Охрана предприятия

№4 (74), 2020

Оглавление

Охрана предприятия за рубежом

Как меняется индустрия безопасности на Ближнем Востоке

Книжное обозрение

Internet of Things, for Things, and by Things

Исследования

Расходы на кибербезопасность в 2020 году. Тенденции

Коронавирус и индустрия безопасности

Пандемия коронавируса существенно сузила функциональность корпоративной безопасности в ряде отраслей экономики, но одновременно приобрела критически важное значение в других секторах. Новая реальность, пишет Кейт Оринжер в апрельском выпуске журнала Security Magazine, вынудила многие охранные предприятия и службы безопасности компаний перестроиться, поменять приоритеты и векторы деятельности.

Одно из главных требований сегодня – сохранение здоровья и жизни сотрудников, особенно в тех сферах деятельности, где риски заразиться наиболее высоки, т.е. в здравоохранении, розничной торговле, на транспорте… Эшли Купер, руководитель Paladin Security Group (охранное предприятие, активное в странах Азиатско-Тихоокеанского региона) , директивно вменил всему персоналу в обязанность поддерживать чистоту на рабочих местах, используя дезинфицирующие средства, регулярно мыть руки, соблюдать социальное дистанцирование, носить маски и перчатки.

Некоторые клиенты Paladin Security Group, продолжающие деятельность в условиях пандемии, в частности, банки, обеспечивают охранников средствами индивидуальной защиты. Немало объектов, которые закрылись из-за вируса, но по-прежнему требуют охраны, в частности, музеи. Там, практически, никого нет, кроме охранников, соответственно и риски заразиться сравнительно невысоки.

Наиболее сложная ситуация – в сфере здравоохранения. В некоторых госпиталях, где имеются инфекционные отделения и лежат больные коронавирусом, отмечает Купер, предприняты чрезвычайные меры безопасности: резко ограничен доступ в здания и помещения, усилен контроль по периметру безопасности и внутри зданий, увеличено

число охранников. Последние перебрасываются с одного объекта на другой, как того требует складывающаяся ситуация.

Охранное предприятие Securit, расположенное в Нью-Йорке, столкнулось с падением спроса на его услуги среди ритейлеров, многие из которых закрылись, а некоторые и съехали вовсе. В то же время пошли заявки от новых клиентов. В их числе – пустующие или едва заполненные городские отели. «Владельцы требуют круглосуточную вооруженную охрану, - говорит Лиза Долан, президент Securit. - Город словно вымер, похож на город-призрак. Редкие прохожие. Этим пользуется криминал. У полиции хватает и своих дел. Именно частной охране приходится заниматься защитой имущества закрывшихся предприятий».

Владельцы этих предприятий обеспокоены ситуацией и просят увеличить число охранников и мобильных патрулей. И это вполне понятно, говорит Лиза Долан: «Офисы и предприятия закрыты, но осталось офисное имущество, ценное оборудование, служебная информация, секретные данные, все, что требует усиленной защиты в непростые времена. Вот почему они просят обеспечить надежную охрану, особенно темное время суток» (там же).

Находящаяся в Питтсбурге компания St. Moritz Security также сократила число охранников в сфере торговли и обслуживания, направив освободившиеся ресурсы на функционирующие объекты с большим числом штатных работников и посетителей. Помимо прямых своих обязанностей охранники по согласованию с клиентскими организациями выполняют некоторые ранее не свойственные им функции. Например, измеряют специальными датчиками температуру всем, кто входит в здания. Директор St. Moritz Security Шварц отмечает, что охранники работают на пределе сил, по 70-80 часов в неделю.

Естественно, поднимается вопрос о доплате за переработку.

Лиза Долан отмечает, что ее клиенты понимают необходимость тратить больше денег на охрану и безопасность, чем в обычное, нормальное время. Они готовы платить, уверенные, что охранное предприятие не воспользуется ситуацией сорвать куш и не потребует больше, чем действительно необходимо, чтобы справедливо компенсировать реальные дополнительные затраты труда и средств. «Клиенты не рассматривают такие расходы в качестве подарка или бонуса. Они знают, что мы не накручиваем ставки. Если они нуждаются в том, чтобы квалифицированные специалисты работали сверх определенного контрактом времени, то, конечно, должны будут оплачивать дополнительные счета. Мы обсуждаем эти вопросы спокойно и прозрачно. Во всех случаях клиенты соглашаются с нашими доводами, выстроенными на конкретных цифрах, и подтверждают готовность выделять соответствующие средства. Затем мы разворачиваем работу» (там же).

В других случаях доходы, напротив, сокращаются. Долан приводит в качестве примера ресторан, владелец которого попросил вместо двух охранников оставить одного и внести изменения в контракт. Ресторан временно закрылся и вынужден экономить. «Таких клиентов у Securit набралось достаточно, - отмечает Лиза. - Мы с ними сотрудничаем многие годы и уверены в возобновлении полномасштабной работы по завершении пандемии».

В целом по отрасли охранной индустрии, считают эксперты и руководители компаний, в 2020 году из-за коронавируса ожидается падение доходов от 1.5 до 2.5 процентов,

что отразится на зарплатах.

Одновременно растут операционные расходы в связи заболеваниями среди персонала охранных предприятий. Компания Top Guard Security уже в апреле стала обращаться в рекрутинговые фирмы на предмет приглашения охранников по временным краткосрочным контрактам, чтобы заменить заболевших работников. Разумеется, каждый нанятый охранник должен пройти курс дополнительного обучения с учетом специфики нового рабочего места. И это тоже дополнительные расходы.

Транснациональная корпорация Securitas (представительства в 52 странах, общее количество персонала превышает 300 тысяч человек, не путать с Securit – см. выше) развернула новую технологическую платформу с видео и онлайн характеристиками специально для профессионалов, занимающихся поиском, отбором, наймом и адаптированием охранников к новым условиям.

Говоря о неизбежном временном спаде индустрии безопасности, эксперты и специалисты в этой области довольно оптимистично смотрят на долгосрочные перспективы охранного дела.

Уроки пандемии для корпоративных служб безопасности

Онлайновый журнал Security Magazine разместил в майском выпуске результаты опроса ведущих специалистов и руководителей в сфере корпоративной безопасности на тему приобретенного опыта и уроков работы в условиях пандемии коронавируса.

«Мы глубоко осознали ценность, значение людей, профессиональных кадров для нашей работы, - говорит Майк Вэник, директор корпоративной безопасности United Therapeutics. - Вы можете владеть лучшими в мире технологиями, но без людей они бесполезны. Они ничтожны, если ваши сотрудники, в совершенстве владеющие этими технологиями, нарушают элементарные требования охраны своего здоровья в той форс-мажорной ситуации, в которой мы все оказались».

