Охрана предприятия

№4, 2008

Оглавление

Главная тема

В.Светозаров
Охрана предприятия в условиях финансово-экономического кризиса

Защита информации и интернет-технологий во времена финансового кризиса

Новые технологии, методологии

Сравнительные характеристики биометрических методов охраны предприятия

Конвергенция в охранной индустрии

Риски и угрозы безопасности бизнеса и организаций

Десять недооцененных аспектов охраны предприятия

Оценка состояния и уровня безопасности в школах

Защита гуманитарных миссий – новая роль для охранных предприятий?

Системы контроля и управления допуском

Охрана медицинского комплекса

Борьба с преступлениями среди персонала

Воровство металлов: слишком накладно, чтобы игнорировать

Проверка будущих сотрудников

Охрана малого предприятия

Не экономьте на охране

Книжное обозрение

Business Security: Over 50 Ways to Protect Your Business!
by T. A. Brown , 2004

Профессиональная этика

Кодекс профессиональной этики Ассоциации охранных предприятий Новой Зеландии

Охрана предприятия за рубежом

Американский супермаркет: сложные взаимоотношения между охранниками и покупателями

Исследования

Программы по безопасности в транснациональных компаниях

В.Светозаров, Охрана предприятия в условиях финансово-экономического кризиса

Разразившийся в мировом масштабе финансово-экономический кризис, так или иначе затрагивает все сферы и аспекты бизнеса. Охрана предприятия – не исключение. В тяжелые времена эта индустрия подвергается повышенному риску. Во-первых, все внимание предпринимателей фокусируется на проблемах выживания и некоторые, кажущиеся второстепенными вопросы, включая безопасность, уходят на задний план. Во-вторых, кризис ведет к сокращению персонала и огромное число работников, имеющих доступ к секретной служебной информации, оказывается под угрозой увольнения. В-третьих, вынужденная экономия средств зачастую оборачивается резким снижением расходов на охрану. Наконец, в-четвертых, резко возрастает уровень преступности.

«Многие предприниматели урезают статьи на безопасность в период финансового кризиса, - пишет Роджер Шмедлен, специалист по физической охране из Мичигана, - а между тем, именно в такое время имеет смысл уделять безопасности бизнеса повышенное внимание. Охрану предприятия трудно измерять с точки зрения рентабельности производства. Когда все тихо и спокойно (благодаря надежной охране предприятия), то у руководства может появиться мысль, что, собственно, и незачем особенно беспокоиться о безопасности, появляется искушение здесь сэкономить».

Если сокращение персонала, включая охрану, неизбежно, то, как считают западные эксперты, целесообразно сконцентрировать средства и время на тренингах по безопасности для всех остающихся в фирме сотрудников. «Возможно, самое важное,

что могут сделать управляющие компанией в условиях сокращения штата – вкладывать деньги в обучение и тренинг сотрудников по вопросам безопасности», отмечает Джон Бамбенек, эксперт из Иллинойса.

Эрни Хейден, глава консалтинговой компании 443 Consulting, говорит о необходимости сделать всех работников «частью единой команды по охране и безопасности фирмы». По его мнению, через обучение и тренинги следует развивать «паранойю подозрительности» в отношении сомнительных электронных сообщений, приходящих в компанию, а также неадекватного поведения коллег…

Чем глубже экономика погружается в кризис, тем чаще регистрируются случаи классического воровства: золотых часов в магазинах, металла на производстве, ценного оборудования в офисах. Крис МакГойи, эксперт по вопросам безопасности, рост воровства в торговых центрах напрямую связывает с сокращением персонала, в том числе и занятого в охране. Однако главной причиной роста воровства он считает падение уровня жизни населения: «Даже у обычно честных людей нет-нет, да появляется искушение что-нибудь приобрести задаром. В районах с бедным населением воровство продуктов, сигарет, алкоголя становится обычным явлением».

Кражи на американских предприятиях принимают угрожающий характер. В последние месяцы высокой популярностью у преступников пользуются изделия из меди. Особенно страдают коммунальная и энергетическая сферы: тащат в первую очередь медные провода (отдельный материал о воровстве металлов см. в этом номере журнала).

Уоррен Аксельрод, отмечая необходимость уделять первоочередное внимание охране предприятия в условиях кризиса, предлагает ряд рекомендаций. В частности:

Управление допуском. Когда под воздействием кризиса происходят организационные и функциональные изменения, необходимо заново проконтролировать, кто и куда имеет доступ, проанализировать, кто и как пользуется правом проходить в различные здания и помещения предприятия. Соответственно изменившимся условиям работы предприятия списки доступа пересмотреть, ужесточив контроль.

Предотвращение злоупотреблений и воровства. Когда смерч «Катрина» обрушился на побережье США, все стали свидетелями жуткой волны мародерства и иных преступлений в районах стихийного бедствия. Конечно, сейчас нет прямых параллелей с финансовым смерчем, захлестнувшим Уолл Стрит и весь мир. Однако финансовая и экономическая дестабилизация создает благоприятные условия для роста криминала. Поэтому так важно усилить физическую охрану предприятия в эти сложные времена. Это делать нелегко, когда все вокруг рушится, когда не хватает оборотных средств, но крайне необходимо.

