Охрана предприятия

№2 (30), 2013

Оглавление

Охрана предприятия за рубежом

Охрана торгово-развлекательного комплекса в праздничные дни

Охрана периметра крупных объектов

Книжное обозрение

Risk Analysis and the Security Survey, Fourth Edition.

Исследования

Американские банки и их клиенты все более успешно противостоят интернет криминалу

О тенденциях индустрии безопасности в 2013 году

(по материалам журнала Security Management)

В 2013 году ожидается усиление тенденции врастания функции охраны предприятия в профильный бизнес компаний. Наиболее продвинутые предприниматели воспринимают функцию безопасности как фундаментальную для бизнеса. Безопасность становится важным фактором различных направлений в компании – финансовой, юридической, кадровой, маркетинговой, а также бесперебойной работы цепочек поставок и т.д. Фактически охранные функции трансформируются в систему управления рисками с широким диапазоном действия – от охраны корпоративного имущества до защиты торговой марки. Удачно интегрированная в бизнес стратегию функция безопасности на макроуровне влияет на государственную политику регулирования экономики, непосредственно отражающуюся на положении дел в компании и на рынках.

Если говорить коротко: фокус внимания СБ – бизнес компании, а не только охрана.

Руководителям корпоративных служб безопасности и охранных предприятий также необходимо обратить внимание на технологические тенденции:

Торжество мобильных девайсов
Консалтинговая и исследовательская компания «Гартнер» предрекает, что в 2013 году доступ в интернет мобильными средствами станет преобладающим, а к 2015 году смартфоны займут 80% рынка сотовых телефонов. Естественно, будет возрастать роль

смартфонов в качестве компонента СКУД и в целом систем электронной охраны.

Разнообразие интернет-функций мобильных персональных устройств
Мобильные девайсы наделяются все большими функциями, связанными с использованием интернет технологий. В их числе: сенсорные технологии, функции распознавания изображений, локальные коммуникации – от дистанционного управления дверными замками до интернет-банкинга.

«Облачные» хранилища данных
Облачные технологии постепенно вытесняют ПК в качестве хранилища данных. Конечно, они предлагают уникальный выбор разнообразных услуг. Но, вместе с тем, требуют и более высокий уровень защиты информации, как персональной, так и корпоративной.

Интеграция служб ИТ и охраны
С внедрением «облачных» технологий служба безопасности и отдел ИТ обязаны более тесно взаимодействовать, идти по пути интеграции.

Большие Данные
Растущий как снежный ком информационный массив интернет ресурсов вынуждает кардинально пересматривать архитектуру корпоративных хранилищ данных. Тенденция – переход от единой базы данных, где хранится вся корпоративная информация, необходимая для принятия решений, к более сложной, разветвленной, множественной структуре с отдельными, но связанными друг с другом хранилищами для разных информационных потребностей.

Технологические стандарты СКУД - фактор безопасности

Бернард Скалионе – директор подразделения безопасности медицинских учреждений корпорации G4S, а кроме того руководитель ряда общественных, в том числе международных, организаций по охране объектов здравоохранения. Он побывал на ежегодной конференции производителей металлоизделий для зданий (в том числе производителей металлических дверей и аксессуаров к ним). На него произвело впечатление стремление участников конференции договориться относительно стандартизации продукции, что, по мнению Скалионе, имеет огромное значение для сферы безопасности.

В статье, опубликованной в журнале Security Magazine (December 2012), он пишет: «Не обязательно добиваться стандартизации буквально каждого компонента СКУД, но некоторые вещи надо принимать во внимание. Это, прежде всего, стандарты в производстве дверей. Также имеет смысл стандартизировать некоторые электронные компоненты системы СКУД и продукты идентификации».

Уже опубликованы минимальные требования стандартизации в этой сфере. ISO/IEC 7810 Identification предлагает одинаковые физические характеристики для идентификационных карт – размеры, устойчивость с сгибанию, огню, воздействию химических веществ, температурным перепадам, влажности и жаре. Другой международный документ – Transportation Worker Identification Credential –

устанавливает стандарты идентификационных карт на транспорте.

Значение стандартов неоспоримо, подчеркивает автор. К примеру, ассоциация производителей металлоизделий, на конференции которой он присутствовал, установила стандарты замков, запорных устройств различных уровней прочности и долговечности. Один стандарт подходит для офисных учреждений, работающих фиксированное время в сутках.

Другой стандарт годится для больниц и госпиталей, где устройства используются круглосуточно все дни недели, а, следовательно, требуют повышенной износостойкости. Эти стандарты опубликованы в специализированных изданиях, так что каждый пользователь может выбрать и заказать то, что ему больше всего подходит.