«Я понял, как опасно быть чересчур самонадеянным, самоуверенным, - отмечает Джефф Хаук, руководитель управления безопасности медучреждения Memorial Healthcare. - Вы перестаете слушать других, уважать «противника». Недооценка «врага» ведет к сокращению тренингов, к желанию облегчить свою работу. Но самое опасное – пренебрежение серьезной и честной проверкой своей готовности противостоять вызовам, подобных тем, с которыми мы сталкиваемся сегодня. Еще один урок, который я извлек из пандемии, это необходимость всегда готовиться к худшему из всех возможных сценариев развития обстановки (в данном случае - нехватка средств индивидуальной защиты, потеря из-за болезни ключевых или большой группы сотрудников, гигантский наплыв пациентов)».

«Для меня главным стало наличие эффективных коммуникаций, - замечает Эрик Клэй, директор безопасности Cox Health. – Когда разразилась пандемия, первое, что мы сделали, это установили и усилили коммуникации между офицерами безопасности всех наших больниц. Мы также обеспечили двусторонний обмен оперативной

информацией с местными правоохранительными органами. Одновременно нарастили обмен данными внутри службы безопасности. В условиях пандемии крайне важно располагать актуальной и точной информацией о происходящем вокруг. Информацией, которая помогает избавиться от панических настроений и преодолевать разногласия и недоразумения».

«Для меня ценным стал не «новый урок», а обращение к опыту прошлого, - говорит Эдди Анкерс, директор корпоративной безопасности NTT Global Data Centers Americas. – Экстремальная ситуация подчеркнула критически важное значение коммуникаций и слаженной командной работы. Чтобы обеспечить бесперебойное функционирование центра обработки данных, мы усердно и круглосуточно контактируем с местными и региональными отделениями МЧС, компаниями ЖКХ, традиционными партнерами и поставщиками. Пандемия стала серьезным экзаменом нашей готовности встретить и противостоять вызовам. Кризис заставил нас сосредоточить внимание на вопросах отладки командной, коллективной работы, обеспечения персонала средствами эффективной защиты от коронавируса».

Джесон Вейок, директор безопасности GoDaddy (поставщик платформ вебсайтов и смежных услуг) назвал главным уроком развитие способности как можно раньше, как можно быстрее осуществлять имеющиеся в компании планы действий в экстремальных условиях. «Хотя у нас не было детального документа на случай форс-мажора, но, обнаружив на горизонте первые признаки приближающейся грозы, мы немедленно мобилизовали все имеющиеся в наличии ресурсы и средства, необходимые, чтобы бизнес продолжал более-менее нормально функционировать в обстановке кризиса».

Дэвид Фортино, руководитель группы по антикризисному управлению Pratt & Whitney (производитель авиационных двигателей для гражданской и военной авиации, в настоящий момент является частью транснациональной корпорации United Technologies), полагает самым важным «эффективное налаживание и поддержание системы обмена информацией и средствами индивидуальной защиты между многочисленными филиалами и отделениями компании, разбросанными по миру». Также он обращает внимание на значение быстрой переориентации отдельных направлений производства на обслуживание потребностей медицины (выпуск масок и прочих остродефицитных средств).

Маргарет Левин, вице-президент корпорации Bridgestone Americas (производство автомобильных шин, запчастей и прочих товаров), опираясь на уроки, полученные в ходе нынешнего кризиса, считает необходимым разработать специальный план мероприятий на случай повторения пандемии. «Антикризисные программы, которые создавались в компании ранее, были рассчитаны на предсказуемые катаклизмы, например, ураганы, смерчи, природные пожары, и, к сожалению, не учитывали специфику нынешнего мирового бедствия. Поэтому будем работать над отдельным документом, который вберет опыт, полученный в условиях пандемии коронавируса».

Как стать своим в правлении

компании

Значение функции безопасности в деятельности компаний за последние годы выросло до уровня совета директоров, отмечают авторы статьи в журнале Chief Security Officer (February 18, 2020) Дж. Бокэм и Дж.М. Поруп. Из оперативной функции она превратилась в стратегическую.

Эксперты рекомендуют руководителям корпоративных служб безопасности проявлять максимум энергии и креативности для завоевания и поддержания высокого статуса в системе управления бизнесом. Для этого недостаточно время от времени делать презентации о своей работе, полагает Селим Айсси, ответственный за безопасность компании Ellie Mae (один из ведущих провайдеров облачных платформ для финансовых организаций).

«Вы должны обращаться в совет директоров не только в связи с инцидентом безопасности, - говорит Николе Монтефорте, вице-президент Booz Allen Hamilton (консалтинговая фирма в области информационных технологий). - Ваше взаимодействие с первыми лицами должно быть постоянным».

Формирование таких взаимоотношений требует от директора СБ коммуникационных способностей, знания определенных приемов общения с коллегами и начальством. Цель – стать надежным и уважаемым партнером в бизнесе, а не просто профессионалом в своей области, о котором вспоминают и к которому обращаются лишь когда возникают проблемы.

Руди Бакалов, директор развития цифровых технологий Booz Allen Hamilton, рекомендует знакомиться с аналитическими материалами, годовыми отчетами, стенограммами заседаний правления компании, другим важными внутренними документами, чтобы быть всегда в курсе текущих процессов и тенденций, бизнес планов компаний.

Б. Аустин (компания TCE Strategy) рассказывает, что ему в качестве директора кибербезопасности удалось заручиться поддержкой первых лиц, войти в правление во многом благодаря тщательному изучению биографий топ менеджмента, их роли и веса в структуре управления компанией. «Такой путь позволяет многое узнать об их взглядах и подходах, соответственно формировать взаимоотношения».

Эксперты настоятельно рекомендуют участвовать во всех заседаниях правления, других важных совещаниях, даже если вопросы безопасности не стоят в повестке дня. Достаточно просто сидеть, слушать, записывать полезную информацию в блокноте.

Эксперт Брайан Хаугли советует искать любой подходящий повод для контакта за рамками официальных мероприятий. Таким поводом, например, может быть совместный ланч.

Бакалов утверждает, что члены совета директоров должны доносить до СБ свои планы и свои ожидания от корпоративной безопасности. «Каждый волен рассуждать, как ему видится повышение эффективности данной функции. Но я уверен, что охрана и безопасность – совместная ответственность. Критически важно, чтобы правление компании ясно озвучивало, какие риски они могут терпеть, а какие ни в коем случае,

каков, по мнению правления, должен быть формат докладов о состоянии безопасности, на какую ответную, ориентирующую информацию могут рассчитывать те, кто отвечает за охрану и безопасность».