Защита информации. В быстроменяющихся условиях обмен финансовой информацией между разными организациями и внутри предприятия ускоряется невиданными темпами. И это обстоятельство требует усиленного внимания к защите данных, принятия всех возможных мер по предотвращению случайных и злонамеренных утечек.

Технологические вызовы. Обычно переход к новым технологиям занимает многие месяцы. Нынешний кризис требует немедленных, быстрых действий. Нет времени на планирование, продумывание всех деталей. Поэтому надо сконцентрировать внимание

тех новых технологиях, которые в потенциале могут представить серьезные риски для безопасности бизнеса.

Человеческий фактор. Важно проявить чисто человеческое внимание к работникам предприятия, которые, естественно, беспокоятся за свою судьбу. Тогда служащие будут более адекватно вести себя в сложных условиях. В конце концов, кризисы рано или поздно заканчиваются, и жизнь продолжается. И кто знает, как взаимоотношения в трудный период работы скажутся в будущем на климате в коллективе.

(На основе материалов веб-сайтов www.csoonline.com, www.bloginfosec.com/2008/09/30 и других интернет-ресурсов)

Защита информации и интернет-технологий во времена финансового кризиса

Известная западная исследовательская и консалтинговая фирма по вопросам управления интернет-технологиями Enterprise Management Associates (EMA, www.enterprisemanagement.com) выпустила аналитическую записку о возросших угрозах для корпоративных информационных систем и технологий вследствие финансового кризиса.

Совершенно очевидно, что разразившийся кризис вынуждает самым пристальным образом обратить внимание на проблемы защиты информации и управления рисками, говорится в записке. Профессионалы, работающие в этих областях, должны задуматься о том, с чем они могут столкнуться, заранее подготовиться к неприятным последствиям».

Среди перечисленных в записке угроз и рекомендаций, можно выделить следующие моменты (использована публикация на сайте www.quantasesecurity.com):

* Злоумышленники (прежде всего хакеры) предпочитают «ловить рыбку в мутной воде». Их жертвами могут стать, в первую очередь, кредитопользователи, отчаянно ищущие возможности расплатиться с банками. Профессиональные мошенники наверняка будут предлагать «легкие пути» выхода из положения.

* Объектом атак могут стать и финансовые организации, переживающие сложные времена, – хотя бы из простой мести.

* Дополнительные опасности проистекают из убыстряющихся процессов слияния и поглощения на фоне банкротства ряда финансовых организаций, когда один из конкурентов «заглатывает» другого. При этом «заглатываются» не только бизнес-процессы, но и инфраструктура, призванная обеспечить защиту этого бизнеса. Здесь и открываются дополнительные возможности для преступников, которые рассчитывают на то, что клиенты банка, фирмы не сразу узнают о перемене владельцев и их можно поймать на удочку фишинга.

* Важно, чтобы меры по обеспечению безопасности бизнеса распространялись не

только на инструменты защиты, но и на все сети, системы, которые задействованы на предприятии и могут стать объектом атаки со стороны преступников.

* «Самая большая угроза финансового кризиса для безопасности интернет-технологий, - отмечается в аналитической записке EMA, - кроется в менталитете корпоративных руководителей. Если они по-прежнему будут рассматривать эти технологии исключительно с позиции их главного предназначения, и лишь время от времени - с точки зрения потенциальных угроз для защиты бизнеса, то вопросы безопасности предприятия так и не выйдут на уровень тех требований, которые предъявляет кризисная ситуация».

Сравнительные характеристики биометрических методов охраны предприятия

Сравнительные характеристики биометрических методов охраны предприятия

Продолжаем публикацию в кратком изложении исследования Хантера Памелла и Дэна Маркса «Биометрическая безопасность предприятия» (www.ncycle.com). Начало см. в журнале №3

Идентификация по рукам

Этот метод используется, как правило, для охраны крупных объектов по причине больших размеров контрольного устройства, которое, кстати, стоит недешево в сравнении с другими системами биометрической проверки. Обычно применяется для обеспечения безопасности помещений, где хранится секретная информация, особых зон внутри офисов, и самих зданий.

Удобство в использовании среднее

Уровень безопасности средний

Степень распространенности средняя

Отпечатки пальцев

Используется специальный сенсор с недорогим биометрическим чипом. Особенно хорош этот метод для контроля допуска в компьютеры и сети. Небольшие по размеру устройства могут быть легко встроены в информационные технологии.

Удобство в использовании высокое

Уровень безопасности среднее

Степень распространенности высокая

Сетчатая оболочка глаза

Применяется довольно сложная техника, не очень удобная для пользователя (проверяемого лица). Некоторые фирмы, правда, пытаются создать небольшое устройство, которое можно было бы также устанавливать на верхнюю панель компьютерных мониторов. Тем не менее, пока что это используется главным образом для контроля за физическим допуском (в помещение, здание).

Удобство в использовании низкое

Уровень безопасности высокий

Степень распространенности средняя

Радужная оболочка глаза

Принцип сканирования в целом такой же, как в предыдущем случае. Отличается в лучшую сторону тем, что не требует позиционирования глаза в определенной точке.