Такой пример. Батареи электронных замков требуют регулярной замены. В одних случаях каждый год, в других каждые два года. В большинстве больниц замена требуется каждые три-четыре месяца. Поэтому они вынуждены обращаться к ограниченному числу производителей, которые специализируются на производстве электронной продукции специально для медицинских учреждений.

Еще один пример. Стандартизация замковых отверстий в дверях позволяет использовать и заменять запорные устройства разных производителей с неодинаковой начинкой внутри.

Стандартизация программной платформы позволила бы выпускать взаимозаменяемые продукты (компоненты, узлы) СКУД. Они дешевле, быстрее осваиваются, удобнее и легче в эксплуатации. Речь идет о считывателях, контроллерах, идентификационных картах и других компонентах.

Компетенции и качества успешного руководителя СБ

По просьбе журнала Security Magazine группа экспертов провела опрос 39 руководителей корпоративной безопасности с целью понять, какие их компетенции (всего в списке именованы 67 компетенций) имеют приоритетное значение для успешной работы и карьеры в сфере охранной индустрии. Основные выводы опубликованы в журнале за 2 января 2013 года.

Авторы исследования не удивились, обнаружив, что две трети респондентов в первую очередь назвали такие качества как честность и неукоснительное следование кодексу этики. Действительно, пишут эксперты в своем заключении, безопасность – «очень чувствительная функция», требующая от исполнителей любого уровня осмотрительности, осторожности. Сегодня, в условиях растущей взаимозависимости и в мире бизнеса, и в общественной жизни, любая оплошность, связанная с этическими аспектами, может уничтожить репутацию.

Исследователи обращают внимание, что в числе приоритетов – коммуникабельность, умение налаживать и поддерживать взаимоотношения на разных уровнях и с разными

группами партнеров и коллег, с начальством, кураторами, клиентами-пользователями охранных услуг и т.д. Искусство диалога, умение слушать - ключевой фактор, отмечают эксперты. Такие «мягкие» качества, по их мнению, мощно стимулируют профессиональный рост, а их отсутствие сможет сломать карьеру в самом начале.

Верхние строчки заняли такие компетенции как умение ориентироваться, не теряться во внештатной ситуации, организационные способности. В нынешних условиях быстрых изменений и нестабильности лучшие специалисты по безопасности должны действовать выдержанно, спокойно, но в то же время принимать быстрые, а иногда и жесткие, непопулярные действия, чтобы решить проблему в зародыше и окончательно. Для этого требуются сила духа, твердая уверенность и поддержка сверху.

«Знания – сила». Однако, отмечают эксперты, сами по себе они бесполезны, если нет умения (или желания) реализовывать их в практической деятельности.

Вот главные, приоритетные компетенции, названные избранной группой руководителей корпоративной безопасности. Что делать с этой информацией?

Эксперты рекомендуют принять ее во внимание тем, кто только начинает свою карьеру в индустрии безопасности. Проанализируйте, обладаете ли вы названными качествами? А если нет, то где и как их можно приобрести? Авторы исследования отмечают, что в большинстве крупных компаний имеются опытные наставники, курсы повышения квалификации, тренинговые программы. Необходимые знания и компетенции дают бизнес школы. Еще один путь – попросить старших, более опытных коллег по работе, отвечающих самым строгим требованиям, помочь вам в профессиональном росте.

Что такое социальная инженерия и как от нее защищаться

Термин «социальная инженерия» («social enigineering») получил распространение в последние годы. Под этим термином понимается злонамеренное проникновение в офисные здания и помещения, в системы и базы данных с использованием фактора человеческой психологии.
Отличие «социального инженера» от хакера или примитивного грабителя состоит в том, что он не будет пытаться взломать защиту компьютерных сетей, не будет залезать ночью в офис с фомкой в руках, а просто позвонит конкретному лицу в компанию, представится работником ИТ отдела этой компании и попытается заполучить пароль на вход в систему.

Старший редактор онлайнового журнала Chief Security Officer Джоан Гудчайлд рассказывает о наиболее популярных приемах социальной инженерии и способах защиты от нее.

Автор напоминает об удачном проникновении в частную компанию Криса Никерсона, руководителя консалтинговой фирмы, с целью продемонстрировать, насколько серьезной может быть успешная социальная инженерия. В футболке Cisco, которую Крис купил за 4 доллара, он легко обманул охрану компании, представившись

представителем уважаемой корпорации, которого пригласили для проведения профилактических работ. Он свободно перемещался по офису, и даже на глазах ничего не подозревающего персонала смог с помощью своих флешек «погулять» по корпоративным сетям. О чем и рассказал потом в прессе.

