время: «Любой из СБ может позвонить и попросить посмотреть, что там случилось на 30 этаже, и будет ли команда как-то реагировать».

Несколько камер размещены в подземном гараже. С их помощью нетрудно рассмотреть госномера въезжающих и выезжающих автомобилей, лица водителей и пассажиров. Если номер машины не совпадает с базой данных, сигнал предупреждения поступает дежурному охраннику.

Система видеонаблюдения чрезвычайно полезна, когда, например, кто-то из резидентов или гостей споткнется, поскользнется, упадет, ушибется... Отчетливо зафиксировавшая несчастный случай видеозапись покажет, по чьей вине это произошло. Особенно важно иметь в наличии такую запись при составлении отчета, копия которого может понадобиться страховой компании.

Предусмотрены даже мелкие конфликты, которые случаются иногда между резидентами и управляющей компанией. К примеру, камеры четко фиксируют, кто из жильцов, выводящих собак на прогулку в специально оборудованном помещении, не убирает за своими питомцами...

Инсайдерские угрозы и физическая охрана

(окончание, начало см. журнал №62)

Оба эксперта, Джефф Беркин, главный офицер по безопасности корпорации CACI, и Стенли Борджиа, вице-президент компании Rolls-Royce North America Inc. по безопасности, подчеркивают необходимость иметь в штате службы безопасности специалиста с компетенциями расследователя.

«Инсайдерские угрозы, контрразведка – область достаточно специфическая, - говорит Беркин, - Поэтому особую ценность приобретают специалисты, обладающие опытом работы в силовых структурах, таких как ФБР или военная контрразведка. Профессионалы с таким послужным списком хорошо разбираются в методах действия предполагаемого противника. И соответственно знают, на какие индикаторы риска следует обращать внимание и как реагировать. Они обладают навыками расследования и допроса, т.е. компетенциями, которых у гражданских служащих обычно нет» (Security Management, May 2018),

Борджиа в свою очередь обращает внимание, что при всех угрозах со стороны киберкриминала сохраняется чрезвычайно высокий уровень традиционных рисков, когда, например, важные корпоративные документы физически выносятся за пределы предприятия.

Важное средство минимизации угрозы инсайдерства – внимание к нуждам работников организации, к их личным проблемам, особенно финансовым. Нельзя доводить ситуацию до той точки, когда попавший в беду служащий не видит иного выхода кроме как пойти на преступление.

Другой ключевой компонент программы противодействия инсайдерству – не только доходчиво объяснять персоналу как себя вести, на что обращать внимание и как докладывать о своих подозрениях, но и втолковывать, чем может для него/нее обернуться игнорирование служебных инструкций.

Подавляющее большинство компаний сегодня проводят бэкграундную проверку при найме на работу. Но это одноразовая акция. Растущий тренд - мониторинг персонала на постоянной основе. Система мониторинга призвана сигнализировать, если с кем-то из работников происходит неладное: финансовые затруднения, задержание полицией за нарушение общественного порядка, подозрительные контакты и тому подобное. Такие вещи далеко не всегда ведут автоматически к увольнению. Но во всех случаях являются индикаторами, что работник испытывает стресс и, возможно, нуждается в помощи.

Сигналы могут служить началом расследования, подготовки к встрече и беседе. Эксперты уверены, что нельзя сразу подозревать наихудшее. На первом этапе расследования необходимо выдерживать благожелательное отношение к сотруднику, пытаться разобраться, помочь.

Борджиа считает постоянный мониторинг поведения работников средствами физической охраны и кибербезопасности жизненно необходимым для обнаружения угроз, исходящих от злоумышленников, имеющих или добивающихся доступа к закрытой информации. Значение тренинговых программ для тех, кому такой доступ разрешен соответственно его служебным обязанностям, невозможно переоценить: «Мы добиваемся, чтобы сотрудники организации имели ясное представление о методах промышленного шпионажа, предполагающие, в частности, попытки знакомства и сближения на выставках и конференциях, а также попытки прямого или косвенного подкупа».