Ссылаясь на собственный опыт, Селим Айсси говорит о необходимости для директора СБ готовить отчеты и доклады таким образом, чтобы вопросы безопасности легко транслировались в термины бизнеса. Он, например, заранее договаривался с топ менеджерами о метриках, которые хотел бы использовать для измерения эффективности функции. «Это позволило сравнительно легко сравнивать результаты работы СБ сегодня и, скажем, год назад». Айсси в начале своей карьеры директором кибербезопасности призвал в неформальные советники двух ветеранов компании, которые в разное время занимали место в правлении. Последние, хорошо зная корпоративную культуру организации, особенности управления процессами бизнеса, помогли ответить на вопросы, возникавшие при составлении первых презентаций: «Я планирую рассказать о существующих рисках и угрозах компании. Правильно ли расставляю акценты? Будет ли работать избранный мной подход? Смогу ли я своим отчетом закрепить отношения с первыми лицами?».

Многие эксперты советуют выделить среди топ менеджмента одного-двух лиц, которые бы помогали продвигать программы охраны и безопасности. «Вы не можете просто позвонить президенту компании и сказать, что хотите представить на правлении отчет. Вам нужен кто-то из членов правления, кто бы предложил вас заслушать», - говорит Хаугли. Ищите «спонсора», который бы высказывал особый интерес к вопросам безопасности, имел бы наилучшее представление об этой функции в организации.

Эксперты рекомендуют продвигать идею о создании в компании специального комитета с участием топ менеджеров и акционеров, который бы целенаправленно рассматривал вопросы охраны и безопасности, готовил эти вопросы для заседания совета директоров, анализировал предлагаемые решения.

Шесть вопросов потенциальному работодателю от соискателя на место руководителя СБ

В прошлом выпуске нашего журнала (№ 73) мы публиковали 10 вопросов, обычно задаваемые работодателями претенденту на руководящую должность в службе корпоративной безопасности.

Сейчас предлагаем вниманию читателя 6 вопросов, которые, по мнению Дж.М. Порупа, автора статьи в журнале Chief Security Officer, должен прояснить сам соискатель во время собеседования.

1. Сколько времени первые лица компании уделяют проблемам охраны и безопасности организации?

Культура безопасности формируется сверху. Если владелец компании или

гендиректор не понимает и не поддерживает функцию безопасности, то все ваши усилия пойдут насмарку. Что знает о безопасности гендиректор? Конечно, вы можете (и должны) предварительно посмотреть служебные профили топ менеджмента на корпоративном сайте и в соцсетях. Вам необходимо знать, является ли безопасность в числе главных приоритетов компании. Автор статьи рекомендует до принятия решения о переходе на новую работу обязательно встретиться если не с первым лицом, то с кем-то из верхнего эшелона, кто курирует вопросы охраны.

2. Как организация реагирует на инциденты безопасности?

Избегайте компании, где сотрудника могут уволить за то, что он попался на фишинговую приманку. Задайте такой вопрос: «Допустим, компания в результате ошибки персонала потеряла миллион долларов. Меня интересует, как поступит компания с виновником утечки?». Формулируйте вопросы так, чтобы на них нельзя было ответить простым «да» или «нет». Не надо ожидать, что интервьюер огласит конфиденциальные детали (уже одно это должно вас, как минимум, насторожить). Вас интересует подход компании в целом к неизбежным в реальной практике инцидентам.

3. Почему открылась позиция руководителя СБ?

Если речь идет о замене руководителя, то спросите, как потенциальный предшественник работал, что получалось, почему оставляет должность, что руководство ждет от нового человека на этой должности. Если вакансия открыта уже долгое время, то это совсем не означает, что организация «токсична» и никто не хочет в ней работать. Просто на рынке труда сохраняется острый дефицит сильных, высококвалифицированных специалистов по корпоративной безопасности, и, бывает, вакансия главы СБ месяцами остается незаполненной.

4. Характеризуется ли бизнес культура компании формулой «быстро и напролом»?

Желательно так формулировать вопрос: «Сколько времени компания тратит на поддержку существующего положения дел в бизнесе, и сравнительно сколько - на внедрение инноваций». Положительный ответ в пользу инноваций сам по себе ничего плохого не означает. Но если много сил и времени уходят на новые вещи, остается ли время на функцию безопасности? Во всяком случае, есть о чем подумать...

5. Рассматривает ли компания службу безопасности как подразделение «нет»?

Вопрос: «Расскажите о программе ознакомления персонала с рисками (awareness programs)?». Вы должны знать, является ли эта программа «фиговым листком» для акционеров и регуляторов, о которой вспоминают раз в год, и после которой уже через день никто ничего не помнит. Постарайтесь также разузнать о моральном, психологическом климате в коллективе. Спросите, к примеру, какие жалобы поступали от сотрудников СБ.

6. Каков бюджет на охрану и безопасность?

Финансы во многом определяют, насколько успешны вы будете в качестве руководителя СБ. Выделяемые на эту функцию средства, конечно, зависят от бизнеса организации, ее размера, модели рисков и угроз. Важно, чтобы хватало денег на «дорожную карту» имплементации стратегии безопасности.

Беспилотники: как справляться с угрозами?

Риски и угрозы, исходящие от беспилотников, с годами становятся все сложнее, отмечает Макс Клейн, главный технолог компании SCI Technology (производство IT решений) в публикации журнала Security Management (February, 2020). В самом начале эры дронов они представляли собой забаву для взрослых. Затем стали вторгаться в разные сферы экономики, бизнеса и общественной жизни. Беспилотники вошли в арсенал армий и силовых структур. Мимо новых технологий не прошли и «плохие парни» - дроны поставлены на службу промышленного шпионажа, криминальных группировок, террористических организаций.

В Европе и Северной Америке компании, имея дело с беспилотниками, сталкиваются с дилеммой: свобода и (или) безопасность. Технологии развиваются столь быстро, что законодательство, нормативная база просто не поспевают. В Азии и Африке, на Ближнем и Среднем Востоке отношение проще: в большинстве стран частным компаниям не запрещают глушить сигналы и даже сбивать дроны.

Система противодействия рискам и угрозам, связанным с дронами, состоит из двух компонентов: 1) обнаружение и идентификация; 2) нейтрализация.

Самое важное – вовремя обнаружить и опознать приближающийся беспилотник: какой организации принадлежит, зарегистрирован ли, где находится оператор, им управляющий. Для борьбы с нарушителями применяются различные технологии:

- Радиолокационные станции с обзором;

- Лидары (LIDAR - технология получения данных об удаленных предметах при помощи обработки сигнала отраженного света; источником света могут быть любые устройства, но чаще всего для этих целей используется лазер);

- Оптические средства;

- Тепловизоры;

- Акустические средства;

- Радиочастотные глушители дронов;

- Бластеры (радиоэлектронные устройства для постановки помех).