Одна из причин ротозейства – уверенность, что в компании «нечего красть» и злоумышленнику здесь «не интересно». При этом люди не задумываются, что преступника интересует, может быть, не место их работы, а персональные данные, с помощью которых он собирается, к примеру, украсть деньги с банковского счета.

Преступники тщательно, неделями и месяцами, готовятся, прежде чем позвонить или лично посетить компанию. Они ищут список телефонов персонала, фамилии сотрудников, другие данные, активно используя популярные социальные сети (Фейсбук и т.п.). Эксперт по социальной инженерии Крис Робертс рассказывает, как однажды, разыскивая (в тестовом режиме) электронный адрес одного менеджера, обнаружил и адрес, и номер его рабочего телефона, которые тот оставил на форуме для человека, который бы мог продать билет на концерт. Представившись «журналистом», Крис позвонил ему на работу и без труда выведал другие персональные данные: номер мобильного телефона, домашний адрес, даже информацию о закладных...

Испытанный прием: влезть в доверие к одному из персонала, а через него осуществлять дальнейшие действия. Преступники стремятся расположить к себе. Иногда используют профессиональный жаргон, принятый в компании. Наиболее изощренные злоумышленники записывают музыку, которая звучит в корпоративных телефонах, чтобы прикинуться коллегой из другого управления той же организации. Но не всегда звонят перед «визитом». Иногда действуют по наглому: «Ой, подержите дверь, пожалуйста, я оставил свой пропуск (электронный) дома». И пропускают. Некоторые сами изготавливают пропуска- бэджи со своей фотографией. Их легко принимают за «своих». Один из экспертов свободно проходил в компанию по бэджику, на котором было написано: «Выкиньте меня отсюда». И никто не обратил внимания.

Но главное средство и источник информации для социальной инженерии – социальные сети. Об этом - в следующем номере журнала.

Уроки «Сэнди»

Небывалое наводнение, затопленное метро, тысячи разрушенных строений, миллионы людей без электричества. Таковы результаты кратковременного визита на восточное побережье США урагана «Сэнди». Власти признались, что не были готовы к столь разрушительным последствиям. Сейчас время извлечь уроки на будущее. Об этом – статья в журнале Security Magazine (January 2, 2013).

Самой сложной проблемой, говорит Билл Райш, директор международного исследовательского центра при Нью-Йорском университете по стратегическим рискам (International Center for Enterprise Preparedness), стало нарушение работы энергетических компаний. Без света и тепла остались почти 9 миллионов людей. Работа ряда компаний и организаций была остановлена. Поэтому на будущее, отмечает Билл, кампаниям надо заранее позаботиться об автономных источниках энергии, таких как генераторы.

Эта проблема усугубляется плачевным состоянием гидротехнических сооружений и тепловых станций в США. На многих из них оборудование устарело, отсутствуют механизмы и средства защиты от стихийных бедствий. Правительство США это понимает, но мало что может сделать: 90% предприятий энергетики в частных руках, их деятельность регулируется местными властями.

Таким образом, на повестку дня встал вопрос о «самовыживании». Рассказывает Томас Pop, директор компании Worldwide Corporate Security for Carestream in Rochester, Нью-Йорк: «Один из заводов компании в результате урагана оказался обесточенным. Но мы были готовы к такому повороту и смогли достать мощный генератор. В экстремальной ситуации ярко проявилось значение хороших, добрых связей с партнерами. Нас выручил небольшой близлежащий аэропорт, обслуживающий исключительно местное население и организации. В то время как крупные аэровокзалы были закрыты, мы смогли воспользоваться его услугами».

Конечно, нельзя предусмотреть все до последней детали, продолжает Томас. Можно выкрутиться с подачей энергии, но что делать с рабочими, которые в трудные дни заняты защитой своих семей, и их не заставишь вернуться на работу! Тем не менее, заранее продуманные планы и программы для экстремальных ситуаций критически необходимы.

Исполнительный директор нью-йоркского управления мостовым хозяйством Джон Белуччи утверждает, что в случае повторения подобной стихии необходимо максимальной задействовать Твиттер и другие популярные социальные сети для объективного и полного информирования населения. Столько всяких ложных слухов ходило по городу перед началом урагана – и что «все мосты закроют», и что «до управления мостами невозможно дозвониться», и т.п.