Мониторинг поведения работников в интернете нацелен на выявление отклонений от принятых в компании правил и норм использования виртуального пространства, что может выражаться, например, в необычно частом и объемном скачивании или передаче электронных писем с приложениями. Поведенческий анализ – эффективный инструмент. Специальные программные продукты, отслеживающие онлайновую активность работников, помогают в автоматическом режиме обнаруживать аномалии.

Промышленный шпионаж или конкурентная разведка?

Интернет-издание Chief Security Officer (July 2, 2018) публикует краткий перечень действий, характеризуемых как «промышленный или корпоративный шпионаж»:

- Незаконное проникновение на территорию организации или несанкционированный доступ к информации

- Попытки выдать себя за представителя конкурирующей фирмы с целью выведать служебные секреты или другую конфиденциальную информацию
- Подслушивание, незаконный перехват информации конкурентов
- Хакерские атаки на корпоративную сеть конкурентов
- Попытки заразить вебсайты конкурентов вирусами и прочими зловредами

Но не всегда корпоративный шпионаж носит столь драматический характер, подчеркивает журнал. Нередко речь идет о банальном подкупе работника конкурентной фирмы.

Промышленный шпионаж часто путают с легальной специальностью «конкурентная разведка», которая преподается в ряде западных университетов, а профессионалы объединены в ассоциацию SCIP (Society of Competitive Intelligence Professionals). Компании и специалисты по конкурентной разведке занимаются легальным сбором информации из открытых источников в строгом соответствии с национальными законодательствами.

Это в теории. На практике линия, разделяющая шпионаж и КР, выглядит не всегда отчетливой. Существует так называемая «серая зона», подразумевающая действия, которые могут трактоваться двусмысленно, но при этом не попадать под прямое действие законов. К примеру, в Америке случались скандалы, связанные с попытками нанятых детективов покопаться в мусорных отходах конкурентов. Такие инциденты нередко доходили до суда.

Другие примеры. Как характеризовать «тайных покупателей» (secret shoppers), направляемых для тайной закупки и последующего изучения нового конкурентного продукта? Ничего противозаконного в этом нет. Как нет ничего криминального в найме специалиста по конкурентной разведке для работы на выставках и конференциях.

Поскольку не каждый случай корпоративного шпионажа можно рассматривать как противозаконную деятельность, министерство юстиции США выпустило руководство, признающее необходимым судебное преследование при следующих обстоятельствах:

- Криминальная активность с вовлечением иностранного правительства, иностранного агента или иностранного инструментария
- Высокий уровень ущерба для обладателя корпоративных секретов
- Противозаконное овладение корпоративными секретами
- Наличие эффективных гражданско-правовых средств защиты от посягательств на интеллектуальную собственность
- Когда судебное преследование служит средством предупреждения и предотвращения повторных посягательств

Журнал приводит типичный пример корпоративного шпионажа. Два выпускника одного из американских университетов, работая в компании, регулярно сливали служебную информацию своим подельникам в Китае, рассчитывая открыть в этой стране собственный бизнес.

Важно отметить, что огромное число фактов промышленного шпионажа, даже в случае их обнаружения, остаются вне поля общественного мнения, так как репутационный ущерб намного превосходит материальный.

В море рисков

(окончание, начало см. в журнале №62)

Кибератаки могут быть нацелены на завладение доступом к системам управления и информации портовых организаций и морских судов. По данным исследования международной ассоциации судовладельцев, проведенного в 2017 году, уголовники, террористы, иностранные спецслужбы и инсайдеры стремятся внедрить вирусы в киберсистемы судоходства с целью их компрометации. Особой опасности подвергаются службы спутниковой связи, навигационное оборудование, системы контроля за передвижением и хранением грузов.