У каждой опции свои плюсы и недостатки, говорит Клейн. Радары обладают большим диапазоном покрытия, определяют удаленность объекта, но часто ошибаются в обозначении высоты летящего объекта. Средства оптического обнаружения ограничены по дальности и широте обзора, зато информируют о высоте и местонахождении. В сочетании же обе системы дают более точную информацию о том, где находится дрон в каждый данный момент и каковы характеристики полета (маршрут и поведение).

Взаимодействие разных технологий требует их интеграции. Это не всегда просто, но в

итоге эффективно. К примеру, радар показывает, что фиксируемый в воздухе объект является дроном, а не крупной птицей, оптические устройства дают тот же результат, тем самым подтверждается наличие реальной потенциальной угрозы.

За исключением радиочастотных технологий, инструменты обнаружения и слежения обычно не ограничиваются законом и могут использоваться частными организациями. Вопрос в том, насколько быстро и точно они действуют. Клейн говорит, что у службы корпоративной безопасности для обнаружения, реагирования и нейтрализации беспилотника, как правило, есть не более 20 секунд. Конечно, расширение горизонта обзора средствами слежения полезно, но не всегда себя оправдывает, если скорость полета дрона превышает 150 км в час.

Один из путей обеспечения эффективности Клейн видит в минимизации уровня ложных сигналов, в настройке систем опознания на раннее предупреждение и максимальную точность получаемых данных. Это означает, что чем быстрее и точнее организация оценит риск – скорость, размеры, грузоподъемность, маршрут беспилотника, а также способ управления им – тем лучше подготовится к нейтрализации.

Эксперты считают важным иметь в компаниях толковую инструкцию, как реагировать на дроновые угрозы. Первый немедленный шаг при обнаружении неопознанного дрона – сообщить в правоохранительные органы по заранее согласованному каналу коммуникации. Следующий или одновременный шаг – ослепить установленные на беспилотнике видеокамеры с помощью специальных устройств, включая лазерные.

Также надо попытаться найти оператора, лишить его возможности управления. Обычный для этого способ – подавление сигналов. Но этот прием не во всех странах разрешен. В США он под запретом из-за опасности негативного воздействия на работающие легально коммуникационные системы, например, технологии GPS, используемые в аэронавигации. В США также запрещено частным компаниям самостоятельно сбивать подозрительные дроны.

В России «беспилотные воздушные суда» - именно такое название беспилотников приняли в МВД РФ - только полицейские могут принудительно приземлить, а человека, управляющего аппаратом, задержать. В настоящее время проект документа, где конкретно определено, в каких случаях и каким способом производится такая вынужденная посадка, представлен для общественной экспертизы. Приказом министра внутренних дел России будет утвержден порядок принятия решения о пресечении нахождения беспилотных воздушных судов в воздушном пространстве. Прекратить полет полиция может, применив специальные технические средства для подавления или преобразования сигналов дистанционного управления беспилотными воздушными судами.

В крайнем случае аппарат может быть поврежден или уничтожен. Но только в самом крайнем случае. Ведь, пишут эксперты, «даже случайная поломка аппарата, например, потеря управления, может привести к беде». Действительно, падение в толпу с десятиметровой высоты конструкции весом в несколько килограммов, даже без гранаты на борту, может кого-то покалечить и даже убить. А что, если такая «железяка» попадет в припаркованную рядом машину и вызовет пожар или взрыв? (Российская газета, 11 мая 2020).

Как наиболее эффективно использовать выделенные на безопасность деньги

Журнал Chief Security Officer (April 27, 2020) взял интервью у ряда экспертов по корпоративной безопасности относительно экономии бюджета в непростых условиях, в которых сегодня оказался бизнес. Специалисты рекомендуют следующие пути и способы повышения эффективности расходов на охрану и безопасность:

1. Внедрять автоматизацию

Согласно недавно проведенному компанией Cisco опросу, 77% из охваченных исследованием 2,800 профессионалов заявили, что планируют в 2020 году более широко и интенсивно использовать роботы и другие автоматы.

2. Перестроить баланс компетенций и профессиональных кадров внутри СБ

Нередко случается, что одни специалисты перерабатывают, другие трудятся в более щадящем, спокойном режиме. Эксперты советуют внимательно проанализировать распределение функций и обязанностей внутри команды с таким расчетом, чтобы обеспечить более эффективное функционирование СБ без привлечения дополнительных кадров, что всегда ударяет по бюджету.

3. Обновлять приоритеты

Ландшафт угроз постоянно меняется. Необходимо периодически анализировать, какие риски и угрозы выходят на первый план, соответственно гибко перераспределять финансовые и материально-технические ресурсы, не выходя за пределы выделенных средств. «Сейчас подходящее время критически посмотреть на риски для бизнеса, - говорит Кейн МакГлэдри, занимавший в течение ряда лет должность директора кибербезопасности компании Pensar Development (инженерные слуги в разных отраслях экономики, включая IT). - Мы можем хорошо делать не более чем три вещи одновременно, поэтому надо выделить самое важное направление, на нем сосредоточить преимущественное внимание. Это вопрос направления средств, в том числе и финансов, на задачи, которые наиболее актуальны, остры на данный момент, оставив в тени все, что и так выглядит достаточно благополучным».

4. Критически оценить эффективность имеющихся в компании систем кибербезопасности

МакГлэдри советует пересмотреть планы закупок новых технологий, исходя из формулы «бери лучшее по лучшей (более низкой) цене». Сегодня для этой формулы самое подходящее время, так как в условиях экономического кризиса, обусловленного пандемией коронавируса, производители и поставщики охотнее идут на скидки за поставляемые продукты и услуги.

5. Добиваться для кибербезопасности отдельного бюджета

Во многих организациях практикуется формирование цельного бюджета на IT, который включает расходы на кибербезопасность. Последняя нередко оказывается

«золушкой», чьи реальные потребности недооцениваются. Поэтому важно лоббировать в пользу отдельного, самостоятельного бюджета для кибербезопасности, причем на долгосрочной, многолетней основе, что даст возможность успешно разрабатывать и осуществлять перспективную стратегию управления технологиями и кадрами профессионалов.

6. Расширять по возможности практику аутсорсинга

Руководителям СБ необходимо тщательно изучить кадровый и материальный потенциал команды, определить какие задачи и функции целесообразно с точки зрения эффективности и экономии средств передать «третьей стороне». Речь идет о некоторых позициях, которые не требуют полной занятости, или об уникальных компетенциях и узких специальностях.