Рэй Томас, руководитель отдела консалтинговой фирмы Booz Allen, также верит в необходимость создания в каждой организации четкого и ясного «плана выживания» в экстремальных условиях, который бы предусматривал множество мер, включая обеспечение безопасности персонала, возможность переезда временно в другое помещение, прекращение поставок…К сожалению, до сих пор многие бизнесмены недооценивают программу управления рисками, не включают ее список приоритетов. Это большая ошибка. Конечно, для крупных корпораций не составляет труда свернуть на время производство в одном месте или перенести его в другой регион. Но что делать малым предприятиям – вот им то и надо выживать.

Энергетика: кибер-терроризм страшнее урагана Сэнди

Американская организация National Research Council опубликовала отчет, из коего следует, что энергетическая инфраструктура США требует срочных мер по защите от террористов, прежде всего кибер-террористов. Удачная хакерская атака может оставить огромные регионы страны без тепла и света на недели и месяцы, говорится в отчете (csoonline.com).

Основные уязвимости и проблемы:

Федеральное законодательство еще в середине 90-х годов прошлого столетия открыло свободную конкуренцию на рынке энергетики, что привело к возникновению массы мелких предприятий в этой сфере.

Оборудование большинства предприятий устарело. Это, в частности, касается технологии проверки и контроля за рабочим состоянием энергообъектов.

Компании в первую очередь озабочены извлечением прибыли и не уделяют достаточного внимания вопросам охраны и безопасности.

Многие коммунальные компании – поставщики электричества – в целях экономии средств пошли по пути централизации и кооперации корпоративных сетей. А это означает, что в случае успешного вторжения в сети из строя будут выведены сразу несколько предприятий.

В отчете содержатся рекомендации, что делать для снижения рисков:

Начинать надо с капиталовложений в исследования. Сейчас на эти цели отпускаются несерьезно малые средства.

Помимо денег необходимо разрабатывать, внедрять, выпускать и размещать на энергообъектах высоковольтные трансформаторы, которые позволят в случае необходимости хотя бы на какое-то время заменить используемые ныне импортные трансформаторы, изготовление и поставка которых из-за границы занимает месяцы, если не годы.

Что же касается контрольной аппаратуры, то авторы отчета рекомендуют изолировать ее от интернета. Если это невозможно, то заменить ее на принципиально другую технологию, либо поставить мощные, по последнему слову техники, системы безопасности, надежно защищающие корпоративные сети от несанкционированных проникновений и саботажа, способные замечать, сигнализировать и реагировать на любые погрешности и отклонения в работе сетей.

Исследователи также рекомендуют федеральным властям инициировать и осуществить программу тестирования безопасности в сфере энергетики по всей стране. Эта программа должна стать моделью для региональных властей.

Следует также поощрять обмен информацией между госструктурами и частными компаниями. Что же касается законодательства, то, как известно, частный бизнес выступает против жесткого регулирования в области интернет технологий.

Защита информации: каковы тенденции и ожидания?

На этот вопрос попытался дать ответ эксперт МакКаурт в журнале Security Magazine (December 2012).

Автор предвидит рост числа банкротств в результате успешной хакерской атаки на корпоративную сеть, чреватой невосполнимым материальным и репутационным

уроном.

Поскольку кибер угрозы год от года возрастают, тенденция интеграции службы безопасности с ИТ отделом и другими подразделениями в рамках одной организации будет усиливаться. К концу 2013 года уже в половине американских организаций служба безопасности возьмет на себя функцию защиты информации (по опросам в 2012 году, такой расклад был характерен лишь для каждой пятой компании).

Есть серьезные основания надеяться, что в течение ближайшего года Конгресс США примет, наконец, закон, предусматривающий минимальные требования к защите инфраструктурных объектов от хакерских атак.

Расходы компаний на защиту корпоративных данных продолжат расти вне зависимости от общеэкономической ситуации. По оценкам некоторых экспертов, рынок в этом сегменте уже через несколько лет будет измеряться десятками миллиардов долларов.

На рынке технологий безопасности начался процесс стандартизации продуктов и сокращения брендов, что позволит уменьшить расходы на освоение и эксплуатацию технологий, на обучение персонала.

Как составить инструкцию по безопасности

Брэндон Грэг, эксперт по внутрикорпоративным расследованиям, обращает внимание работодателей на необходимость постоянно напоминать своим работникам о строгом соблюдении принятого в компании свода прав и обязанностей персонала, особенно в той его части, которая имеет непосредственное отношение к безопасности бизнеса.

В статье, опубликованной в журнале Chief Security Officer (January 8, 2013), он пишет о все более популярной моде приносить на работу собственные компьютеры, мобильные девайсы, что, по его мнению, чревато утечками служебной информации. В обязанностях сотрудников - официально регистрировать личные девайсы, используемые в работе, что не только помогает снизить риски, но и проводить расследование в случае несанкционированных утечек.