Так, к примеру, в 2013 году в Антверпене нанятые наркодельцами хакеры смогли получить несанкционированный доступ в портовую систему, контролирующую грузооборот контейнеров, внести изменения в данные. Это позволило преступникам беспрепятственно вывезти со склада контейнер с припрятанными там наркотиками.

Сегодня судоходство, как и многие другие отрасли экономики и бизнеса, переходит на цифровые решения, широко использует интеграцию физических и кибер технологий, внедряет автоматизацию. Всё это факторы дополнительного риска, поскольку расширяют поверхность соприкосновения с интернетом.

В свою очередь службы безопасности разнообразят и усиливают меры защиты, включая продвинутые технологии контроля за грузооборотом, системы оповещения об угрозах, проверку персонала на благонадежность. В Америке иностранец после надлежащей проверки может получить работу на судах под американским флагом только при условии невозможности заполнить данную вакансию гражданином США.

Получают широкое развитие планы работы в форс-мажорных ситуациях (emergency management plans). Они предусматривают подготовку экипажей судов и персонала портовых организаций по таким дисциплинам как «ознакомление с потенциальными рисками и угрозами», «реагирование на чрезвычайные ситуации», «эвакуация», «коммуникации в условиях форс-мажора».

Такие тренинги эффективны при условии надлежащей подготовки всех работников, предполагающей практические занятия и сценарные игры. К сожалению, отмечают авторы статьи в журнале Security Management, это происходит далеко не везде. Печальным примером служит катастрофа с паромом Sewol в Южной Корее (апрель 2014), когда из-за нераспорядительности экипажа утонули более 300 пассажиров, в основном школьники. Хотя паром тонул три часа, многие на борту так и не получили своевременного уведомления об опасности и необходимости срочной эвакуации. Трагедия свидетельствует о провале плана действий в чрезвычайных условиях.

В 2006 году правительственное агентство U.S. Federal Emergency Management Agency (FEMA) выпустило брошюру «Fundamentals of Emergency Management», которая предлагает три основных вида учебы:

Штабная тренировка (tabletop exercise) – проводится в учебной аудитории на основе конкретного сценария, предусматривает обсуждение возможных мер реагирования.

Функциональная тренировка – полевое занятие с целью отработки одной-двух

функций из плана действий.

Полномасштабная тренировка – полевое занятие, охватывающее все функции плана и всех участников его реализации.

Конечно, необходимо признать невозможность предусмотреть все нюансы в реальной практике. Поэтому так важно в ходе тренингов развивать креативность, умение импровизировать соответственно изменениям в ситуации.

Как разработать должностную инструкцию

С подготовки перечня служебных обязанностей начинается процесс найма специалиста по безопасности, пишет Джерри Бреннан в онлайновом издании Security Magazine, June, 2018.

Такие инструкции нередко страдают существенным недостатком: содержат слишком много задач, функций и требований. Их авторы исходят из неверного посыла – чем больше задач, тем выше зарплата. Но это тот случай, когда «больше» не значит «лучше».

Бреннан предлагает свое видение документа, который должен отражать:

Главное назначение

Необходимо сформулировать предназначение должностной позиции в двух-трех фразах, чтобы соискателю было ясно, какова миссия, какова главная задача.

Обязанности

Надо определить 5 – 8 основных функций и примерно оценить время (в процентах), необходимое для выполнения каждой из них. Здесь же обозначить: степень контроля со стороны непосредственного начальника, уровень автономности в работе:

1. Работа выполняется в определенный период времени и в пределах задач, поставленных супервайзером.

2. Планируемая работа предварительно обсуждается с непосредственным начальником, в результате чего устанавливаются в первом приближении задачи и объем работы, расписание по времени.

3. Вступающий в должность сотрудник разрабатывает подробный план работы и утверждает его у непосредственного начальника.

4. Другой вариант: сотрудник формулирует план и приступает к его реализации без предварительного утверждения, но постоянно держит руководство в курсе дела через регулярные доклады и отчеты.

5. Третий вариант: сотрудник разрабатывает план и выполняет его, а по завершении докладывает о результатах.

