Охрана предприятия

№4 (32), 2013

Оглавление

Money Laundering: A Guide for Criminal Investigators, Third Edition

Исследования

Что более приоритетно – производительность или защита данных?

Как создать эффективную службу безопасности

Корпоративная служба безопасности призвана решать проблемы бизнеса, а не только охраны, утверждает Микаэл Линч, директор СБ компании DTE Energy в Детройте. По его словам, необходимо освобождаться от стереотипных подходов к этому виду деятельности, господствовавших на протяжении многих десятилетий (securitymagazine.com, 3 June, 2013).

В прошлом, говорит Линч, в службу безопасности компании зачастую набирали людей, не способных проявить себя в других сферах занятости. Затем стали привлекать профессионалов из силовых структур. И это был шаг в правильном направлении. Но сегодня и этого уже недостаточно.

Линч подчеркивает, что ныне он формирует команду из людей, имеющих опыт работы в разных сферах, связанных с безопасностью. В команде есть бывшие работники правоохранительных органов, в том числе отставники ФБР. Наряду с ними работают бывшие сотрудники прокуратуры, специалисты в области информационных технологий, люди с опытом службы в кадровых подразделениях. Кроме того, в СБ есть работники, отличающиеся особенной креативностью и предпринимательскими способностями. Такой разброс в бэкграунде штатных сотрудников помогает более успешно реагировать на проблемы бизнеса, так или иначе связанные с безопасностью.

Серьезное значение имеет выстраивание правильных взаимоотношений с менеджментом компании, укоренение взгляда на безопасность как на не последний фактор бизнеса. Линч в этой связи вспоминает, как несколько лет назад руководство компании пожаловалось на несанкционированные отборы электроэнергии в сетях, попросту говоря – на кражи энергии. Этим вопросом президент попросил заняться службу безопасности, хотя охрана сетей и не входила в прямые обязанности СБ. В течение пары лет сотрудниками СБ было совершено 386 задержаний злоумышленников. Кривая краж резко пошла вниз. Это, естественно, отразилось на финансовых результатах компании.

Президент DTE Energy Джерри Андерсон со своей стороны подчеркивает, что руководитель корпоративной службы безопасности работает фактически как профессиональный бизнесмен, хорошо разбирающийся в приоритетах и проблемах компании, выстраивающий на этой основе собственные планы и тактику, которая помогает достижению конечных целей компании.

«В своей работе я ориентируюсь на 7 критериев, - отмечает в той же публикации

журнала Security Management Джон Тьюри, руководитель департамента управления рисками и безопасности глобальной корпорации TE Connectivity Ltd., имеющей бизнес в 90 странах мира, - Это уважение к коллегам, честность, соблюдение корпоративной этики, умение работать в команде, упорство, инновационный подход, способность к развитию и совершенствованию таланта». Все эти моменты в совокупности составляют стиль руководства. Возглавляемый им департамент занимается в основном управлением рисками, вопросами безопасности и охраны, проблемами выживания бизнеса в условиях кризиса. Большую часть рабочего дня он проводит за изучением рыночных трендов, оценивая стратегию и цели компании, стремясь ответить на вопросы: «насколько работа департамента отвечает этим целям, как выполняются поставленные задачи, имеются ли в его команде талантливые сотрудники, отвечающие целям и вызовам, с которыми организация может столкнуться в недалеком будущем».

Клод Небель, вице-президент компании со 150-летней историей Global Security of Cargill в городе Миннеаполисе, делится опытом стимулирования творческого подхода сотрудников компании к своим обязанностям. Он вовлекает их в процесс выработки стратегии компании, в подготовку различных проектов и планов. Ничто так не делает людей причастными к общему делу, как включенность в процессы планирования стратегии и программ, говорит он. Небель также практикует регулярные встречи со своими подчиненными, во время которых обсуждает не только текущие и перспективные дела, но и, насколько этично и возможно, их личную жизнь: «То, что волнует, беспокоит человека вне рабочего времени, так или иначе, отражается и на выполнении им своих должностных обязанностей. Поэтому важно знать, что тревожит коллегу, чем мы можем ему помочь», заключает Клод Небель.

Биометрическая аналитика: баланс безопасности, удобства, ненавязчивости

Охранные биометрические системы постоянно совершенствуются, пишет Билл Залуд, редактор и автор онлайнового журнала Security Magazine, в статье опубликованной 8 мая 2013 года. Они становятся все более точными. Многие активно применяются, поскольку очень удобны в обращении и эксплуатации. Общая тенденция – гармонизация функции безопасности с удобством для пользователей, когда они не раздражают и не требуют сверхусилий.

Наибольшую популярность в повседневной практике приобрели отпечатки пальцев и геометрия руки (hand geometry). Довольно распространен метод идентификации по сетчатке, радужной оболочке глаза, кровеносным сосудам ладони, конфигурации лица. Все чаще входят в моду такие биометрические показатели как распознавание голоса, особенностей печатания на компьютерной клавиатуре, движения тела во время ходьбы. В числе недавно появившихся технологий автор статьи называет биохимию ДНА (DNA), строение ногтей и даже запах тела.

У каждого способа свои плюсы и минусы. Общий для них и главный критерий – точность. К примеру, сетчатка глаза превосходит отпечаток пальца по точности,

однако пользователи находят отпечатки пальцев более удобным, «комфортабельным» способом идентификации и проверки. Тем более, что отпечатки обеспечивают достаточно высокую степень безопасности.