Автор излагает рекомендации к составлению инструкции по безопасности, которая может быть частью общей политики компании. Инструкция должна содержать, как минимум, следующие моменты:

Цель инструкции. Во вступлении надо разъяснить, что круглосуточный мониторинг корпоративных сетей предназначен не для слежки за сотрудниками, имеющими доступ в сети, а для защиты информации, бизнеса и самих работников.

Фокус внимания: что следует делать для защиты сетей. Если написать: «все электронные данные подвергаются мониторингу», то это звучит слишком размыто, общо. С другой стороны, излишняя детализация только запутывает. Поэтому важно соблюсти правильный баланс. Не надо перечислять конкретные девайсы с подробным

описанием, как они должны использоваться. Лучше сосредоточить внимание на содержании. Например, приемлем такой вариант: «Компания отслеживает весь электронный трафик: почтовую переписку и все файлы, которые хранятся в сети и на мобильных девайсах, могут содержать служебную информацию и персональные данные. Компания имеет право доступа и просмотра всех сообщений и файлов на любом мобильном устройстве в любое время и без уведомления».

Наказание за нарушение инструкции. Следует четко прописать, что любое отклонение от установленных правил преследуется дисциплинарными взысканиями вплоть до расторжения трудового договора. Если замечено, что сотрудник ввел служебную информацию в свой домашний компьютер или персональный мобильник, ему ставится ультиматум: или немедленно приносит и сдает на контроль компьютер (мобильник), либо подлежит увольнению.

Важно упомянуть право компании передать расследование нарушений третьей стороне. Например, «компания оставляет право передавать информацию о нарушениях в правоохранительные структуры и/или другой третьей стороне, не спрашивая согласия сотрудников». Предупреждение, что информация, касающаяся работников, может быть предоставлена полиции, адвокатам или кому-либо еще, хороший аргумент в пользу соблюдения инструкции.

Еще один момент надо учитывать. Иметь в наличии инструкцию, с которой ознакомлен весь персонал, исключительно важно, если дело дойдет до суда.

Как обеспечить безопасность, работая в странах высокого риска

В погоне за прибылью транснациональные корпорации активно осваивают рынки таких стран как Ирак, Пакистан, Нигерия, Судан, для которых характерны политическая нестабильность, вооруженные конфликты, неразвитая инфраструктура, слабый контроль правительства на местах, низкий уровень здравоохранения и т.п. В таких условиях нередко работают и различные международные, в том числе неправительственные, организации.

Руководителям служб безопасности компаний и организаций, полагает Дэвид Хардинг, надо знать, как минимизировать риски для персонала, работающего в столь сложных условиях (securitymanagement.com, January 2013). Для этого требуются: тщательная предварительная разведка, налаживание хороших отношений с местным населением, умение правильно и быстро решать возникающие острые проблемы.

Распространенный способ получить предварительную информацию о ситуации в стране – воспользоваться услугами местной частной детективной или консалтинговой фирмы. Недостаток этого пути – отсутствие прямого выхода на носителей первичной информации и альтернативных источников. Автор советует организовать серию прямых контактов в формате «вопросы-ответы» с максимально возможным числом информаторов, живущих в стране, сравнивая данные, зачастую противоречивые, из разных источников.

Основной риск заключается в потенциально враждебном отношении местного

населения к иностранцам. Некоторые компании ведут себя неправильно, отгораживаясь от аборигенов высокой «китайской стеной». Это не спасает, а напротив, увеличивает риски. Автор статьи вспоминает, как, работая в послевоенном Ираке офицером связи в одной гражданской американской организации, он получил информацию, что местные жители затевают что-то недоброе. Как выяснилось, те заподозрили чужеземцев в «шпионаже». И это исключительно по причине добровольной изоляции, отсутствия нормальных контактов.

Чтобы расположить к себе население, Дэвид Хардинг рекомендует иностранным фирмам принимать участие в благотворительной деятельности, в частности, спонсировать работу социальных, медицинских организаций на местах. Это важно для создания благоприятного имиджа в глазах местных жителей, в конечном счете, для успешной работы.

Здесь важны мелкие детали. Например, некоммерческие и неправительственные организации напрямую раздают продовольствие и питьевую воду детям в бедственных районах. Родители этих детей могут испытывать чувство ущербности, собственной несостоятельности…Чтобы не вызывать раздражение, автор статьи, будучи в Ираке, пошел другим путем. Он предложил местному лидеру через него распределять помощь. Этот маневр сработал.