Удобство в использовании низкое

Уровень безопасности высокий

Степень распространенности средняя

Голос/произношение

Система верификации выстроена исключительно на алгоритмах, программном обеспечении. Используется для приложений дистанционного управления. К примеру, в здравоохранении - находящийся дома пациент клиники сообщает с помощью специальных телефонных устройств о том, как протекает болезнь, как действуют лекарства и т.п.
Известно широкое применение данной технологии в системах электронного шпионажа. Пока реже – в коммерческих целях, но перспективы здесь есть.

Удобство в использовании высокое

Уровень безопасности средний

Степень распространенности средняя

Почерк/подпись

Биометрическая верификация отличается от обычного способа сравнения почерка или подписи тем, что с большей точностью фиксирует степень нажима, расстояние между словами и строчками, и даже скорость написания. Хороший метод для выявления подлогов и фальшивок: даже если злоумышленник достаточно точно скопировал почерк, разница в нажиме и скорости поможет разоблачению. Однако надо иметь в виду, что один и тот же человек может со временем менять характер написания. Поэтому абсолютизация идентификации может обернуться необоснованными

сомнениями в подлинности автографа. Метод особенно распространен в финансовой и правовой сферах экономики.

Удобство в использовании низкое

Уровень безопасности высокий

Степень распространенности средняя

Лицо

Сканируются характерные особенности лица, которое, впрочем, с годами меняется. Наиболее эффективное применение – в условиях дистанционной идентификации, когда нельзя использовать методы сканирования по рукам, пальцам, глазам.

Удобство в использовании высокое

Уровень безопасности низкий

Степень распространенности низкая

Особенности движения

Этот способ заключается в мониторинге характерных особенностей походки, а также движения рук при работе на компьютере и в других случаях. Требует использования достаточно сложной технологии с пространственными и временными параметрами, определенного ракурса. Поэтому наиболее практично применять данный метод для идентификации при работе на компьютере, поскольку в этом случае объект зафиксирован по месту.

Удобство в использовании высокое

Уровень безопасности средний

Степень распространенности низкая

Конвергенция в охранной индустрии

Индустрия физической охраны сегодня находится на перепутье в виду бурного роста информационных технологий, которые все более интегрируются с электронными системами безопасности. Хотя между физической и ИТ системами охраны немало общего, последняя развивается значительно быстрее, ее технологическое обновление измеряется не годами, а месяцами.

В исследовании на сайте www.securitygrowthconference.com отмечается, что сейчас перед компаниями, работающими в сфере физической охраны, стоит выбор. Или продолжать развиваться по проторенному пути, достаточно самостоятельно, независимо, модернизируя собственные технологии, а также заимствуя инновации из

других секторов экономики. Или же выбрать иной путь, предполагающий радикальное изменение продукта (услуг), внедрение новой бизнес-модели, основанной на интеграции с Интернет-системами безопасности.

Авторы исследования, подчеркивая преимущества второго пути, подробно анализируют те возможности и проблемы, с которыми сопряжена данная альтернатива. Они выделяют три аспекта конвергенции физической и ИТ видов охраны.

1. Конвергенция технологий

Она предполагает интеграцию информационных технологий (базы данных, программное обеспечение, кабельные и беспроводные компьютерные сети, методы информационного процессинга) в электронные системы безопасности (идентификация, контроль за физическим допуском, видео и аудио-наблюдение, мониторинг безопасности). Это приведет к тому, что значительная часть либо все функции физической охраны сольются с бизнес-процессами собственно охраняемой организации. При этом технологическая конвергенция происходит в рамках компетенции специалистов по интернет-технологиям, в то время как службам физической охраны предстоит серьезная перестройка.

2. Интеграция систем

Речь идет о внедрении программных приложений в физическую охрану. Эти приложения охватывают такие функции безопасности как, например, идентификация личности, контроль за допуском - как в помещения, так и в сети, мониторинг безопасности. Интеграция способствует преодолению технологического разрыва между возможностями физической охраны и ИТ систем, достигающего порядка нескольких лет.

3. Интеграция менеджмента

Имеется в виду создание объединенной службы, которая бы отвечала за все риски, связанные с безопасностью бизнеса, включая информзащиту. В то время как непосредственное руководство такой службой осуществляет специально назначаемое должностное лицо – Chief Security Officer, первые лица компании, принимающие стратегические и тактические решения, постоянно контролируют работу службы как интегрированной части бизнеса. Преодоление «сепаратизма» означает огромный прорыв в индустрии безопасности. К сожалению, этот процесс тормозится из-за психологической неготовности ряда компаний, занятых в сфере физической охраны, к данной интеграции. В то же время перед интернет-компаниями открываются новые возможности проявить себя на рынках физической охраны.

(продолжение в следующем номере журнала)

Десять недооцененных аспектов охраны предприятия

Продолжаем изложение материала, опубликованного 29 ноября 2006 года под этим названием на сайте www.darkreading.com

2. Защита служебной информации

У крупных компаний ежедневные отходы, т.н. «мусор», измеряются тоннами. Там, где нет четкой политики по уничтожению использованной документации, устаревшего оборудования, в горах мусора можно откопать золотые крупинки важнейшей, конфиденциальной информации, за которой охотятся конкуренты и преступники.

Для них настоящим сокровищем, например, может оказаться выброшенный на свалку использованный жесткий диск. Очень часто компании, модернизируя информационные технологии, старые компьютеры и другую ставшую ненужной офисную технику отправляют в утильсырье, либо дарят школам, разным благотворительным фондам, или просто выбрасывают в мусорные контейнеры, не удосуживаясь тщательно выскрести из памяти всю служебную информацию.