Считыватели отпечатков пальцев с 2005 года используются в системах СКУД второго в Европе по объему грузооборота порта Амстердама и крупного порта Zeebrugge (Бельгия), где расположен самый большой в Европе терминал природного газа. Структура большого морского порта требует, чтобы работающие там люди, а также постоянные посетители, представляющие разные компании, могли свободно перемещаться между различными зонами и зданиями, имея на руках единый для всех постов СКУД электронный пропуск - смарткарту с биометрическим отпечатком пальца. Считыватели сверяют биозапись на карте с хранящимися в базах данных СКУД данными.

Индустрия биометрии в охранном деле зависит от сравнительно небольшого числа компаний, инвестирующих в биометрические алгоритмы, и интеграторов, которые внедряют средства биометрии в охранные системы, отмечает автор. Он приводит такой пример. Компания Samsung Techwin America вступила в партнерство с фирмой FaceFirst (программные продукты) с задачей приспособить систему распознавания лица для мегапиксельных камер видеонаблюдения. Камера схватывает изображение лица и одномоментно сверяет со списком фотографий в базе данных. Результаты идентификации немедленно отправляются (в зависимости от предназначения системы сверки) в компьютеры СБ, на сотовые телефоны, или регистраторы наличного оборота.

Аналогичные или схожие методы лицевого распознавания используются в системах уличного видеонаблюдения, на спортивных сооружениях, в учебных заведениях, везде, где поток людей ничем и никем не прерывается.

Биометрия находит широкое распространение и в обеспечении информационной безопасности. Так, в частности, в результате партнерства с производителем программных решений информзащиты Watchful Software одна глобальная консалтинговая компания по вопросам управления информационными технологиями внедрила у себя систему классификации и шифрования информации, препятствующую попыткам несанкционированного входа изнутри и извне в корпоративные базы данных. Здесь используются или планируются к использованию в самое ближайшее время биометрические технологии, в частности, метод идентификации по ритму и манере работы на компьютерной клавиатуре. Этот метод построен на измерении индивидуальных особенностей каждого пользователя компьютером, а именно – времени, когда клавиша нажата (т.е в положении «key down»), а также промежутком времени между переходом с одной клавиши на другую (между «key up» и «key down»).

Как улучшить охрану магазина без создания проблем для покупателей

Хорошая охранная система стоит немало денег, сильно обременяет бюджет. Стремящиеся на всем экономить торговые компании не понимают, что капиталовложения в системы охраны - зачастую вложения не в средства охраны, не в технологии безопасности, а в инфраструктуру. К примеру, магазины обычно имеют

кабельные аналоговые системы видеонаблюдения, но многие хотят обзавестись IP камерами с функцией дистанционного мониторинга. При этом не учитывают, что для IP камер требуется сеть Ethernet, довольно дорогостоящая, особенно если в здании нет для этого соответствующей инфраструктуры.

Выход из ситуации гибридные технологии. Например, специальные конверторы (media converters) оцифровывают видео изображения, которые передаются от аналоговых камер слежения, значительно повышают качество картинки.

Гибридные решения появились на рынке сравнительно недавно. Их уникальность в том, что они могут использовать коаксильные кабели для передачи как аналоговых, так и цифровых изображений. Они хороши в тех случаях, когда торговые фирмы, полагая полный переход на Ethernet слишком дорогостоящим предприятием, хотят уменьшить затраты на новое оборудование, утилизируя уже имеющеюся кабельную инфраструктуру. Гибридные решения позволяют использовать прежнее оборудование в мониторинговом центре.

Если бюджет магазина ограничен, то лучше начать с установки камер внешнего слежения, считает Франк Де Финна, старший вице-президент компании Sales & Marketing при корпорации Самсунг. Мегапиксельная технология позволяет минимизировать количество камер, необходимых для полного обзора. Мегапиксельные камеры надо размещать в первую очередь при входе, а также в районе паркинга, чтобы отслеживать потоки покупателей. Если позволяет бюджет, можно начать постепенное размещение камер внутри магазина, в первую очередь, в тех разделах, где самые дорогие товары или высокий уровень краж.

Видеонаблюдение все чаще используется как средство защиты брэнда. Отделение корпорации Тойота в Северном Голливуде традиционно использовало аналоговое видеонаблюдение для предотвращения краж и вандализма. В ходе модернизации охранных систем камеры, установленные в пяти залах торгового центра и в паркинге, были заменены на цифровые, что позволило отслеживать малейшие детали происходящего в магазине и вокруг, включая контроль за работой персонала. По мнению менеджеров, переоснащение видеонаблюдения положительно сказалось на работе служащих, на их подготовке и обучении, так как теперь можно показывать и критически разбирать работу продавцов.

Видеонаблюдение становится неотъемлемой частью стратегии безопасности бизнеса, которая начинается с базовых основ – охранной и пожарной сигнализаций, а также включает системы СКУД – не только на входах в торговый центр, но и в помещениях хранения товаров, в комнатах администрации. Эксперты настаивают, что помещения, куда разрешен вход только персоналу, должны охраняться с помощью электронных карт, перекодирование которых намного проще, чем смена замков в случае потери ключей.