Отчетность

Кто непосредственно руководит работником (т.е. кому он подчиняется и перед кем отчитывается)? Помимо ответа на этот вопрос необходимо указать, как выглядит должностная позиция в иерархической структуре: сколько ступеней отделяют ее от топ-менеджмента. Это важно для демонстрации значения, которое придают в организации данной должности.

Полномочия

Обычно в должностных расписаниях указывают число подчиненных. По мнению автора, необходимо также перечислить работников партнерских организаций (включая аутсорсинг), которых курирует сотрудник на данной позиции.

Влияние

Какое влияние оказывает должность внутри и вовне организации? Речь идет о потенциальных потерях для компании в случае, если нанятый работник завалит работу.

Внутренние и внешние взаимоотношения

Необходимо определить и указать, с кем из будущих коллег соискатель должен наиболее часто взаимодействовать. То же самое относится и к внешним, партнерским организациям.

Службы безопасности спортивных клубов и стадионов совместно решают проблемы

«Наши болельщики определенно хотят безопасности, хотят, чтобы рядом была охрана, но в то же время не желают испытывать дискомфорт», утверждает К. Лениер, директор по безопасности Национальной футбольной лиги США (Security Magazine, July, 2018). В структуре лиги создана группа обмена информацией между службами безопасности футбольных клубов и спортивных сооружений, в рамках которой регулярно проводятся совещания для обсуждения стандартов безопасности, разбора последних по времени инцидентов на стадионах, передачи опыта.

Джим Меркурио, генеральный менеджер Levi’s Stadium, отснял короткометражный фильм о порядке и направлениях эвакуации на случай чрезвычайных обстоятельств. Этот фильм демонстрируется на большом электронном табло перед каждым матчем. Его коллега из спорткомплекса Baltimore Ravens использует на тренингах охранников учебные видеофильмы по эксплуатации магнетометров, о правилах общения с болельщиками. Их примеру последовали СБ многих клубов и стадионов.

Практикуются совместные учебные занятия. Говорит Тони Браун, вице-президент Cleveland Browns: «Мы приглашаем на тренинги коллег из Cavaliers, Indians и других клубов. Никакого соперничества, никаких границ. Вместе проводим и практические

тренинги и теоретические занятия за одним общим столом. Мы наладили каналы постоянного и быстрого обмена полезной информацией».

Темы для тренингов самые различные: отравление некачественной пищей, наезд автомобиля на толпу болельщиков, террорист-стрелок и так далее. Представители СБ любого клуба, входящего в лигу, могут не только наблюдать, но и активно участвовать в этих тренингах. Нередко на них приглашаются офицеры местных правоохранительных структур.

Новый стадион Mercedez-Benz Stadium (город Атланта) расположен в самом центре по соседству с Georgia World Congress Center и прочими крупными организациями и корпорациями. Директор по безопасности стадиона Джо Кумер еженедельно, перед каждым матчем, собирает совещания с участием партнеров и ближайших соседей, где рассматриваются и решаются детали предстоящего мероприятия: время проведения, логистика, эвакуация, погодные условия, возможные задержания и аресты буйных болельщиков, предупреждение терактов...Периметр безопасности фактически выходит за пределы территории стадиона. Кумер использует новейшие технологии видеонаблюдения для наблюдения за поведением болельщиков, раннего выявления потенциальных опасностей. Видеозаписи затем внимательно анализируются во время учебных занятий СБ.

В Кливленде Джо Браун заменил 90 аналоговых видеокамер на 350 цифровых: «Мы используем их как инструмент расследования и предотвращения инцидентов». Новая система позволяет в кратчайшее время определить признаки конфликта и вмешаться, пока он не перерос в драку. Видеонаблюдение также помогает контролировать работу охранников во время состязаний, следить, чтобы никто из них не покидал без разрешения свои места.