В ходе одного из международных исследований, посвященных этому вопросу, на рынках разных стран мира приобрели более 300 б/у жестких дисков. На многих дисках обнаружили информацию, которую нужно было бы уничтожить перед продажей. В том числе: данные о зарплатах, имена и фото сотрудников, интернет-адреса, информацию по сетям, номера мобильных телефонов, копии инвойсов, номера банковских счетов.

И это касается не только отслуживших компьютерных дисков. Авторы другого исследования закупили старые мобильные телефоны. На 9 из каждых 10 аппаратов обнаружили далеко не безобидную для бывших владельцев информацию.

«Система файлов в мобильнике такая же, как в компьютерах, - отмечает эксперт Норм Лаудермилх (компания Trust Digital) , - нажимая на кнопку «delete», вы не уничтожаете информацию, а просто меняете индекс файловой системы».

И, конечно, нельзя недооценивать старейший способ кражи корпоративной информации – бумажные отходы. Джим Стиклей (компания TradeSecurity) говорит, что, роясь в кучах мусора одной компании, он обнаружил массу весьма чувствительной служебной информации, которая не прошла через специальную технику для уничтожения документов».

Оценка состояния и уровня безопасности в школах

В журнале The High School Magazine, Vol.6 No.7, May/June 1999 опубликована статья Кеннета Трампа «Снижение рисков через оценку степени безопасности в школах».

Автор выделяет три довода в пользу регулярной проверки состояния безопасности в школах:

1. Обеспечить готовность к предотвращению и противодействию актам насилия.
2. Снизить риски и угрозы.
3. Повысить репутацию школы в глазах общественности.

Конечно, пишет автор, проверки еще не гарантируют от опасных инцидентов, не являются панацеей от потенциальных угроз. Их задачи сводятся к тому, чтобы оценить существующий уровень безопасности, выявить уязвимости, сформулировать рекомендации по усилению охраны. Проверка начинается с администрации, но должна вовлекать в процесс также учащихся, их родителей, представителей охранного предприятия, местные правоохранительные органы.

В идеале проверка должна проводиться профессионалами с опытом охраны учебных заведений. Может ли администрация школы сама организовать проверку? Автор отвечает положительно, но подчеркивает, что итоги будут весьма ограниченными в сравнении с результатами, которые способна дать работа профессионалов в этом деле.

Проверка безопасности это не просто прогулка по помещениям школы, хотя и не требует, с другой стороны, «парализующего все и вся анализа». Она включает обязательные беседы с администрацией, оценку проводимых мероприятий и мер по обеспечению безопасности, анализ криминогенной ситуации в районе, осмотр помещений.

Профессиональная проверка безопасности школы включает следующие вопросы и компоненты:

* *Штат охранников*. Достаточно ли персонала, занятого в охране школы? Насколько охранники профессионально подготовлены?

* *Проводимые мероприятия по обеспечению безопасности.* Насколько они адекватны конкретной ситуации, новым возможным угрозам?

* *Инструкции на случай чрезвычайной ситуации.* Имеются ли в наличии? Не устарели? Содержат ли рекомендации для действий в различных обстоятельствах («что делать, если…»)?

* *Подготовка и тренинги.* Проводятся ли учения и тренинги? Их количественная и качественная оценка.

* *Физическая охрана.* Что можно сделать для улучшения работы СКУД, системы охраны по периметру, поддержания безопасности в ночные часы и в не учебное время?

* *Кадровая безопасность.* Достаточны ли меры по соблюдению безопасности при приеме сотрудников, по информационной безопасности и другим вопросам, связанным с человеческим фактором?

* *Взаимодействие с правоохранительными органами, местным управлением МЧС, районной и городской администрациями, родительским комитетом и общественностью*. Что нужно и можно здесь улучшить?

Защита гуманитарных миссий – новая

роль для частных охранных предприятий?

Автором статьи, размещенной на сайте известной международной корпорации ArmorGroup, является Джеймс Феннел, имеющий немалый опыт работы по оказанию гуманитарной помощи в неспокойных районах Африки, Центральной Азии и в бывшей Югославии (www.armorgroup.com/armorview).

По его мнению, проблемы обеспечения безопасности различных гуманитарных миссий, которые призваны оказывать помощь населению, пострадавшему в результате этнических войн и иных конфликтов, требуют привлечения и использования опыта коммерческих охранных предприятий. Он пишет: «Возможно, для коммерческих охранных предприятий пришло время более активно участвовать в дискуссиях на тему о том, как лучше защитить население, ставшее жертвой гуманитарной катастрофы». Автор не ограничивает роль коммерческих компаний участием в обсуждениях. Он считает необходимым для них напрямую участвовать в гуманитарных миссиях, обеспечивая безопасность как самих миссий, так и местного населения.

Как показывают события практически во всех конфликтных зонах, где население нуждается в защите и гуманитарной помощи, сотрудники миссий подвергаются серьезной опасности стать жертвой насильственных действий. Причем - не случайной жертвой. Полевые командиры нередко рассматривают международные гуманитарные миссии как серьезную помеху для своих военных действий, направленных на запугивание и деморализацию местного населения.