Dreamless Wireless, небольшая фирма по продаже беспроводных коммуникаций в Карлсбаде, штат Калифорния, закупила систему видеонаблюдения, решая задачу минимизации воровства и краж без найма охранников. Система состоит из 5 цифровых камер и интегрированной сети, обеспечивающей функцию СКУД и видео аналитику через единый интерфейс. Сюда же интегрированы пожарная и дверная сигнализации. Владелец магазина Киршнер особенно высоко ценит возможность просматривать видео в режиме реального времени и архивы в любой момент и из любого места, поскольку ему приходится часто разъезжать по делам.

(по материалам журнала Security Magazine, 1 April, 2013)

Новые охранные технологии для кампусов

Студенты университета Susquehanna (штат Пенсильвания) используют новое приложение в своих смартфонах, которое позволяет моментально информировать службу охраны в случае опасности. Подавляющее большинство учащихся (всего студентов здесь более двух тысяч) живут в университетском кампусе, а некоторые предпочитают снимать жилье в близлежащем городке Selinsgrove. В целом этот район достаточно спокойный. В кампусе иногда случаются кражи, было несколько случаев сексуального преследования и конфликтов (драк). Служба охраны, насчитывающая 8 профессионалов, поддерживает тесные связи с местной полицией. Кроме того, круглосуточно работают 30 камер видеонаблюдения, большая часть которых предназначена для внешнего контроля (по периметру кампуса), а несколько камер установлены в студенческом клубе и рядом с банкоматами. На территории кампуса (около 200 га) действует система телефонов тревожной сигнализации (blue light phones).

Тем не менее, администрация университета нашла средства для закупки программного продукта EmergenSee U, который намного эффективнее (и дешевле) традиционных средств охраны и наблюдения. Система эта работает следующим образом. В персональные айфоны, айпады, андроиды и прочие девайсы, принадлежащие студентам, загружается специальное программное приложение. Всякий раз, когда студент, находясь на территории кампуса и даже вне его, чувствует, что подвергается опасности (преследование, угроза нападения и т.п.), он просто нажимает на соответствующую иконку на экране своего смартфона, который немедленно начинает транслировать изображение от встроенной видеокамеры на монитор службы охраны, одновременно передавая GPS координаты нахождения студента. Все эти данные поступают дежурному диспетчеру службы охраны. Он запрашивает, нужна ли помощь. Студент может ответить, нажимая высвечиваемые на экране девайса кнопки «да», «нет», «все нормально». Все сигналы и переговоры записываются и архивируются для последующего возможного использования.

К этому надо еще добавить, что местная полиция разрешила университету расширить зону действия системы на город Selinsgrove и предместья. Таким образом, студент, находясь за пределами кампуса, способен быстро сообщать и ориентировать службу охраны о потенциальных угрозах. Диспетчер эту информацию тут же пересылает в отделение полиции.

Система может решать самые разные задачи. Например, сообщать о последствиях стихийных бедствий, о пожарах…В частности, система хорошо показала себя во время урагана Сэнди.

В настоящее время 500 студентов загрузили приложения системы. При этом все расходы взял на себя университет. Довольна администрация. Довольны и родители.

В будущем планируется расширять функциональность системы и зону покрытия на значительные расстояния, включая зарубежные поездки студентов на стажировку.

(по материалам журнала Security Magazine, June 2013)

Доверяй, но проверяй

В наши дни, когда персональные и корпоративные данные «уходят» из офисных баз данных в «облачные» технологии и мобильные носители информации, пословица «доверяй, но проверяй», становится все более актуальной и востребованной, пишет в журнале Canadian Security, 8 April, 2013, Тони Болл. Пословица адекватно отражает реальность нынешнего мира, где контакты между людьми все больше смещаются в онлайн. Поэтому как никогда ранее мы нуждаемся в механизмах проверки идентичности тех, с кем вступаем во взаимодействие.

Как показывает опыт, идентификация надежна тогда, когда она не ограничивается простыми паролями. Между тем, организации обычно фокусируют внимание на защите периметра своих сетей, полагаясь на статичные пароли для идентификации пользователей внутри организации. Этого совершенно недостаточно, особенно учитывая массовое распространение практики «принеси в офис свой девайс». Пароль как единственное средство защиты легко преодолевается злоумышленниками и нуждается в дополнительных факторах защиты. Более того, мульти-факторная идентификация должна стать частью эшелонированной стратегии безопасности, которая бы включала идентификацию девайсов, защиту браузеров, проверку вступающей в контакт с вами стороны, защиту приложений. Чтобы все это иметь, необходима программа обнаружения угроз в реальном времени и интеграционная платформа.

Автор отмечает, что в онлайн-банкинге и электронной торговле довольно широко используется технология, помогающая выявлять мошенничество. Изменения в этой сфере характеризуются внедрением жестких правил и норм безопасности, в первую очередь защиты клиентских данных. Строгие требования безопасности включают полный диапазон средств идентификации и предотвращения мошенничества, используемых при совершении платежей в онлайне и с мобильных носителей.

Что касается «облачных» технологий, то сегодня дискуссии вокруг защиты «облачных» данных концентрируются, в основном, на вопросах обеспечения безопасности платформы. Поскольку компании продолжают отправлять свои приложения в «облака», выбирая для себя модель «программное обеспечение как сервис» («Software as a Service»), по мнению автора, критически важно выстроить гибкую систему ввода и отмены идентификационных данных пользователей для всех «облачных» приложений, одновременно обеспечивая простой и надежный вход пользователей в эти приложения.