7. Обучение и тренинги проводить собственными силами

Эксперты рекомендуют не увлекаться аутсорсингом в отношении обучения и тренингов персонала СБ и компаний. Собственные модули позволяют не только учитывать специфику организации, но также измерять эффективность занятий, держать под контролем расходы на эти цели.

8. Извлекать максимальную пользу из имеющихся в наличии систем и инструментов охраны и безопасности

Говорит Джон Шаффер, главный менеджер по информации инвестиционного банка Greenhill: «Исключительно важно протестировать все технологии и системы. Я не уверен, что во всех организациях руководители СБ ясно представляют себе, как они работают. Вы просто обязаны тщательно изучить, делают ли они то, что должны делать, насколько эффективны и оправдывают ли вложенные в них средства. Если те или иные инструменты не дотягивают до того, что было обещано производителями, предъявляйте последним претензии, либо ищите других поставщиков».

9. Сократить до минимума число поставщиков

Идеальный вариант: разные инструменты от одного поставщика. Такой подход к закупкам технологий позволяет, во-первых, экономить деньги на приобретение, во-вторых, меньше тратить на обучение персонала, в-третьих, сокращать число операторов, управляющих средствами охраны и безопасности.

10. Добивайтесь централизации управления технологиями безопасности

В крупных организациях случается дублирование инструментов безопасности в разных подразделениях. Это не экономично и не эффективно. Можно сэкономить немало денег на унификации технологий и централизации управления ими.

Риски удаленной работы

Пандемия коронавируса вынудила многие организации отправить своих работников трудиться на дому. Новый формат трудовых взаимоотношений возник неожиданно и без традиционной предварительной обкатки и тестирования. Он принес множество

рисков, которым ранее не уделялось первостепенного значения. Целенаправленные атаки с использованием приемов фишинга рассчитаны на менее защищенные по сравнению с офисными стационарами домашние компьютеры для вторжения в корпоративные сети.

Журналист и эксперт Вал Ле Теллье отмечает, что нынешний кризис послужил катализатором давно наметившейся тенденции к переводу все большего числа офисных работников на «удаленку». Для специалистов по кибербезопасности проблема защиты информации в новых условиях приобретает перспективный, стратегический характер.

Автор полагает важным обратить внимание на следующие аспекты этой проблемы.

Жесткий административный контроль («Governance»)

Контроль предполагает разработку инструкций и политик относительно мер защиты конфиденциальных данных, которые бы, в частности, включали четкую классификацию данных, шифрование, хранение, системы обнаружения подозрительной активности, разумные ограничения по доступу в хранилища данных, а также в обязательном порядке – тренинги персонала, регулярные аудиты кибербезопасности, мониторинг трафика.

Учитывая, что многие сегодня впервые попали на дистанционную работу, надо тщательно разъяснять, что от них ждут в плане кибербезопасности и на какую помощь со стороны организации могут рассчитывать.

Непредумышленные инсайдерские риски

Это наиболее распространенные, а потому и опасные инциденты безопасности как результат невнимательности, неорганизованности, несоблюдения элементарных норм предосторожности. Но даже и дисциплинированные сотрудники могут совершать фатальные ошибки из-за рабочих перегрузок, депрессии, под грузом личных или служебных проблем. Эксперты рекомендуют менеджерам обращать внимание на изменения в поведении и стиле работы своих подчиненных, хотя это непросто делать, когда все они не находятся под одной крышей. Общим признаком аномального поведения может служить заметное снижение активности работника, его контактов по электронной почте, телефону со своими коллегами, партнерами, клиентами. Отсюда логично вытекает необходимость более плотной работы с персоналом, несмотря на отсутствие условий для традиционного, т.е. очного, непосредственного общения.

Работа с кадрами

Хорошее знание подчиненных – важнейшее условие успешной с ними работы, тем более, в т.н. «распределенном офисе». «Постоянные личные контакты необходимы для моральной поддержки, обеспечения слаженной командной работы, для здоровья – физического и ментального», - подчеркивает Теллье. Он советует вкладываться в технологии, позволяющие еженедельно и чаще проводить видеоконференции и совещания. По возможности регулярно общаться с каждым из членов команды. Работающим дистанционно следует предоставить гибкий график, но при этом выделить в расписании часы для видеоконференций, которые бы устраивали всех участников.

Управление данными

Здесь первым делом необходимо взять на вооружение надежные приложения, обеспечивающие строгую аутентификацию привилегированных пользователей, защищающие от несанкционированного вторжения в сети. Профессионалам по кибербезопасности рекомендуется перевести фокус своего внимания с защиты сетей на защиту самих данных путем формирования культуры «нулевого доверия» («zero trust»). Такая культура предполагает, что все электронные сообщения и файлы шифруются перед отправкой и дешифруются по достижении адреса с использованием системы многофакторной аутентификации. Кроме того, в режиме реального времени отслеживается весь трафик сети, все задействованные компьютеры, дивайсы и приложения на предмет обнаружения аномалий, подозрительной активности.

Управление дивайсами

Замечено, что дистанционная работа часто вызывает у сотрудников желание пренебречь строгими правилами, процедурными ограничениями, «спрямить углы». Например, пользователь сети выгружает на свой персональный дивайс служебный файл, руководствуясь стремлением облегчить себе работу (редактирование, распечатка и т.п.). В результате важные корпоративные данные могут оказаться вне контроля организации и даже самого пользователя, т.е. практически без защиты.

Автор публикации советует использовать специальные программные решения, которые ограничивают функциональные возможности удаленных пользователей, например, копирование, распечатки, загрузка в персональные дивайсы. Такие решения позволяют детально анализировать действия пользователей. В конечном счете, существенно снижают инсайдерские риски «распределенного офиса».

Риски «третьей стороны» - это серьезно

Кражи и утечки конфиденциальной информации приняли глобальный масштаб. В мире в одном только 2018 году зафиксированы утечки 5 миллиардов закрытых данных. И это только верхушка айсберга, поскольку многие компании скрывают подобные инциденты, боясь навредить репутации.

Как отмечает Мишель Друайе в журнале Chief Security Officer, значительная часть информационных утечек, так или иначе, вызвана проблемами с безопасностью у партнеров и поставщиков. Но нельзя забывать, что ответственность за утраченные или украденные по вине третьей стороны корпоративные данные лежит на вашей организации со всеми юридическими и финансовыми последствиями. Надо помнить, что популярный, особенно в последнее время, аутсорсинг при всех его плюсах расширяет пространство, где хранятся и обрабатываются служебные данные, следовательно, и увеличивает вектор потенциальных хакерских атак.