Особенно большому риску подвергаются гуманитарные миссии в тех конфликтных зонах, где их деятельность не обеспечивается и не защищается миротворческими вооруженными силами. Таких зон предостаточно – Судан, Ангола, Конго (Браззавиль)…

Международное вмешательство для защиты населения могло бы, подчеркивает автор, воспользоваться кадрами и опытом коммерческих охранных предприятий. При этом он отмечает, что речь не идет о военной составляющей. Непосредственное участие в вооруженном конфликте «нанесло бы непоправимый ущерб репутации охранного предприятия».

Но что тогда могут предложить охранные предприятия?

В первую очередь, помочь гуманитарным агентствам лучше подготовиться к работе в неспокойных районах, имея в виде обеспечение безопасности членов миссии и имущества. В гуманитарные миссии необходимо, по мнению Феннела, включать квалифицированных специалистов, которые на месте способны оказать поддержку не только в защите миссии, но и в «роспуске или обезвреживании боевых групп», в разминировании местности, в решении иных задач, требующих специальной подготовки.

Любой руководитель гуманитарного агентства обязан сознавать, что малейший организационный промах из-за недостатка соответствующего опыта и квалификации, может привести к гибели его сотрудников. Он должен понимать, как важно реалистично и всеобъемлюще планировать и осуществлять работу по защите членов миссии и имущества. В этом процессе охранные предприятия могут выступать в

качестве легитимных и весомых партнеров.

Охрана медицинского комплекса

На сайте www.securitysolurions.com подробно раскрывается структура охраны крупного медицинского центра в американском штате Коннектикут, который включает отдельно стоящие здания клинической больницы на 617 мест, отделения для новорожденных (более 60 мест), научно-образовательного центра, школы медсестер, хирургического и онкологического отделений. Здесь работают более 3000 служащих и 600 врачей. Служба безопасности насчитывает 135 человек – как контрактных охранников, так и сотрудников по безопасности из числа административного персонала.

Руководит службой безопасности женщина – Люсьетта Данлоп. У нее богатый опыт работы в охранном бизнесе: президент и партнер местной охранной корпорации, руководитель по безопасности крупной страховой компании, а также директор службы охраны и детективов универмага в столице США. «Когда я пришла в медицинский комплекс в 1990 году, - говорит она, - здесь практически не было систем по охране. Но времена меняются, требуя все более серьезного контроля за безопасностью».

Начиная, по ее словам, «с нуля», Л. Данлоп создала полностью интегрированную систему охраны, которая включает практически все, что используется сегодня в индустрии безопасности – от камер видеонаблюдения до детекторов движения. В зданиях имеются 105 камер наблюдения. В помещениях архива, во врачебных кабинетах и других помещениях, которые пустуют во внерабочие часы, установлены инфракрасные детекторы. Вестибюли для посетителей и служебные входы контролируются видеокамерами и детекторами движения.

«В числе первых шагов, сделанных мною здесь, - рассказывает Данлоп, - резкое сокращение количества входов для посетителей». Что же касается служащих медицинского комплекса, то на всех служебных входах установлены специальные считыватели электронных пропусков и видеокамеры. Камерами видеонаблюдения также охватывается прилегающая к зданиям комплекса территория с парковками автомобилей. Видеонаблюдение интегрировано с другими охранными системами, в частности, противопожарной.

Особое внимание уделяется охране родильного и детского отделений. Там действует специальная система, использующая электронные бирки для новорожденных. Если предпринимается не санкционированная попытка вынести новорожденного из отделения, немедленно включается тревожная сигнализация на этаже и на центральном пункте охраны. Одновременно электронными средствами блокируются все двери, так что никто не может ни войти, ни выйти из отделения, пока не подоспеют офицеры по безопасности. На экране видеомонитора крупным масштабом возникает дверь, через которую пытались пронести ребенка.

Упомянутый пункт охраны позволяет осуществлять из одного места (в данном случае – комнаты) мониторинг всех функций по охране во всех зданиях и помещениях. Здесь

постоянно – 24 часа в сутки, семь дней в неделю – дежурят 3 офицера службы безопасности.

Для персонала СБ предусмотрена специальная тренинговая программа. Базовая подготовка осуществляется охранным предприятием First Security Services Corp (город Бостон), которое имеет свой филиал в районе расположения медицинского комплекса. Как только новые охранники выходят на службу, с ними проводят 16-часовой тренинг по специальной программе, включающей ознакомление с особенностями функционирования медицинских учреждений, задействованными здесь охранными технологиями и оборудованием, например, пожарной сигнализацией, системой электрической безопасности и т.п.

Последнее происшествие, потребовавшее вмешательства СБ, связано с попыткой кражи строительных инструментов. Монитор видеонаблюдения в центральном пункте охраны зафиксировал некоего мужчину, который пытался протолкнуть тележку, используемую обычно в супермаркетах, через один из турникетов на выходе. Туда немедленно прибыли офицеры по безопасности, задержали подозреваемого и передали его местной полиции. В тележке обнаружили инструменты для всяких строительных нужд на сумму свыше $1 000. Мужчина пришел в клинику и зарегистрировался как посетитель одного из больных. Получив разрешение, он действительно встретился с пациентом больницы, а на обратном пути решил прихватить оставленный без присмотра набор строительных инструментов.