Технологии идентификации еще более востребованы с распространением практики «принеси в офис свой девайс». Отделы ИТ не всегда в состоянии контролировать использование персональных носителей, насыщать их антивирусными и прочими защитными программами. Организации не могут оставлять у себя личные девайсы, когда сотрудники увольняются. Важно искать нестандартные, инновационные пути решения проблем безопасности. Автор советует обратиться к опыту все более популярного применения в системах СКУД смартфонов, ноутбуков и иных мобильных устройств. Здесь он видит возможности использования бесконтактных моделей

идентификации для работы в корпоративных сетях. В частности, смартфоны могли бы служить не только электронным пропуском в служебное здание, в офисное помещение, но и ключом идентификации для входа в корпоративную сеть.

Безопасность как фактор доходности компании

Шон Кларк, учредитель и президент консалтинговой фирмы Clark Consulting Group, рассказывает на сайте securitymagazine.com (4 июня 2013) о способах продемонстрировать доходность эффективной охраны предприятия для компании.

Для этого надо, чтобы «заработала» база данных конкретных фактов успешной работы СБ. Приложение Excel и более современные программные приложения позволяют суммировать и вести учет всех сторон работы СБ, а также образовывать и поддерживать единую интегрированную систему управления корпоративной безопасностью, куда закладываются все данные, включая финансовые аудиты, результаты тестирования физических и информационных систем защиты, факты обнаружения и предотвращения мошенничества, внутрикорпоративных расследований и так далее. Одно-два нажатия мышкой и на экране монитора высвечивается досье историй, связанных с разоблачением попыток мошенничества или воровства за тот или иной период времени, скрупулезно переводимых в цифры потенциальных, но не случившихся финансовых потерь.

Особенно важно, подчеркивает Кларк, показать, что департамент безопасности – не «пожиратель» бюджета компании, а приносящая дополнительный доход структура. Это возможно в том случае, если налажена работа по анализу и предотвращению мошенничества и воровства (fraud analytics strategy). С помощью информационных технологий накопленные по данному направлению данные не только отвечают на вопросы: кто, что, где, когда, почему и как, но дают т.н. «большую картину» возвращенных компании средств как в исторической ретроспективе, так и в режиме «реального времени». А в некоторых случаях – и прогностическую перспективу (ориентировочную величину предупрежденного потенциального ущерба).

Инновационные программы безопасности, охватывающие fraud analytics strategy, способны обнаруживать и предотвращать не только факты криминала, но и чисто производственные упущения, ошибки в управлении бизнесом, для исправления которых бывает достаточно быстрых технических мер или изменений в корпоративных политиках. Но такой широкий охват разнородных проблем требует налаживания тесного партнерства службы безопасности с другими департаментами компании – продаж, маркетинга, связей с клиентами, информационных технологий… Такой подход помогает формировать репутацию службы безопасности как структуры с большим видением (big vision, big picture), способной решать задачи помимо прямых, непосредственных функций СБ. Но всё впустую, если не налажена система информирования менеджмента, персонала компании о проводимой СБ работе, главное – о практических результатах. Первые лица компании, и особенно прямой куратор в совете директоров, должны быть в курсе всех значительных успехов – фактов, переложенных на понятный руководителям язык цифр сэкономленных, возвращенных средств.

Не менее важно взаимопонимание с внешними партнерами. К примеру, взаимодействие с владельцами арендуемого компанией здания/помещения необходимо для нахождения и реализации эффективной, продуктивной конфигурации системы внутреннего и внешнего видеонаблюдения, максимальной отдачи от СКУД, точного учета и контроля потоков клиентов и персонала компании. Значение эффективной службы безопасности не ограничивается подсчетом предотвращенных убытков, подчеркивает Шон Кларк. Ее успешная работа – залог репутационных показателей, котировки бренда, в конечном счете – высокой корпоративной культуры.

Как обеспечить охрану товаров во время транспортировки и хранения

Согласно исследованию, проведенному фирмой Deloitte, процессы глобализации, связанное с ними стремление предпринимателей повышать эффективность своего бизнеса, в том числе снижением себестоимости, накладных расходов, серьезно увеличивает риски по цепочкам поставок. Их становится больше, а сами риски все дороже. В результате 71% бизнесменов полагают сегодня, что без учета рисков, связанных с прохождением товаров по всей цепочке поставок, стратегическое планирование невозможно (securitymanagement.com, April 1, 2013).

По мнению авторов исследования, для управления рисками в этой сфере ключевую роль играют следующие факторы:

• Прозрачность. Способность прослеживать движение товара по всему маршруту и своевременно выявлять сопутствующие риски.

• Гибкость. Способность незамедлительно реагировать на возникающие проблемы без серьезных дополнительных затрат.

• Тесное взаимодействие с партнерами – поставщиками, транспортными и охранными предприятиями.

• Контроль. Означает иметь в наличии соответствующие корпоративные политики, а также средства мониторинга и контроля.

Аналогичные факторы могут быть отнесены и к вопросам хранения товаров. Охрана складских помещений и дистрибьютерских центров имеет два аспекта – внутренний и внешний.

Одна из проблем заключается в расположении видеокамер внутри помещений. Склады, как известно, имеют длинные проходы, которые только частично покрываются традиционными методами видеонаблюдения. По мнению Эндрю Элвиша, вице-президента маркетинговой фирмы Genetec, целесообразно использовать вертикальный прямоугольник обзора вместо традиционного горизонтального.