Автор публикации рекомендует уже на старте взаимодействия с новым партнером, клиентом или поставщиком самым серьезным образом проверить надежность его систем кибербезопасности. Для начала задайте себе и партнеру следующие вопросы:

- Почему необходимо отдавать на аутсорсинг данную услугу (информацию)?

- Чем конкретно придется делиться с партнером и так ли уж нужно делиться корпоративными данными?

- Как хранится и защищается информация у партнера? Например, шифруется ли она?

- Планирует ли партнер нанимать специалистов (или фирму по субконтракту) для осуществления проекта, и если да, то предполагается ли передача им вашей информации?

- Где находится центр обработки данных, которым пользуется третья сторона?

- Как сформулированы в проекте контракта вопросы, связанные с возможными инцидентами безопасности?

Ясный и четкий план мер реагирования на инцидент кибербезопасности должен быть прописан в контракте очень конкретно: кто за что отвечает, разумный период времени на ликвидацию последствий и восстановление атакованных сетей и баз данных, линии коммуникации в кризисной ситуации. Мишель Друайе подчеркивает необходимость серьезного внимания к самым, на первый взгляд, незначительным, мизерным уязвимостям и возможным инцидентам, ибо последние, подобно снежному кому, могут быстро превратиться в большую угрозу.

Не принимайте на веру слова, что все у партнера в порядке. Предусмотрите регулярную проверку состояния систем информзащиты. В тексте контракта надо прописать обязательства партнера по защите передаваемых ему данных, требования адекватно реагировать на инциденты, детальный план контроля и тестирования систем, а также перечень внешних контактов, каналов, по которым могут утекать данные.

Подобный документ, жестко регламентирующий защиту информации в процессе аутсорсинга, очень даже пригодится в судебном заседании, где решается вопрос о виновной стороне в утечке персональных данных или другой важной конфиденциальной информации. Просчеты в составлении контракта и прочих документов для аутсорсинга, к примеру, невозможность отслеживать, как обрабатываются и хранятся переданные третьей стороне данные, чреваты серьезными негативными последствиями для вашей организации, подчеркивает Друайе.

Если в процессе аутсорсинга вы убеждаетесь, что ваш партнер не выполняет принятые на себя обязательства, зафиксированные в соответствующем документе, не мешкая, разрывайте контракт!

Что надо учитывать при разработке плана поддержки кибербезопасности на случай непредвиденных

обстоятельств

Еще в начале этого года мало кто мог предсказать, чем обернется для мира пандемия коронавируса. Эпидемия затронула практически все аспекты нашей жизни, вынудила многие бизнесы кардинально поменять базовые операции.

Журнал Chief Security Officer (April 14, 2020) публикует рекомендации по составлению плана кибербезопасности на случай экстремальной ситуации, будь то пандемия, природные пожары, наводнения или смерчи.

Такой план (или программа) действий должен учитывать следующие моменты:

Сокращение числа работников IT и СБ на рабочих местах

Кризис, подобный нынешнему, может привести к драматическому сокращению персонала по причине болезни или невозможности добраться до офиса. Эксперты советуют заранее предусмотреть возможность обратиться за помощью к провайдеру услуг по безопасности на то время, пока ситуация не вернется к норме. Надо заблаговременно выбрать организацию для аутсорсинга и согласовать условия партнерства.

Защита корпоративных сетей при «удаленке»

Не дожидаясь, пока «гром грянет», надо привести в порядок и протестировать имеющиеся в наличии инструменты удаленного доступа и системы защиты информации, включая программное решение, которое предназначено отслеживать поведение пользователей, реагировать на аномалии и отклонения.

Защита систем кибербезопасности

Необходимо предусмотреть надежную защиту онлайновых и внутренних систем и сервисов, предназначенных для работы в кризисной ситуации. Служба кибербезопасности должна быть готова обеспечивать контроль безопасности даже в случае сокращения числа специалистов. Ее роль – правильно определить приоритеты своей работы с учетом того, откуда исходят самые опасные риски, какие решения и приложения надо надежно защитить в первую очередь.

Защита систем кибербезопасности партнеров или поставщиков

Организации должны знать и проверять, как обстоят дела с вопросами кибербезопасности у ключевых партнеров. План действий в условиях кризиса должен предусматривать особенности взаимодействия с ними в случае форс-мажора. То же самое касается поставщиков и клиентов. Последние должны быть вовремя предупреждены о рисках сбоя бизнес процессов.

Перестройка программ обучения и тренингов

В период кризиса резко активизируется криминал, в первую очередь, хакеры. В этом мы еще раз убедились на примере пандемии коронавируса. Организации обязаны предвидеть такую опасность и внести необходимые дополнения и коррективы в программы ознакомления персонала с угрозами и рисками. Особое внимание уделить

фишинговым схемам как наиболее популярному у хакеров инструменту для взлома сетей.

Важно извлечь уроки из нынешнего катаклизма. Эксперты советуют составить отдельный конкретный план, предусматривающий, что надо улучшить в инфраструктуре кибербезопасности, чтобы с наименьшими потерями встретить и пережить новый кризис в будущем.

Как планировать кадровое обновление

Джерри Бреннан в очередной своей публикации (майский номер журнала Security Magazine за этот год) поднял тему планирования кадрового обновления в корпоративной службе безопасности.

Стратегия обновления, по его мнению, должна, в частности, включать следующие моменты:

- Составление долгосрочного плана развития функции безопасности в организации.
- Тщательное изучение компетенций и потенциала сотрудников СБ.
- Организация шефской помощи молодым перспективным работникам.
- Формирование культуры прозрачности в кадровой работе.

Бреннан предупреждает о необходимости избегать ошибок, которые могут навредить кадровой политике. Например, он против большого разрыва в зарплатах руководителя СБ и тех, кто ему непосредственно подчинен. Он считает, что рост зарплаты при каждом должностном повышении на одну ступень не должен превышать 10-15%.

Эксперт предупреждает, что подготовка кандидатов на руководящие позиции в службе безопасности не должна ограничиваться сугубо профессиональными компетенциями. Важнейшую роль играет развитие коммуникационных способностей, умение общаться с коллегами из других подразделений компании, с топ менеджерами – не только на темы охраны и безопасности, но и по широкому кругу вопросов бизнеса данной организации.

Бреннан придает большое значение наличию индивидуальных планов профессионального роста перспективных работников, которые предусматривают не только повышение квалификации в рамках конкретной специализации, но и развитие лидерских, личностных характеристик, без которых успешное карьерное продвижение маловероятно. Важно, чтобы такие индивидуальные планы методологически соответствовали бизнес культуре организации, ее традициям и нормам.