Воровство металлов: слишком накладно, чтобы игнорировать

Воровство металлических изделий с целью продажи – проблема не только российская. Спрос на металлолом в последние годы возрастал. Только в США этот рынок в 2007 году оценивался в 61 миллиард долларов. Соответственно росла и цена. Перед финансовым кризисом за килограмм лома меди в США давали почти 8 долларов, за алюминий – более двух долларов, титан – около десяти долларов. Не удивительно, что в Америке кража металлоизделий для последующей продажи приняла масштабы, которые, по мнению экспертов, нельзя игнорировать. В ход идет все, что содержит ценные металлы, что плохо или совсем не охраняется, например, медные трубки кондиционеров на крышах домов и офисов, дорожные указатели,… Нередки в США и кражи непосредственно из цехов металлообработки. Все это сдается в пункты приема металлолома, причем приемщики не слишком щепетильны. Обычно не интересуются, откуда металлы, не требуют документы. Ситуация нам в России знакомая и понятная.

Между тем, во многих американских штатах имеются скрупулезно разработанные законы и правила, регламентирующие этот бизнес. Например, в штате Калифорния местный «Кодекс бизнеса и профессий» обязывает пункты скупки металлолома документировать время и место каждой сделки, имя и личные данные продавца, регистрационный номер автомашины, на которой доставлен металлический груз. Все эти данные должны храниться в течение 2 лет. В реальности же требования не исполняются.

Директор управления корпоративных услуг компании Diversified Risk Management

Реджина Мартинец, опираясь на личный опыт многочисленных расследований краж металлов, рассказывает в своей публикации на сайте www.diversifiedmanagement.com/articles/:

«Один из наших клиентов, фирма в Лос-Анжелесе, производящая металлоизделия, обнаружила, что ежемесячно теряет сырье на сумму $5 000. Глава фирмы не понимал, кто и как ворует металлы, просил провести независимое расследование. Мы отправили к нему «на работу» залегендированного агента. Он вскоре обнаружил, что один из работников, контактирующий по должности с субподрядчиком, не документировал объем и вес металла, который должен возвращаться на фирму. С помощью скрытой съемки был прослежен путь украденного металла и место его сбыта. Когда подняли документацию приемщика металлолома, то обнаружилось, что похититель давал ложные данные о себе, выдавая за человека, который к тому времени уже 10 лет отбывал тюремное наказание. По факту возбуждено уголовное дело».

В другом случае, рассказанном автором статьи, в компанию обратилась фирма, работающая в сфере коммунальных услуг. С территории фирмы регулярно воровали медные провода электросети, нанося убыток в десятки тысяч долларов. Проведенное расследование обнаружило слабые места в охране территории. Совместно с местной полицией был выслежен и задержан молодой человек, наркоман с криминальной историей. Он признался в регулярных кражах медных проводов. В ходе допроса воришка был обескуражен и расстроен, когда ему сказали, что сбытая им за несколько сотен долларов медь на деле стоила почти $100 000.

Проверка будущих сотрудников

Чтобы быть уверенным в своих сотрудниках, необходимо перед наймом проводить глубокую проверку их служебной и личной истории. Часто проверка осуществляется самой компанией, но в последние годы все чаще обращения в специализированные фирмы – информационно-поисковые или охранные организации.

В их числе – компания AlliedBarton. Руководитель отдела компании по персональным ресурсам Джим Коллинс говорит, что «одна из первых рекомендаций, которые он дает обращающимся в компанию клиентам – проанализировать свои риски. Располагая ясной картиной рисков, и директор по безопасности клиентской организации, и компания, осуществляющая персональные проверки, четко видят, на что надо обращать особое внимание, проверяя прошлое кандидатов на работу» (www.securityinfowatch.com/article/).

Коллинс также добавляет, что наряду с первичной проверкой целесообразно проводить повторное расследование, а в некоторых случаях организовывать проверку отдельных сотрудников ежегодно: «Слишком часто компании ограничиваются первой проверкой при приеме на работу, а затем на годы забывают об этой важной для безопасности процедуре».

Другой эксперт, Билл Вайтфорд (вице-президент компании ChoicePoint), советует бизнесменам тщательно выбирать фирму для персональных проверки, ориентируясь на ее репутацию, отзывы других клиентов, убедившись, что фирма строго следует законодательству в работе с персональными данными.

Кроме проверки будущих сотрудников на предмет их моральных качеств, важно выяснить, имеют ли они право на работу в вашей компании. Речь идет в первую очередь об иммигрантах. Игнорирование этого аспекта может привести к неприятным последствиям для компании, если иммигрантов собираются принять на работу охранниками или, например, уборщиками, которым по роду занятий доступны источники служебной информации (компьютеры, печатные документы). Поэтому в каждом таком случае желательно обращаться в государственную организацию, занимающуюся вопросами иммиграции, для перепроверки информации, предоставленной кандидатом о себе.

Глубина, интенсивность проверки напрямую зависит от должности, на которую претендует кандидат. Чем шире полномочия, доступ к секретной информации, тем, естественно, проверка должна быть глубже, тщательнее, детальнее. По словам Коллинса, его компания берет информацию из различных источников, включая данные из территориальных судебных органов. Обычная проверка занимает несколько часов. Если полученная информация не удовлетворяет или настораживает, процесс может занять несколько дней. Средняя стоимость проверки - $40.

