В 2017 году в Европейском регионе, куда входит Россия, кибер-риски заняли второе место среди наиболее серьезных рисков для предприятий. Об этом говорится в ежегодном исследовании Allianz Risk Barometer, которое проводится среди директоров и риск-менеджеров крупных предприятий.
В 2016 году по количеству зарегистрированных утечек информации Россия заняла второе место (213 зарегистрированных случаев утечки конфиденциальной информации и 70 млн атак на российские информресурсы). В среднем одна украденная запись обходится компании в 158$, а в будущем эта цифра может увеличиться до $200-300. Ущерб от кибератак в России в 2015 году составил 203,3 млрд рублей (0,25% ВВП). Среди громких кибератак в России последних лет — утечки персональных данных и SMS у оператора сотовой связи «Мегафон» в 2011 году, атаки на банки с целью вымогательства (инцидент с «Банком Санкт-Петербург») в 2016 и в 2015 годах, а также атаки вируса WannaCrypt0r 2.0. В марте 2017 года вирус проник в ряд банкоматов, предприятий («Мегафон», «РЖД»), банков («Сбербанк») и госучреждений («МВД»). Пострадавшие организации не были застрахованы от кибератак. Каков может быть размер потенциального ущерба? По данным страховой компании Allianz, крупные компании в среднем тратят около 11 млн рублей на ликвидацию последствий, средние и малые – 1,6 млн рублей. И это без размера прямого убытка.
На фоне возрастающих угроз инвестиции в информационную безопасность крайне необходимы. При этом нужно помнить, что превентивные меры не дают 100% гарантии, именно поэтому важно подумать о минимизации возможного ущерба, если все же атаку не удалось остановить. Для таких случаев есть продукты страхования кибер-рисков.
В настоящее время объем страховых премий в России на данном рынке не превышает 10 млн рублей. Однако согласно оценкам Mains Insurance Brokers & Consultants, уже в 2019 году начнется экспоненциальный рост рынка, а в 2025 году его объем достигнет 1 млрд рублей.
Важно отметить, что существует прямая зависимость между скоростью обнаружения и нейтрализации утечки и стоимостью урегулирования. С каждым годом такие расходы растут, что говорит о необходимости инвестиций в технологии защиты данных и развития внутренней экспертизы для сокращения времени реагирования и обнаружения утечки, а также быть уверенными в компенсации затрат на привлечение сторонних экспертов для снижения размера убытка.

Законодательство в области страхования киберрисков

В России законодательство в части нарушения сохранности данных развито слабо.

Сумма штрафов варьируется от 1 до 50 тыс. рублей. Однако ситуация должна измениться в ближайшие годы. В рамках программы «Цифровая экономика» государство реализует меры, направленные на формирование цивилизованного рынка кибер-страхования в России. Одной из таких мер может стать обязательная покупка полиса страхования киберрисков.

«Законодательные органы, как в России, так и за рубежом, проявляют большой интерес к регулированию онлайн среды и контента – подтверждением тому служат «Закон Яровой» и GDPR, которые должны вступить в силу летом 2018 года. Одновременно с ужесточением требований к работе компаний, эти законы повышают и ценность самих персональных данных. Даже если страхование кибер-рисков и не станет обязательным, законодательных предпосылок для добровольного страхования кибер-риски становится все больше», — комментирует Вадим Михневич, Заместитель директора департамента страхования финансовых линий Allianz.

«Уже сейчас в подразделениях риск-менеджмента наших корпоративных клиентов мы наблюдаем активность, связанную с подготовкой стратегии сокращения ущерба от киберрисков через инструменты страхования. Это очень хороший тренд, и его результаты будут наблюдаться уже к концу следующего года», — говорит Павел Озеров, Заместитель генерального директора Mainsgroup.
«Актуальность страхования киберрисков для ИТ компаний, связана с ростом рынка аутсорсинга и облачных решений. ИТ-компании начинают отвечать перед своими клиентами за риски утери данных клиентов и/или хакерских атак, которые приводят в том числе к потерям у клиентов как данных, так и денег. В качестве примера, можно привести компанию, оказывающую услуги по разработке и поддержки Автоматизированной Банковской Системы из-за ошибок разработки и/или поддержки Банк может потерять существенные денежные средства и взыскать их со своего подрядчика», — дополняет коллег Кирилл Солодовников Генеральный директор ГК «Инфосекьюрити».

Источник: Википедия страхования, 29.11.2017