Другая проблема – правильно отстраивать систему контроля на входах в складские помещения (СКУД). Эксперты считают, что количество пропускных пунктов напрямую зависит от потока визитеров, насколько он регулярен. Если их много, то стоит подумать об отдельном входе для посетителей. Для помещений, где хранятся редкие

и ценные металлы, подойдут металлические детекторы как средство борьбы с воровством.

Кроме персонала и визитеров следует держать под контролем и грузовые автомашины. Помимо забора вокруг охраняемой территории, целесообразно установить на въезде и выезде специальные считыватели госномеров, которые бы фиксировали время прибытия, убытия автомашин, время их нахождения на территории склада. Контроль за транспортом и посетителями особенно важен, если ворота открыты практически весь рабочий день. Следует обучать и тренировать персонал на предмет выявления незнакомых лиц, подозрительных личностей.

Охрана внутреннего двора входит обязательным компонентом в план обеспечения безопасности. Камеры слежения должны покрывать всю территорию внутри забора, обладать функцией изменения масштаба изображения (zoom), а также работать эффективно при тусклом ночном освещении.

Эксперты полагают, что системы мониторинга и контроля в процессах транспортировки и хранения грузов имеют значение, выходящее за рамки простого обеспечения охраны товаров. Это технологии, формирующие бизнес и делающие его более эффективным.

О методологии проверок при приеме на работу новых сотрудников

Это теме посвящена публикация в журнале Security Magazine (April 1, 2013) профессора Грэга Аллена, ведущего курс управления безопасностью бизнеса в университете Bellevue.

Автор отмечает несовпадения в подходах экспертов. Сам он полагает, что при наличии разных должностных функций методология проверки соискателей зависит исключительно от того места в организации, на которое он претендует. А вот по мнению Барри Никсона, исполнительного директора Национального института по предупреждению насилия на рабочих местах, необходим единый стандарт проверок для всех должностей в организации – от кассира в бухгалтерии до генерального директора. Никсон считает, что кого бы на работу ни брали, надо проводить проверку на возможное криминальное прошлое, по крайней мере, за последние 7 лет, в картотеках (базах данных) города, района и федерального уровня. Он также настаивает на необходимости проверки данных об образовании.

Одна из проблем, с которой сталкиваются кадровики и офицеры по безопасности, это материальные затраты на проведение проверок. Чтобы минимизировать затраты, пишет Аллен, надо отсеять заявления (резюме), которые показывают, что соискатель не подходит, либо плохо, неправильно составлены. Обычно предварительный анализ и отбор присланных резюме сокращает список соискателей процентов на восемьдесят. Второй этап – собеседование, в результате которого остаются 3-4 кандидата, а то и меньше. После этого проводятся проверки. По мнению Аллена, чем выше должность, тем тщательнее, а, следовательно, и дороже, проводится проверка.

Согласно Марку Винну, директору по безопасности компании Ingram Micro, при приеме

на ответственные, требующие доверия должности проверка должна включать: криминальный бэкграунд за последние 7 лет; кредитную историю; информацию местных и региональных госструктур, а также информацию на федеральном уровне.

Эксперты едины во мнении, что рискованно зачислять соискателя на работу до завершения его проверки. Но такое случается нередко. Подобное следует исключить для рабочих мест, связанных с допуском в корпоративные базы данных, для ответственных должностей. Например, для соискателей на работу в бухгалтерии, в отделе информационных технологий...

В 2012 году Комиссия США по обеспечению равных возможностей на трудоустройство постановила, что организации не вправе отказывать в приеме на работу на том основании, что кандидат арестовывался или сидел по суду. Исключения распространяются на случаи, когда соискатель претендует на должности, требующие особого доверия (финансы, допуск к конфиденциальной информации, высокая степень ответственности), а также в зависимости от тяжести наказания и как давно это произошло.

Эксперты настаивают на необходимости также проводить аналогичные проверки уже зачисленных в штат, работающих в организации сотрудников, особенно, перед назначением на новую, более высокую и ответственную должность, связанную с финансами и/или допуском к служебной информации.

«Черные лебеди» как непредвиденные факторы риска

Что такое «черный лебедь» в терминологии западных специалистов по безопасности? Определение дает профессор Патрик О. Конноли в статье для журнала Security Magazine, May 21, 2013: «Чаще всего это экономическое событие, которое, как правило, невозможно спрогнозировать с помощью традиционной методологии и технологии управления рисками - ERM (Enterprise Risk Management) и которое представляет серьезную угрозу для бизнеса».

По мере глобализации мировой экономики, указывает автор, такие риски возрастают:

геополитические тенденции;
экономические тенденции;
тенденции в сфере права, регулирования;
неустойчивость рынков;
технологические изменения;
условия окружающей среды (включая экологию);
волны терроризма;
традиционная концентрация внимания на внутренних рисках бизнеса;
отсутствие опыта и знаний работы с внешними рисками.

Правильный подход к «черным лебедям» требует от организаций четко различать риски, которые можно предвидеть, рассчитать, спрогнозировать, и риски, которые не поддаются научным расчетам, которые можно лишь обозначить в ходе сценарного

анализа в рамках разработки стратегии.

Для проведения сценарного мозгового штурма необходимо поставить и постараться ответить на следующие вопросы:

- Какого рода события могут случиться?
- Какие события наиболее вероятны?
- Какова вероятность, что событие, характеризуемое как «черный лебедь», может произойти?
- Если такое событий случится, то какие стороны бизнеса оно затронет?
- Какие меры, например, быстрое информирование по всем коммуникационным каналам компании, могут и должны быть предприняты для минимизации угрозы?