Одним из проверенных методов подготовки руководящих кадров в компаниях является направление перспективных специалистов на позиции и участки работы, функциональность которых много шире той специальности, по которой принимался на работу и трудился профессионал. Так проверяется способность работника справляться с поставленной задачей в непривычных, иногда даже дискомфортных для него/нее условиях, проявлять качества, необходимые лидеру.

Тем руководителям, которые планируют себе замену, Бреннан рекомендует практиковать прямой выход кандидатов на деловые контакты с топ менеджментом.

Участие в заседаниях правления, других мероприятиях позволяет перспективным кадрам набираться опыта, а первым лицам непосредственно оценивать деловые и личные качества кадрового резерва.

Желательно иметь в обойме несколько соискателей на замещение руководящей должности. Если в кадровом резерве всего один кандидат, то вы рискуете остаться ни с чем, если он однажды предпочтет делать карьеру в другой организации.

Причины высокой текучести кадров и как с этим бороться

На эту тему высказывается Крис Димитриадис в онлайновом издании Chief Security Officer, April 1, 2020.

Найти и нанять высококвалифицированного специалиста по корпоративной безопасности нелегко. Еще сложнее удержать его в организации. По данным исследования, проведенного ISACA (международная профессиональная ассоциация по вопросам управления информационными технологиями – IT governance), есть 5 фундаментальных причин, по которым уходят кадры:
переманивают конкуренты; ограниченные возможности для профессионального и карьерного роста; неудовлетворенность материальным вознаграждением; рабочие перегрузки; отсутствие внимания и поддержки со стороны менеджмента.

1. Происки конкурентов

Если конкурент может предложить более привлекательную зарплату, то здесь вы мало что сделаете, чтобы удержать специалиста. Однако, деньги не всегда играют решающую роль. Важно понять, почему у конкурента «трава зеленее». Если сотрудник объявил о решении уйти, обязательно надо с ним встретиться и выяснить, какие альтернативы предлагает конкурент. Это важно, чтобы не только попытаться удержать ценного специалиста, но и внести коррективы в кадровую политику.

2. Ограниченные возможности для профессионального и карьерного роста

Инвестиции в обучение, повышение квалификации персонала играют большую роль в удержании кадров. Регулярные занятия по проблемам актуальных угроз и потенциальных уязвимостей в системах охраны и безопасности компании не только повышают эффективность работы команды, но и демонстрируют настрой не жалеть денег на развитие компетенций и знаний. Руководители СБ должны выделять наиболее ценных сотрудников и делать все, что возможно, для их удержания в компании. Если в данный момент нет возможности для продвижения по службе, то, по меньшей мере, надо дать ясно понять, что карьерный рост не за горами, и это поможет справиться с текучестью кадров квалифицированных специалистов.

3. Ограниченность финансов

Малые и средние предприятия не могут конкурировать с акулами бизнеса по части оплаты труда, но могут побороться за ценные кадры между собой. Бизнесменам

нельзя ограничиваться одними лишь разговорами о важности функции безопасности для компании, но надо реально вкладывать деньги в проекты и программы, которые предусматривают достойную зарплату руководителей и ведущих специалистов корпоративной безопасности. Упомянутое выше исследование ISACA выявило, что в большинстве компаний имеются незаполненные вакансии по кибербезопасности, и каждая третья организация тратит полгода и больше, чтобы найти и принять на работу квалифицированного работника. В настоящее время, когда ландшафт угроз и рисков меняется с поразительной быстротой, такая ситуация с кадрами весьма опасна.

4. Перегрузки

Сама по себе работа в области кибербезопасности довольно нервная. Стресс обусловлен калейдоскопом угроз и рисков, форс-мажорными ситуациями, требующими сверхурочной работы по реагированию на инциденты и минимизации последствий. При надлежащей организации труда стресс можно снизить. Это достигается такими способами как регулярная перемена функциональной занятости работников в рамках общих задач, моральная, психологическая поддержка неумышленно ошибающихся сотрудников, наконец, регулярные тренинги, позволяющие не отставать от изменений в тактике поведения и действий криминала.

5. Отсутствие внимания и поддержки со стороны менеджмента

Руководителям корпоративной безопасности надлежит установить правильный стиль, позитивный «тон» для поддержки коллектива. Речь не только об обеспечении команды необходимыми для успешной работы ресурсами. Критически важно внушать акционерам и топ менеджменту, что в нынешних условиях крайне сложно поддерживать надежную безопасность бизнеса, что эта функция требует к себе самого пристального и постоянного внимания, особенно когда случаются инциденты и требуется концентрация усилий и ресурсов по минимизации последствий.

Как меняется индустрия безопасности на Ближнем Востоке

Часть 1

Редактор журнала Security Management Марк Таралло взял интервью у Майкла Пайяно, основателя и президента международной консалтинговой компании Al Thuraya Consultancy, много лет работающего в странах Ближнего Востока.

Как изменилась индустрия безопасности в этом регионе за последние 15 лет?

Пятнадцать лет назад индустрия безопасности, как мы ее сегодня представляем, на Ближнем Востоке не существовала вовсе. Были отдельные компании и консультанты, но четкого понимания, что такое корпоративная безопасность, чем она отличается от государственных структур безопасности, просто не было. Как не было и четкого законодательного регулирования этой отрасли.

Сейчас ситуация постепенно меняется. Основные игроки начинают понимать значение

комплексного подхода к специфическим требованиям каждого клиента на основе разных комбинаций продуктов и услуг. Конечно, еще остается немало проблем, связанных с уровнем профессионализма, воспитанием кадров, законотворчеством.

В чем характерные особенности управления рисками на Ближнем Востоке?

Важно учитывать специфику менталитета народов этого региона. В общественном и бытовом сознании превалирует идея о предопределенности всего, что происходит и совершается в мире, о бессмысленности противостоять божьему промыслу. И трудно что-либо поделать, когда сталкиваешься с плохой подготовкой, неумением и нежеланием осваивать науку управления рисками. Как уже говорил, ситуация медленно, но меняется. Бизнесмены все чаще отзываются на усилия, предпринимаемые профессионалами для минимизации рисков и угроз.

Полагаете ли Вы, что возможности индустрии безопасности в регионе не реализуются в полной мере?

Скорее не возможности, а человеческий капитал далек от своей реализации. Большинство компаний не могут выстраивать органичные взаимоотношения с окружающей их бизнес средой, эффективно использовать имеющийся человеческий потенциал. Здесь всегда ощущался и сегодня еще ощущается разрыв между реальной жизнью и представлением о ней, далеким от действительности. Это важный аспект ментальности людей, который необходимо учитывать, выстраивая отношения партнерства с местными организациями и специалистами.

Что Вы посоветовали бы приехавшему на Ближний Восток профессионалу из Европы с точки зрения адаптации к местной социальной культуре?