Автор приводит еще один пример из опыта своего пребывания в Ираке. Один из маленьких городков лишился электричества. Ему удалось убедить начальство своей компании достать и привезти в этот населенный пункт генератор, несмотря на неспокойную ситуацию по всему маршруту следования груза. Этим он поднял репутацию компанию в глазах населения.

В заключение Дэвид настоятельно рекомендует тщательно готовить персонал к работе в странах повышенного риска, заблаговременно составлять планы действий в потенциально возможных экстремальных обстоятельствах.

Ключевые вопросы для кандидата на работу в СБ

Эрик Коупертвейт, директор по безопасности медицинского центра Providence Health and Services в Вашингтоне, взял за правило: до решения о приеме на работу соискатель должен встретиться и побеседовать с сотрудниками службы безопасности, с кем ему, возможно, придется работать бок о бок. Мнение коллектива учитывается. Но прежде чем принять окончательное решение, Эрик должен задать и выслушать ответ на три важных вопроса.

Как Вы работаете, взаимодействуете с другими людьми?

«Мне важно знать, - говорит Эрик в интервью журналу Chief Security Officer (January 09, 2013) – как новый работник будет контактировать с коллегами не только внутри СБ, но и в других подразделениях компании». Умение работать в команде – важнейший критерий при приеме на работу.

Почему Вы добиваетесь именно этой работы и именно в нашей компании?

Выяснить мотивы кандидата – не просто удовлетворить любопытство. Нередко люди приходят исключительно для того, чтобы пересидеть в поисках другой, более желанной работы, для того, чтобы прибавить веса, солидности резюме. Один из кандидатов, отвечая на прямой вопрос, простодушно ответил: «живу рядом с вашим офисом и мне удобнее к вам добираться, можно сэкономить на электричке». Естественно, ему было отказано.

Какие у Вас ко мне вопросы?

Реакция также помогает прояснить мотивацию. «Когда спрашивают о зарплате и бонусах, то это не ко мне, - замечает Эрик, - Я готов отвечать на вопросы о работе службы безопасности, о стоящих задачах, о том, как они решаются, о перспективах профессионального роста, о роли нового члена коллектива в достижении целей. Вот вопросы, которые я бы хотел слышать».

В послужном списке Даниеля Кеннеди – работа руководителем в различных крупных организациях, в том числе в банке. Его стиль знакомства и собеседования более подходит для кандидатов на руководящие должности в структуре корпоративной безопасности. Вот его два любимых вопроса.

Как Вы будете добиваться права на свое место за столом топ менеджмента компании?

Кеннеди любит это вопрос, так как считает должность руководителя по безопасности стратегической в любой компании. Между тем, нередко бывает, что глава СБ теряется в организационной структуре, малозаметен, слабо влияет на важные решения. Однозначного ответа на этот вопрос нет. Однако, нередко выясняется, что соискатель просто об этом и не думал, у него нет ни плана, ни опыта, ни умения общаться с первыми лицами.

Какими способами и путями Вы добивались на прежней работе повышения значимости программ по безопасности до уровня главных приоритетов кампании?

Важно знать, какие задачи ставил кандидат и насколько успешно их решал. Если он(а) отвечает, что его (ее) роль сводилась всего лишь к рекомендациям и написанию всяких инструкций, то это негативный сигнал, вызывающий сомнения в способности соискателя обеспечить надлежащую роль СБ в деятельности организации. Но если в ответе содержится информация о тесном взаимодействии с профильными направлениями бизнеса компании, о конкретном влиянии СБ на конечные результаты, на цифру доходов, то ясно, что этот человек не просто узкий профессионал, но также и политик, способный завоевать авторитет и уважение, достойно представлять СБ в руководящем эшелоне компании.

Охрана торгово-развлекательного комплекса в праздничные дни

Молл Arden Fair в Сакраменто занимает территорию около 30 гектар. Его ежегодно посещают 10 миллионов покупателей, а в день в среднем 20-40 тысяч. С точки зрения безопасности комплекс не однороден. Его западная часть подходит вплотную к федеральной автостраде и именно здесь совершается большинство преступлений.

Восточное крыло в этом смысле спокойнее.

Стив Рид уже 13 лет возглавляет здесь службу безопасности. Самым большим достижением за эти годы он считает кардинальное обновление системы видеонаблюдения. Базирующиеся на DVR технологии 16 и 29 мегапиксельные камеры слежения обладают повышенной чувствительностью, высоким разрешением. Установленные на территории паркинга, они фиксируют подъезжающие машины и всё, что происходит здесь.