В другой фирме – ChoicePoint, по свидетельству Вайтфорда, проверка обычно требует от 2 до 5 дней, ее стоимость для клиента колеблется от $20 до $100.

Не экономьте на охране

В один прекрасный день руководитель небольшой американской компании по тренингу обнаружил, что ночью в офисе побывал вор. Из компьютеров, общая стоимость которых вместе с сервером превышает $40 000, вор взял только два – бухгалтера и кадровика. Избирательность не случайная. Ясно, что его интересовала не стоимость «железа», но финансовая и персональная информация. Фирма знает толк в проведении тренингов, но не в деле охраны - компьютеры не имели ни ключей, ни паролей к жестким дискам.

Расследование обстоятельств кражи выявило ряд интересных моментов. Входная дверь имеет тревожную сигнализацию. Но поскольку всякий раз последними уходят разные сотрудники, бумажка с кодом сигнализации наклеена у стола секретарши, т.е. доступна всем, включая учащихся. А так как никто из сотрудников фирмы не отвечает персонально за охрану, не исключено, что в ту ночь сигнализация вообще не была включена. Возможен и другой вариант – преступник был днем в офисе (вероятно, как участник тренинговых занятий), заметил и запомнил код сигнализации, чем и воспользовался позднее.

Эта история, рассказанная на сайте www.bizsecurityabout.com, иллюстрирует набирающую силу тенденцию к увеличению подобного рода краж преимущественно в офисах небольших компаний, которые плохо охраняются. Преступников все чаще интересует не материальные вещи, а содержимое компьютеров.

Исследование, проведенное фирмой Nilson, показывает, что такие преступления в США обходятся бизнесу в $20 миллиардов ежегодно. Если в 2005 году 52% опрошенных компаний заявили о случаях воровства в офисах, то в 2006 году их число выросло до 66%.

Причина роста преступности очевидна. Подавляющее большинство руководителей малых предприятий не заботятся о безопасности бизнеса. Многим из них кажется, что тратить деньги на охрану – все равно, что платить за страховку от наводнений в пустыне. Они считают, что если есть деньги, то лучше их потратить на новые технологии, сулящие рост прибылей. На охране экономят, пока гром не грянет. Требуется время и совершенно иное сознание, чтобы безопасность фирмы рассматривалась как неотъемлемая часть бизнес- планирования и стратегии.

Т. Браун, Безопасность бизнеса: более 50 способов защитить ваш бизнес

Business Security: Over 50 Ways to Protect Your Business!
by T. A. Brown , 2004

подробности на сайте http://www.amazon.com

Отклики читателей и экспертов

BC Nina “Nina” (Канада)
Сюжеты этой книги весьма поучительны. Здесь говорится о вещах, над которыми мы обыкновенно редко задумываемся, но которые несут немалые потенциальные угрозы. Хотя название книги указывает на охрану бизнеса, книга полезна и для тех, кто заботится о своей личной, персональной безопасности. Книга увлечет всех, кто интересуется вопросами безопасности, независимо от того, занимаются они бизнесом или нет.

M. Enchelmaier (Германия)
Эта книга представляет собой очень ценное пособие для бизнесменов. В первую очередь для тех, кто занят в международном бизнесе, использует современные информационные технологии, включая Интернет.

Treyce d”Gabriel (г. Феникс, США)
Мне довелось ознакомиться со многими книгами по вопросам безопасности и хочу сказать, что эта книга – одна из лучших. Как руководитель малого предприятия я уже в течение 16 лет, знаю на практике, что такое быть объектом некорректного поведения со стороны и собственных работников, и конкурентов. В книге можно встретить оценки экспертов по безопасности, работающих в самых разных отраслях экономики. Книга подтверждает известный тезис: «предупрежден, значит, вооружен».

Marion Gropen, консультант по издательским вопросам (США)
Насыщенная полезной информацией, книга позволяет приступить к решению проблем, связанных с возникающими рисками. Хотите провести проверку кого-либо, вам задолжал партнер/клиент, - что бы ни произошло, откройте книгу и читайте, что надо делать. Я десятилетия руководил сотрудниками и бизнесом. Но, даже имея большой практический опыт, кое-чему научился, прочитав книгу. Теперь она всегда у меня на столе.

Роберт Сичилиано
Как эксперт и автор публикаций по вопросам безопасности, я нахожу, что данная

книга великолепна. Прекрасное, полезное чтение для представителей равно большого и малого бизнеса. Отличная работа.

Кодекс профессиональной этики Ассоциации охранных предприятий Новой Зеландии

Члены Ассоциации охранных предприятий Новой Зеландии обязуются:

1. Поддерживать высокие стандарты честности и справедливости во всех взаимоотношениях с клиентами и своими служащими, с другими членами ассоциации и общественностью.

2. Осуществлять профессиональную деятельность в интересах общества.

3. Предоставлять достоверную и точную информацию о своих услугах, как и об услугах компании, которую они представляют. Не прибегать к методам обмана.

4. Предоставлять по требованию Ассоциации письменное изложение деталей заключенных с клиентами соглашений, включая стоимость услуг, условия контракта, выплату штрафов и т.п.