Отвечающий за безопасность многофункционального спортивного комплекса STAPLES Center в Лос-Анжелесе Дэвид Борн возглавляет команду численностью 400 штатных охранников. Регулярные учебные занятия призваны повысить эффективность управления в критической ситуации, улучшить обслуживание приходящих на состязания болельщиков. Тренинги проводятся не только в учебной аудитории, но и на открытом воздухе, на территории комплекса и вокруг него. Специально разыгрываются сценарии того или иного развития ситуации. Такие практические занятия посещаются акционерами и верхушкой администрации. Они лично знают многих офицеров, начиная с собеседования при приеме на работу, и часто имеют решающий голос в их карьере.

Охрана артефактов

В конце 2011 года на античной римской вилле в Бургосе (Испания) произошла кража. Воры выломали и унесли с собой мозаику пятого века, при этом повредив многие плитки. Этот инцидент привлек внимание многих организаций, включая международную организацию профессионалов корпоративной безопасности ASIS, к проблеме охраны памятников культуры. Международный фонд ASIS выделил грант для работы специалистов по охране произведений искусства Рикардо Маркоса и Джеймса Кларка в местечке Клуния, где расположена эта античная вилла.

Клуния – место, известное в Испании археологическими изысканиями, которые там

ведутся уже на протяжении ста лет. Раскопки охватывают древний римский форум с раннехристианской базиликой, банями, акведуком, амфитеатром. Ежегодно эти достопримечательности посещают около 15 тысяч человек.

В течение нескольких дней эксперты изучали ситуацию на месте, посещая близлежащие населенные пункты, беседуя с их жителями, мэрами, полицейскими. Перед ними стояла задача выявить все потенциальные риски и предложить меры по их минимизации.

Одна из проблем, на которую обратили внимание эксперты – опасность пожаров. Место сухое и жаркое, вокруг простираются травяные поля с невысокими кустарниками, готовые вспыхнуть от молнии или неосторожного обращения с огнем. С другой стороны, в сезон дождей возникает угроза вымывания почвы, а вместе с ней – ценных артефактов.

Специалисты пришли к заключению, что угроза терроризма в этой малонаселенной, засушливой местности минимальна, но главную угрозу представляют похитители артефактов, а также потенциальный ущерб от стихийных бедствий.

Охрана по 6 километровому периметру и внутри этого музея под открытым небом никак не обеспечивала сколько-нибудь надежную охрану. Сторож, гид, продающий билеты для посетителей, один ночной охранник (без автотранспорта) – и это весь персонал. До ближайшего пункта полиции более часа езды. Местные жители, вооруженные металлодетекторами, практически беспрепятственно охотятся за древними монетами. Исследуя местность вокруг виллы, эксперты обнаружили около 200 ям, оставленных любителями старины.

Рекомендации

На основе проведенного осмотра специалисты предложили развернутый план мер по усилению охраны исторического памятника.

Они предложили установить надежную систему СКУД, которая бы включала тепловизоры, электронные замки и запоры, исключающие возможность потери и замены ключей (что неоднократно случалось в прошлом), а также патрульный автомобиль. Было рекомендовано расположить видеокамеры таким образом, чтобы исключить незаметное несанкционированное проникновение на территорию памятника культуры.

Первоначально предполагалось запретить местным жителям пасти овец на прилегающих холмах и полянах, но затем, поразмыслив, решили не трогать эту тему, поскольку скот пожирает пожароопасную зелень.

Также было предложено установить постоянное дежурство в часы, когда вилла закрыта для посетителей. Для этого требуется, как минимум, два охранника – один для внутренней охраны, второй – для патрулирования периметра.

Важное место в плане мероприятий отводится разъяснительной работе с местными жителями. Акцент – на коммерческих выгодах от культурного туризма (рестораны, хостелы, магазины сувениров и т.п.). Эксперты предложили проводить в местных школах, ассоциациях и прочих муниципальных организациях беседы по истории Клунии, а также разработать проект по увеличению числа туристов.

(по материалам журнала Security Magazine)