В дополнение к ним зона паркинга регулярно патрулируется машинами охраны. Установленные на них специальные считыватели отслеживают номера автомашин и сигнализируют, когда в фокус внимания попадают машины, находящиеся в угоне. Молл Arde Fair, возможно, единственный в США, напрямую связан с базами даннымих Министерства юстиции, где хранится информация о 220 тысячах угнанных автомобилей.

В интервью журналу Chief Security Officer Стив Рид с гордостью отмечает, что благодаря новым технологиям число угонов здесь сократилось в 10 раз. В 2011 году было зафиксировано всего 7 попыток угона (в 2006 году 77 случаев), причем четыре из них удалось предотвратить, а преступников задержать.

Самая большая нагрузка выпадает на рождественские праздники. Перед Рождеством и в праздничную неделю поток покупателей возрастает в разы. Чтобы справиться с наплывом, подготовка к этому празднику начинается накануне летом. С целью частично разгрузить паркинг, Рид подписывает договор с крупной транспортной компанией, которая в дни пик организует автобусное сообщение из расположенного неподалеку выставочного комплекса и других пунктов.

Для поддержания порядка и лучшего контроля за ситуацией в торговом центре и вокруг него Стив Рид договаривается с полицией Сакраменто о командировании в помощь ему профессионалов полицейских, которые обеспечивают в праздничные дни более 700 часов дежурства сверх работы собственной службы охраны комплекса. Также по договоренности с администрацией города Сакраменто меняется система дорожных знаков на подъездах и вокруг молла, чтобы избегать пробок и инцидентов.

Вся подготовительная работа занимает несколько месяцев и ведется по согласованию с торговыми фирмами, работающими в центре.

Охрана периметра крупных объектов

Этой теме посвящена публикация в журнале Security Magazine (January 2, 2013). Автор публикации Клэр Мейер рассказывает о проблемах охраны разных объектов – порта, студенческого городка, транснациональной корпорации.

Студенческий городок High Point University в последнее время заметно разросся. Только за последние 7 лет построены 42 здания, а территория увеличилась втрое. Сейчас весь кампус занимает более 100 гектар. Соответственно возрос и объем работы охранников. Их численность возросла с 12 до 70 человек. Весь городок обнесен забором, освещаемым в темное время суток и автоматическими воротами на въездах. «Поскольку кампус по определению должен выглядеть гостеприимно, - говорит

руководитель СБ университета Джефф Карпович, - по всему периметру мы организовали комнаты приема гостей. Охранник первым встречает гостей, изучает документы, сверяет с имеющейся в базах данных информацией о регистрации визитеров, оценивает внешний вид и поведение, т.е. осуществляет все необходимые процедуры, не забывая при этом проявлять вежливость и радушие. Вход для гостей разрешен с 6 утра до 10 вечера.
Контролю подвергаются не только приглашенные лица, но и персонал, и сами студенты. Случаются и факты несанкционированного проникновения, как случайного, так и намеренного. Каждый такой инцидент тщательно расследуется и фиксируется, отчеты хранятся.

Более сложные вопросы приходится решать директору по безопасности крупного производителя грузовиков корпорации Navistar International Corporation Джону Мартиники. Необходимо заботиться о безопасности персонала и имущества более 100 предприятий по всему миру. Охрана периметра каждого из объектов включает основные компоненты: системы СКУД, тревожную сигнализацию, цифровое видеонаблюдение. Но конфигурация различается в зависимости от местной специфики. Так, например, в Южной Африке делается упор на использование служебных собак. А в городе Мехико – на сенсорные устройства и патрулирование.

Директор по безопасности Massachusetts Port Authority Дэнис Трис согласен, что техническое оснащение охраняемого периметра необходимо. Но решения, в конечном счете, принимают люди. Самая умная видеокамера не может ответить на вопрос, кто данный потенциальный нарушитель – любитель фотограф, приблизившийся к периметру, или злоумышленник. Для преступника забор не помеха, он его перемахнет тем или иным способом. Забор нужен, чтобы у охранников было время подоспеть к месту происшествия и задержать нарушителя. Главное же, по мнению Триса, выстроить многоуровневые взаимоотношения между охраной и персоналом объекта, между службой безопасности и местной полицией.

Еще более важно – наладить контакты с ФБР. Именно через это федеральное агентство при наличии доверенных взаимоотношений можно получать ценную информацию относительно безопасности объекта и ситуации вокруг него.

Risk Analysis and the Security Survey

Risk Analysis and the Security Survey, Fourth Edition.
By James Broder and Eugene Tucker. Elsevier. 368 pages

Значение такого направления бизнеса как управление рисками резко возрастает в нынешней быстроменяющейся рыночной и корпоративной среде, пишет рецензент книги Терри Веттинг, руководитель группы международного аудита вопросов безопасности компании Brinks, Incorporation. Книга дает ответы на многие трудные проблемы вопросы, встающие перед теми, кто работает в этом направлении.