5. Своевременно и адекватно отвечать на жалобы клиентов.

6. Не наносить ущерба профессиональной репутации и практике коллег, клиентов, других членов Ассоциации, разрешать спорные вопросы с клиентами или другими членами Ассоциации в соответствии с требованиями Ассоциации.

7. Не злоупотреблять конфиденциальной информацией, в том числе полученной от нового сотрудника, работавшего ранее в другой компании.

8. Хранить в тайне конфиденциальную информацию о клиенте, раскрывать ее не иначе как с разрешения клиента и в соответствии с законом.

9. Не вступать в отношения с другими членами Ассоциации во вред интересам клиентуры.

10. Строго следовать Кодексу профессиональной этики Ассоциации, Правилам Ассоциации, законам и нормам Новой Зеландии.

Сокращенный перевод материала, размещенного на сайте www.security.org.nz

Американский супермаркет: сложные

взаимоотношения между охранниками и покупателями

Американец Крис МакГоий много лет консультирует по вопросам безопасности. С 1996 года ведет собственный веб-сайт www.crimedoctor.com, где отвечает на различные поступающие к нему вопросы, в том числе, относительно взаимоотношений покупателей и охранников в магазинах и супермаркетах. Предлагаем вниманию читателей некоторые вопросы и ответы.

Я действительно намеревался совершить кражу компакт-дисков, но затем передумал и положил их на место перед выходом из магазина. Однако охрана меня все равно задержала. Имела ли она на это право?

В некоторых штатах Америки попытка спрятать товар рассматривается как кража независимо от того, передумали вы или нет, ибо такая попытка уже говорит о намерении украсть, и этого достаточно для признания факта криминала. В большинстве же магазинов США едва ли вас задержат, если вы положили товар на место. Но на такое отношение все же рассчитывать нельзя. В вашем конкретном случае надо обратиться к адвокату за советом.

Могут ли охранники подсматривать за мной во время примерки в закрытом помещении?

Нет! Посетители торговых центров могут смело надеяться, что их частные права не будут нарушены ни в примерочных комнатах, ни в туалетах. Устанавливать видеонаблюдение в таких помещениях запрещено законом. Однако служащие магазинов могут контролировать ваши действия в примерочной или вне ее, если подозревают, что вы намереваетесь что-то пронести мимо кассы.

Не должен ли я покинуть магазин, прежде чем меня остановит охрана, подозревая в краже?

Законами большинства штатов разрешено задерживать покупателей, заподозренных в краже, внутри магазина. Крупные сети имеют, однако, офицеров по безопасности для задержания вне магазина, если кого-то подозревают.

Как член ассоциации покупателей розничной сети я пользуюсь скидками в магазинах сети. Имеет ли право охрана устраивать проверку моих покупок на выходе?

Такие проверки проводятся обычно по правилам, устанавливаемым самими магазинами, а не законом. Формально покупатели не должны подчиняться правилам. На деле же в официальных документах содержится право охранников проверять на выходе чек, а также досматривать покупки - как условие членства в ассоциации покупателей. Либо вам надо с этим мириться, либо... не вступать в члены ассоциации и не покупать здесь вовсе.

Я был остановлен охранниками и обвинен в краже комплекта батареек, который принес с собой из дома. Охрана игнорировала мои объяснения. Какие у меня есть права?

Очевидно, у секьюрити магазина иное мнение. Охранники уверены, что вы пытались совершить кражу. Возможно, они ошибаются. В таком случае вы можете апеллировать к управляющему магазином, чтобы вас отпустили, или готовиться защищать себя в суде с помощью хорошего адвоката. Документы о приобретении батареек в другом месте и свидетели будут не лишними.

Программы по безопасности в транснациональных компаниях

Международная организация Исполнительный совет по безопасности (Security Executive Council) обнародовала результаты опроса, проведенного среди транснациональных компаний относительно их программ и планов по охране предприятий (www.securityinfowatch.com).

Обнаружен факт: только в 27% опрошенных компаний имеется специальная группа по контролю безопасности, которая регулярно собирается на совещания. При этом примечательно, что среди корпораций, входящих в список Форчун 500, регулярно проводят совещания по вопросам безопасности 87 процентов. В то же время среди компаний из списка Форчун 50 000 таких организаций всего 15 процентов.

«То, что менее трети международных компаний проводят совещания на регулярной основе, а не только лишь при возникновении рисков и угроз, удручает, - говорит Кэтлин Котвица, вице-президент SEC, - к тому же нередко такие совещания проводятся в узком составе, регионально, в то время как «общую картину» можно воссоздать только при участии в обсуждении проблем представителей всех филиалов и отделений компаний.

Исследование также показало, что в более чем половине опрошенных компаний существуют тесное взаимодействие между службой безопасности и корпоративными юристами на предмет отслеживания особенностей законодательства в странах, где компания имеет бизнес. 67% респондентов заявили, что у них разработаны и реализуются планы мониторинга местных законов и норм. Как отмечает К.Котвица, «Мы постоянно слышим жалобы компаний на то, как сложно отслеживать и действовать в согласии с законами в других странах. Поэтому не случайно наблюдается тесное взаимодействие между юристами и офицерами по безопасности: для международных компаний правовые аспекты играют исключительно важную роль в обеспечении безопасности».