Имея в виду разные сценарии развития событий, важно понять их возможное воздействие на:

1. стратегию выживания
2. уровень, методы и эффективность работы с клиентами
3. репутацию организации
4. финансовые результаты

Все выводы и соображения в ходе сценарного анализа необходимо тщательно документировать.

Риски зарубежных поездок

На сайте securitymagazine.com опубликована статья, посвященная рискам, которыми чреваты поездки в развивающиеся страны.

Джеффри Грубер многие годы жил и работал в разных странах, является экспертом по вопросам безопасности зарубежных командировок и путешествий. Он подчеркивает, что компании должны специально готовить к таким поездкам своих сотрудников. В противном случае, последние могут стать жертвой преступлений – от мелких краж до похищений. Он обращает внимание, что в большинстве частных компаний, даже в крупных корпорациях, на эти вопросы обращают мало внимания, плохо знают особенности стран, куда командируют своих работников, не имеют планов подготовки и тренингов.

Такая подготовка перед поездкой обязательна. Она должна включать рекомендации, как пользоваться местным транспортом, прежде всего такси. По прилете в аэропорт, предупреждает автор публикации, не следует брать нелицензионное такси. В некоторых странах, например, Латинской Америке, действуют банды: под видом таксистов увозят из аэропорта прибывших в страну иностранцев в укромное местечко, где у них отбирают деньги, кредитки, ценные вещи, а в ряде случаев подвергают сексуальному насилию. Поэтому правильно поступают те, кто не отвечает на предложение частных «бомбил», а обращается в транспортные местные агентства, представленные во всех крупных аэропортах мира. И еще одно важное замечание. Если вас встречает водитель принимающей стороны, желательно, чтобы на табличке в его руке было написано не имя и фамилия гостя, не название компании, а нечто

нейтральное по заблаговременной договоренности.

Когда вы выбираете отель, то обращайте внимание не только на стоимость номеров, но и на вопросы безопасности, рекомендует другой эксперт, президент компании Secure Source International в городе Сиэтл Дэвид Никастро. Он советует брать номер не выше 8 этажа, так как это предельная высота для стандартной выдвижной лестницы пожарных команд. Также необходимо удостовериться, что дымовые детекторы в наличии и работают исправно, что дверь на запасную (пожарную) лестницу открыты и проход на нее свободен. Кроме того, важно поставить в известность посольство или консульство своей страны о себе.

Все эти вещи проговариваются в ходе подготовки к поездке наряду с медицинскими аспектами (прививки, эпидемии, особенности климата, воды, продуктов). Особое внимание надо уделять вопросам защиты информации. Командированные по делам компании обычно берут с собой в дорогу персональные компьютеры со служебной информацией, мобильники с деловой перепиской, распечатанные документы. Нельзя ни на минуту забывать, отмечает Грубер, что конкуренты могут внимательно следить за вашими перемещениями, охотиться за интересующей их информацией. Поэтому так важно перед поездкой вновь просмотреть принятые в вашей компании политики безопасности и действовать им сообразно. А именно: перед посадкой и до выхода из аэропорта отключать все электронные носители, заранее убедиться в наличии пин-кодов и паролей на всех девайсах и системы шифрования на компьютерах.

В некоторых странах официально, как компонент политики безопасности, в аэропортах могут сканировать информацию компьютеров и мобильных девайсов , замечает Грубер. Среди таких стран он называет Россию: «Здесь надо быть готовым к досмотру ручного багажа, включая мобильные устройства, причем, часть багажа может на некоторое время остаться вне вашего внимания, и, не исключено, просканирована, включая информацию в компьютере» (securitymagazine.com, June 2013). Правда, эксперт оговаривается, что такой досмотр вполне легален и протесты бесполезны.

Несколько советов как добиться необходимого финансирования программ информационной безопасности

Рекомендации предлагает главный офицер по информации (chief information officer) Международного аэропорта в Лос-Анжелесе Доминик Неси (онлайновый портал Chief Security Officer, April 19, 2013).

Прежде всего, наладьте хорошие рабочие взаимоотношения с теми, от кого зависит решение о выделении финансовых средств. Это надо сделать заблаговременно, до того, как вы представите свои предложения по бюджету.

Подготовьте и представьте документы, подтверждающие квалификацию - вашу и ваших подчиненных (дипломы, сертификаты специализированного образования). Это

поможет руководству, отвечающему за финансы, поверить в вас как в специалистов, способных выявлять и оценивать риски, успешно осуществлять планы и программы по безопасности.

Постарайтесь увязать информационные риски с задачами и результатами деятельности всей компании. Акцент исключительно на технических аспектах информационной защиты едва ли встретит понимание у руководства компании и финансистов. Демонстрация, как эти риски могут влиять на нижнюю строчку (прибыль) бюджета, прозвучит значительно убедительнее.

Используйте доступный и простой язык. Чрезмерное увлечение техническими терминами может вызвать негативную реакцию слушателей. Готовьтесь не к монологу, а к дискуссии и не перегружайте свои выступления непонятными для неспециалистов словами и определениями.

Разработайте конкретный план финансирования своей работы, не забывая об объективных ограничениях. Почти все организации испытывают недостаток средств. Об этом надо не только знать, но и специально подчеркивать, что при составлении плана вы учитывали напряженность с финансами и поэтому представили достаточно скромный запрос. Это понравится.