Книга состоит из двух основных разделов.

Первый раздел не только вводит читателя в сложный мир управления рисками, но и демонстрирует, что может произойти с бизнесом, с компанией, если эта работа осуществляется не на должном профессиональном уровне.

Во втором разделе речь идет о кризисном менеджменте, о путях и способах выживания бизнеса в экстремальных ситуациях, о том, какую поддержку могут оказать правительственные организации. Авторы книги настоятельно рекомендуют распространять анализ рисков на всю организацию, а не ограничиваться одним-двумя подразделениями, хотя бы и самыми важными с точки зрения бизнеса.

Книга содержит таблицы, графические приложения, образцы документов, в частности, планов на случай форс-мажорных обстоятельств (contingency plans),

По мнению рецензента, книга представляет собой ценный источник полезной информации для профессионалов в сфере корпоративной безопасности на всех ступенях служебной карьеры.

Risk Analysis and the Security Survey

Risk Analysis and the Security Survey, Fourth Edition.
By James Broder and Eugene Tucker. Elsevier. 368 pages

Значение такого направления бизнеса как управление рисками резко возрастает в нынешней быстроменяющейся рыночной и корпоративной среде, пишет рецензент книги Терри Веттинг, руководитель группы международного аудита вопросов безопасности компании Brinks, Incorporation. Книга дает ответы на многие трудные проблемы вопросы, встающие перед теми, кто работает в этом направлении.

Книга состоит из двух основных разделов.

Первый раздел не только вводит читателя в сложный мир управления рисками, но и демонстрирует, что может произойти с бизнесом, с компанией, если эта работа осуществляется не на должном профессиональном уровне.

Во втором разделе речь идет о кризисном менеджменте, о путях и способах выживания бизнеса в экстремальных ситуациях, о том, какую поддержку могут оказать правительственные организации. Авторы книги настоятельно рекомендуют распространять анализ рисков на всю организацию, а не ограничиваться одним-двумя подразделениями, хотя бы и самыми важными с точки зрения бизнеса.

Книга содержит таблицы, графические приложения, образцы документов, в частности, планов на случай форс-мажорных обстоятельств (contingency plans),

По мнению рецензента, книга представляет собой ценный источник полезной информации для профессионалов в сфере корпоративной безопасности на всех ступенях служебной карьеры.

Американские банки и их клиенты все более успешно противостоят интернет

криминалу

Исследовательская организация Financial Services - Information Sharing and Analysis Center (FS-ISAC) изучила, как американские банки защищают себя и своих клиентов от криминальных хакеров. В результате анализа состояния дел в почти 100 банках организация пришла к выводу, что банкиры и клиенты сегодня намного успешнее по сравнению с прошлым борются с попытками онлайновых взломов и краж.

Тенденция налицо, она подтверждается конкретной статистикой. В 2009 году 70% хакерских атак завершились уводом из банков денег. В 2011 году эта цифра снизилась до 12%, почти в шесть раз. В первой половине 2012 года только 9% хакерских атак, включая использование троянов, приемов фишинга и других видов интернет мошенничества, были успешными.

Объектами преступных посягательств в интернете в первой половине 2012 года стали 2.1% обладателей банковских счетов в финансовых учреждениях, охваченных проектом.

Исследование, проведенное по заказу American Bankers Association, не ставило задачей оценивать общий финансовый ущерб. Однако всё свидетельствует о том, что уровень потерь в последние годы также снижается, утверждает Билл Нельсон, глава FS-ISAC - группы экспертов, созданной еще в 1999 году для изучения киберпреступности.

Урон снижается в результате действия разных факторов, отмечает Нельсон. Клиенты банков осваивают новейшие методы персональной идентификации, все чаще используют компьютеры, эксклюзивно предназначенные только для банковских операций.

В 2009 году, когда эти виды банковских преступлений достигли пика, правоохранительные органы США серьезно взялись с ними бороться. Тогда же многие банки столкнулись с судебными исками по компенсации клиентам их потерь. Можно сказать, «клиенты проснулись».

Эффективной зарекомендовала себя практика обучения клиентов методам зашиты, своевременного закрытия скомпрометированных счетов, а также «ручной» контроль за большими трансакциями, совершенствование методологии регистрации и авторизации.

В то же время нельзя забывать, что преступники чрезвычайно умны, они умеют находить противоядие от новейших технологий защиты. Поэтому, подчеркивает Нельсон, рано успокаиваться, в будущем не исключен новый всплеск атак на банки.