Несколько моментов:

- Для начала хорошо изучите свою команду – профессиональное прошлое, знания и навыки.

- Поддерживайте постоянный личный контакт, хотя бы на минимальном уровне: «Доброе утро!»; «Как ваши дела, семья?». Я лично общаюсь с максимально возможным числом персонала, включая шоферов, уборщиков, работников кухни…

- Проявляйте гибкость, понимание, что не все идет по плану, именно так, как вы представляете себе.

- Внимательно слушайте, что вам говорят, а не ищите то, что хотите от них услышать.

- Адаптируйте свой стиль общения под местную культуру, не жертвуя принципами менеджмента.

- Не просто нанимайте способных специалистов, но развивайте их потенциал. Мы принимаем на работу местных профессионалов, при этом много внимания уделяем развитию у них таких качеств как наблюдательность, желание учиться, внимательность к деталям, интерес к расследованиям.

Каков ландшафт рисков и угроз на Ближнем Востоке? Меняется ли он со временем?

У каждой компании собственное представление об угрозах. Но есть и общие, понятные

всем угрозы: киберкриминал, терроризм, геополитическая и социальная нестабильность, переменчивые покупательские предпочтения, изменения климата, развитие технологий, опережающее финансовые возможности компаний.

Сегодня много дискуссий на тему управления рисками предприятия (enterprise security risk management - ESRM). Как выглядит в странах Ближнего Востока концепция «менеджера по управлению рисками компании»?

Даже в развитых странах Запада подход к корпоративной безопасности с позиции перспектив бизнеса, развития организации в целом зачастую носит теоретический, а не практический характер. Что же говорить о странах Ближнего Востока?! Сегодня речь идет о формировании базовых основ профессии корпоративной безопасности, управления рисками. По мере продвижения этих процессов, но не в самом скором будущем, ответ на этот вопрос будет более конкретным и понятным.

Рецензия

Internet of Things, for Things, and by Things
by Adhik Chaudhuri, Auerbach Publications, 257 pages, $79.95

Книга представляет собой глубокое, всеохватывающее исследование сравнительно нового, но уже прочно вошедшего в нашу жизнь феномена под названием «Интернет вещей». Автор подробно характеризует применение Интернета вещей в повседневной жизни, потенциал возможного использования в будущем на примере различных программных продуктов. Рассматривается широкий спектр объектов и инструментов Интернета вещей – от смартфонов до «умного» дома и даже «умного» города. Проблема излагается последовательно, логично и легкодоступно для понимания не специалистами.

Автор книги подробно анализирует как преимущества новых технологий, так и серьезные риски, которые возникают в случае ненадлежащего пользования ими. Он не забывает коснуться и важной темы прайвеси, говоря о необходимости строго соблюдать хрупкий баланс между безопасностью и правом на защиту личной, частной жизни, персональных данных.

Автор рассказывает об обязанностях и ограничениях, которые берет на себя пользователь Интернета вещей.

Он подробно исследует архитектуру Интернета вещей, требования регуляторов, этические аспекты.

Отдельные приложения содержат информацию о рамочных границах, стандартах и глобальных инициативах, связанных с развитием Интернета вещей.

Каждая из глав монографии завершается рекомендацией дополнительной литературы, с которой читатель может ознакомиться.

По мнению рецензентов, книга достойна занять место на книжной полке любого пользователя этими технологиями.

Расходы на кибербезопасность в 2020 году. Тенденции

Исследователи корпорации ESG провели среди специалистов кибербезопасности разных стран опрос относительно перспектив финансирования этой функции в компаниях в текущем году. Краткий отчет опубликован в Chief Security Officer, February, 12, 2020 Опрос проводился в начале года, и пандемия, скорее всего, внесет свои коррективы в полученные результаты исследования. Тем не менее, обнаруженные тенденции интересны тем, что безоговорочно свидетельствуют о растущем значении кибербезопасности в приоритетах мирового бизнеса.

Вот основные цифры:

- 55% организаций планируют в 2020 году увеличить вложения в целом в цифровые технологии. Это практически каждая вторая организация в здравоохранении, в сфере технологий, в оптовой и розничной торговле, в производственных отраслях, в сфере услуг.

- На вопрос о мотивах и причинах роста инвестиций 36% респондентов ответили, что их организации хотят улучшить работу по управлению рисками, особенно киберрисками.

- 62% организаций увеличат вложения непосредственно в кибербезопасность. Остальные 38% сохранят бюджеты кибербезопасности на уровне последнего года. Самый большой процент компаний, настроенных на рост бюджета кибербезопасности, – технологические организации (73%), затем идут производственные отрасли (68%) и торговля (67%).

- Главные объекты инвестиций в 2020 году: системы предупреждения и обнаружения киберугроз (32%); защита данных (31%); безопасность корпоративных сетей, виртуального периметра безопасности (30%); защита облачных приложений (27%). По мнению экспертов, особое внимание необходимо уделить совершенствованию систем защиты данных и приложений(31%).

- 40% опрошенных назвали кибербезопасность в качестве главного фактора и стимулятора технологических расходов в ближайшие двенадцать месяцев. На втором месте – снижение цен. Это говорит о том, что уже не информационные технологии в комплексе, а кибербезопасность становится главным императивом планирования бюджета IT.

- Среди глобальных технологических трендов самым важным 24% называют улучшение инструментов и процессов кибербезопасности, 14% - укрепление инфраструктуры облачных вычислений.

_ На вопрос, какие характеристики корпоративных сетей респонденты считают наиболее актуальными для бизнеса в ближайшие 12 месяцев, 43% ответили - «защита и безопасность сетей», 29% - «повышение производственной эффективности сетей». Налицо признание приоритета безопасности. И это, полагают эксперты, очень хороший тренд.

Кроме продемонстрированных цифр, авторы исследования сформулировали некоторые выводы:

1. Безопасность в широком смысле, и в первую очередь кибербезопасность, становится важным приоритетом для первых лиц и членов правления компаний.

2. Отношение к вопросам кибербезопасности отличается от сектора к сектору экономики и бизнеса. Например, конкретные требования к кибербезопасности в сети здравоохранения с персоналом 10 000 человек существенно отличаются от требований, предъявляемых финансовыми организациями сопоставимого размера. Эти отличия должны изучаться производителями технологий и находить свое отражение в выпуске конкретной продукции, в маркетинге и продажах.

3. Некоторые вещи не работают. Тот факт, что компании вынуждены каждый год увеличивать вложения в технологии, не должен слишком радовать. У этой тенденции есть и обратная сторона, показывающая, что производство систем кибербезопасности явно отстает от растущих потребностей, не справляется со спросом. У этой индустрии огромный, пока еще не использованный, потенциал развития.