Получив финансирование, строго следуйте плану расходования средств. Ничто так не подорвет доверие к вам со стороны финансового директора, как заявка на одну сумму, а затем попытки выторговать дополнительные деньги на что-то еще.

Обеспечьте систематическое информирование финансистов и руководства компании о выполнении программы безопасности. Регулярно докладывайте о кибер угрозах и тенденциях в этой сфере. Это можно делать и устно, скажем, за обедом, или в форме сообщений по электронной почте.

Используйте внешние ресурсы убеждения. Если к вашим проектам и расчетам в компании относятся с долей скептицизма, предложите компании пригласить независимого специалиста для экспертной оценки. Нередко начальники склонны больше доверять внешним экспертам.

Всегда подчеркивайте, что кибер безопасность не ограничивается понятием «информационные технологии», но имеет самое прямое отношение к управлению рисками.

Как защитить себя от конкурентов на деловых выставках?

Известный специалист в сфере конкурентной разведки Джон МакГональ предлагает на сайте diy-ci.com (May, 2013) некоторые рекомендации, как защитить свои ноу-хау во время проведения деловых форумов, выставок, ярмарок и т.п.

Эксперт советует:

Во-первых, внимательно изучите «географию» своего будущего стенда. Кто будут ваши соседи справа, слева, сзади и напротив? Конкуренты, расположившись по соседству с вами, окажутся в самой благоприятной ситуации для того, чтобы подглядывать и подслушивать, случайно или преднамеренно, ваши разговоры с посетителями и деловые переговоры, отслеживать действия стендистов, ваших потенциальных клиентов и партнеров, интересующихся представленной вами на выставке продукцией/услугами.

Во-вторых, позаботьтесь о надлежащей охране стенда. Примите меры, чтобы стенд ни на минуту – ни на минуту! – не оставался без присмотра. Конкуренту, не говоря уже о профессиональных ворах, достаточно 15-20 секунд, чтобы заполучить важную информацию, а то и стянуть представленное вами изделие.

В-третьих, не позволяйте себе расслабляться в течение всего дня. Обычно посетители где-то ближе к концу своего пребывания на выставке начинают понимать, что из представленной продукции им может быть наиболее полезным и нужным, приступают к более доскональному изучению тех или иных экспонентов. Тут надо быть особенно внимательным, так как конкуренты под видом «покупателей» могут попытаться взять у вас «интервью». Прежде чем начинать обстоятельный разговор, поинтересуйтесь личностью собеседника, не стесняйтесь задать ему вопросы о месте работы, о компании и т.п. Никогда не доверяйте полностью информации бэджика. Фальшивый бэджик – тактика, к которой прибегают не слишком чистоплотные конкуренты. Иногда указывают не основную компанию, а дочернюю, малоизвестную фирму с той же целью – ввести вас в заблуждение и вызвать на откровенный разговор под видом потенциального клиента/партнера.

В-четвертых, когда приводите в порядок стенд после рабочего дня или закрываете стенд по завершении выставки, внимательно следите, чтобы важные печатные материалы, не подлежащие широкому распространению, или записи о переговорах, содержащие, например, данные о ценовой политике, не оказались в мусорной корзине. Не поленитесь отправить отслужившее свое материалы в шредер или захватить с собой, чтобы затем надежно уничтожить. Та же самая рекомендация относительно отеля, в котором вы остановились, приехав на выставку из другого города (страны). Ничего, что может послужить источником информации для конкурентов, не оставляйте после себя, положившись на обслуживающий персонал форумов и гостиниц.

Четыре распространенные ошибки при проведении оценочного тестирования систем безопасности

Регулярные испытания физических и информационных систем безопасности с целью выявить слабости и уязвимости – непременное условие их надежности. Джоан Гудчайлд, ответственный редактор сайта csoonline.com, в статье от 8 апреля 2013 года приводит мнения экспертов относительно наиболее распространенных ошибок при проведении таких проверок.

1. Небрежное и поспешное планирование

Когда команда приступает к подготовке плана проверок, ни одна идея, высказанная вслух или письменно, не должна остаться без внимания и всестороннего обсуждения, отмечает Рожер Джонстон, руководитель Группы по выявлению уязвимостей, Argonne National Laboratory. Ошибочно отмахиваться от идей и предложений, которые, на первый взгляд, кажутся неприемлемыми. Ссылаясь на собственный опыт участия в дискуссиях, в «мозговых штурмах», он замечает, что присутствие начальников обычно сковывает инициативу участников, «дикие» идеи отвергаются с ходу, без попытки анализа. «Хорошие идеи приходят не сразу». Он также советует участникам процесса планирования вести себя «как очень плохие ребята», придумывая самые каверзные и коварные способы преодоления систем безопасности.

2. Не следовать каждой букве корпоративных правил, политик и регламентаций

Джерри Волтерс возглавляет отдел информационной безопасности в медицинском центре OhioHealth и вынужден в той или иной мере учитывать принятый около 10 лет назад в США Закон о преемственности страхования и отчетности в области здравоохранения (Health Insurance Portability and Accountability Act, сокращенно HIPAA). Закон предписывает меры обеспечения конфиденциальности, целостности и доступности цифровых медицинских данных и требует, чтобы медицинские учреждения, хранящие или передающие данные в цифровом виде, предпринимали соответствующие защитные меры административного, технического и физического характера. Волтерс утверждает, что к соблюдению законодательства, равно как и к принятым в компании собственным политикам и правилам, надо подходить творчески, гибко. Совсем не обязательно скрупулезно следовать каждой букве. Он приводит такой пример из практики. В одной из фирм инструкция предписывает охранникам в определенное, фиксированное время заступать на дежурство. Это, по мнению эксперта, ошибочное правило, поскольку раскрывает режим, расписание работы. У профессионала охранного дела две заботы: выполнять свою работу и следовать при этом разным предписаниям и правилам. Часто то и другое входят в противоречие. В этих случаях профессионал должен руководствоваться критерием безопасности.

3. Плохой отчет

Волтерс считает никуда не годными отчеты, которые обозначают проблемы, но не дают ответа, как их решать. Обычно это бывает, когда испытание систем безопасности на надежность вскрывает множество ошибок, уязвимостей. Эксперт рекомендует не спешить с обвинениями в адрес сотрудников, которые ответственны за эти ошибки, но сосредоточиться на латании обнаруженных «дыр».

4. Нежелание или неумение внедрить результаты проверок в корпоративную культуру безопасности

Джонстон отмечает, что не всегда и не все обнаруженные во время испытания проблемы можно разглашать всему персоналу компании. В то же время многие сотрудники привыкли смотреть на вопросы безопасности как на нечто, не имеющее к ним прямого отношения. Данный подход в корне порочен. Эксперт советует те результаты тестирования, которые можно без ущерба для дела предавать огласке внутри компании, обсуждать «всем коллективом». Таким путем постепенно прививается корпоративная культура безопасности, охватывающая весь персонал.

Money Laundering: A Guide for Criminal Investigators, Third Edition

Money Laundering: A Guide for Criminal Investigators, Third Edition
By John Madinger

Рецензент А. Барни обращает внимание, что книга, автор которой в недавнем прошлом расследователь экономических преступлений, представляет замечательное введение в мир отмывания грязных денег.

Большой интерес вызывает раздел, посвященный истории финансовых «прачечных», который проиллюстрирован фактами прошлого, например, операциями незабвенного Аль Капоне, или знаменитого скандала Уотергейтс, который, в частности, включал незаконное финансирование избирательной кампании.

Все последовательные процедуры отмывания денег описаны в деталях, с примерами из реальной жизни.

Два раздела посвящены законодательству и регламентации финансовых операций на федеральном уровне (США). В нескольких главах идет речь о партнерстве в бизнесе, банковских операциях и прочих аспектах функционирования бизнеса, без знания которых не может обойтись ни один расследователь финансовых преступлений.

В третьем издании значительно переработаны и дополнены разделы, касающиеся финансирования терроризма. Детально рассказывается о каналах наполнения бюджета Аль Кайды через исламские «благотворительные» фонды. Подробно разбирается древнейшая на Ближнем Востоке система финансовых сделок и потоков «Хавала».

Книга снабжена практически полезными приложениями, графиками, солидной библиографией.

Что более приоритетно – производительность или защита данных?

(результаты опроса, проведенного научно-исследовательским институтом Ларри Понемона)

Респондентам предложили выбирать между производительностью и надежностью информационной защиты – двумя вещами, которые иногда приходят в противоречие друг с другом. Такой пример: в самолете менеджер компании, спеша на важное совещание, раскрывает ноутбук, чтобы завершить доклад, внеся существенные поправки по свежим материалам. Содержание экрана доступно соседям. У него выбор: или доделать отчет или закрыть компьютер, сохранив конфиденциальные данные.

Исследование дало следующие результаты.

Среднее и старшее поколения менеджеров отдает предпочтение безопасности перед производительностью. Авторы исследования полагают, что старшие по возрасту работники, не уверенные в надежной защите данных на своих рабочих компьютерах, работают менее охотно, чем их младшие коллеги в аналогичных условиях. Другими словами, младшие работают больше и продуктивнее. Они спокойнее относятся к проблемам защиты информации, предпочитая продуктивность работы вопросам безопасности. Авторы объясняют данный феномен тем, что молодое поколение чуть ли с грудного возраста знакомится и вырастает с компьютерными технологиями в руках. Молодые настолько сживаются с технологиями, что часто не задумываются о безопасности, например, в момент использования мобильного девайса для дистанционного просмотра служебных файлов. Кроме того, у них по сравнению со старшими коллегами сильнее проявляется стремление добиться успехов, сделать карьеру, что также отражается на отношении к безопасности.

Другой итог исследования: менеджеры среднего и высшего эшелонов работают с данными намного производительнее, чем их подчиненные. При этом важно учитывать, что старшие по должности менеджеры чаще имеют дело с конфиденциальными данными по сравнению с рядовыми сотрудниками.

Если анализировать результаты исследования по гендерному принципу, то выясняется, что женщины «работают больше и дольше мужчин и, по сравнению с последними, более ответственно относятся к защите данных» (Chief Security Officer, May 31, 2013). В целом 56% опрошенных заявили, что рассматривают privacy делом важным и очень важным. Среди женщин такой подход разделяют 61%, среди мужчин – 50%. Кроме того, столкнувшись с выбором – отправиться домой по завершении рабочего дня или остаться еще поработать в офисе – 62% женщин и только 48% мужчин согласны поработать сверхурочно.

И еще несколько показательных цифр. 47% респондентов заявили, что не уверены или не считают, что руководители их компаний уделяют должное внимание защите корпоративных данных при работе с мобильных устройств вне офиса. 58% не уверены, что их коллеги в этих условиях проявляют осторожность и думают о защите информации.