Представители страхового сообщества все чаще задумываются о новых точках роста для бизнеса. Одной из таких новоявленных опор может стать страхование кибер-рисков, убежден президент Российской национальной перестраховочной компании (РНПК) Николай Галушин.

О том, как это устроено в мире и как дела могут обстоять у нас, он рассказал в интервью порталу Коринс.ру.

— Видите ли вы заинтересованность в проекте страхования кибер-рисков в РФ, с какими страховщиками ведутся переговоры о сотрудничестве?

— Стоит начать с того, что сегодня в области кибер-страхования в мире очень прочное место занимает США. На сборы по этому виду страхования в США приходится более 90% всех мировых сборов страховой премии по кибер-страхованию.

С чем это связано? С повышенной опасностью или с высокой страховой культурой? Не совсем так.

Ответа два – требуется декларировать специальной государственной службе все факты кибер-атак, а, кроме того, менеджмент компаний несет ответственность за последствия для бизнеса от кибер-атак. Оба эти фактора и породили ответное действие – страховую услугу по страхованию последствий от кибер-атак.

Было высказано мнение о том, что сегодня есть две категорий компаний в привязке к действиям кибер-преступников: те компании, которые уже подвергались атакам, и те, которые не знают, что их системы уже поражены действиями кибер-преступников.

В России с точки зрения страхования кибер-страхования мы находимся в начале большого пути. У нескольких компаний есть базовые продукты, которые они готовы предлагать клиентам, но сами процедуры принятия рисков на страхование достаточно сложны.

Простого решения нет, как нет и простого способа оценить качество риска при принятии его на страхование и объективно оценить последствия кибер-атаки. При РНПК создана рабочая группа из страховщиков, которые готовы тему кибер-страхования развивать. Идет обсуждение. Мы исходим из того, что совместными усилиями надо попытаться формализовать страховой продукт, который бы мог заинтересовать российский бизнес. А риски по продукту могут быть распределены через перестрахование с участием РНПК. Ведущие страховщики страны входят в рабочую группу.

— Какая модель сотрудничества может быть выстроена, какое место в ней может быть

отведено РНПК?
— У нас место есть. Мы перестраховщик, который должен снять часть риска (и, соответственно, часть убытка) со страховщиков при реализации кибер-страхования. И мы хотим, чтобы участники рынка смогли сформулировать общее видение возможного страхового продукта, включая все его составные части: оценка риска, тарификация, набор рисков, процедуры урегулирования убытков.
— Есть ли оценка потенциального объём рынка страхования кибер-рисков в РФ?
— Такая оценка не производилась. Сейчас речь идет о нескольких миллионах рублей, потому что рынка кибер-страхования просто нет. Все дальнейшее (к сожалению, совсем небыстрая история) зависит от действий страховщиков и от окружающих факторов, которыми могут быть, например, регуляторные требования, требования кредиторов и инвесторов, увеличение случаев кибер-преступлений и т.д.
— Что может в себя включать покрытие? Что вы понимаете под кибер-страхованием?
— Сейчас это означает повреждение имущества страхователя (самое разнообразное – от станочного парка до компьютерных систем и баз данных) в результате стороннего и несанкционированного вмешательства в информационные системы страхователя, а также – в качестве дополнительной опции — убытки от перерыва в производстве / деятельности в результате такого вмешательства. Также может быть предоставлено покрытие в отношении гражданской ответственности перед третьими лицами за вред, который может быть нанесен в результате вмешательства в информационные системы и манипулирования с чужой информацией.
— Кто потенциально может выступать страхователем?
— Абсолютно все, кто имеет доступ в интернет. Уязвимы все – от пользователей домашних компьютеров и до …
— Из чего складывается тариф? Какая база для оценки берётся за основу?
— Непростой вопрос. Поскольку нет рынка, то сейчас он складывается не из истории убытков на рынке, а из факторов взаимодействия с конкретным потенциальным клиентом: страховая сумма, деятельность страхователя, насколько система уязвима или представляет интерес для потенциальных злоумышленников, сценарии возможных последствий для деятельности компании в результате несанкционированного проникновения, наличие внутреннего плана действий на случай подобных ЧП, способы защиты информации и систем, отношение менеджмента к защите, причины покупки страхования и т.д.
— Были ли нашумевшие случаи наступления кибер-рисков, как оценивались потери? В какую сумму можно оценить максимальный размер лимита по 1 случаю?
— В нашей практике нет. Мы подписали долю участия в облигаторном договоре одной международной компании по кибер-страхованию. Хотим использовать этот опыт и для наращивания практики в России. Пока ведется общение с несколькими компаниями по запуску совместных (двухсторонних) проектов. Мы не хотели бы начинать нашу практику с больших страховых сумм, потому что в случае убытка это может остановить всю последующую деятельность по этому направлению. По этой причине мы предпочли бы формировать сбалансированный перестраховочный портфель с не очень крупными страховыми суммами и постепенно формировать историю страхования клиентов, увеличивая страховые суммы и расширяя покрытие.
— Какие тренды вы видите в мире? Действительно ли это самое быстрорастущее направление страхования в США и Британии?

— Как уже сказал, основной рынок — это США. Великобритания и континентальная Европа — это еще около 5-6 %. Все остальное – остальной мир.
— Ряд зарубежных программ гарантируют погашение расходов на восстановление баз данных, которые были утеряны, либо частично украдены; покрытие расходов на PR-деятельность, связанную восстановлением имиджа; погашение судебных издержек, возникших вследствие подачи исков по потере информации; покрытие рисков ошибок программирования, когда неверный код приводит к сбою. Дополнительно к этим программам предлагается аудит IT-систем.
Какие составляющие этих программ могли бы быть востребованы в РФ, какие нет и почему?
— Допускаю, что они все могут быть востребованы и в российской практике. Но начинать, как мне кажется, надо с защиты собственных рисков страхователя – имущества и убытков от перерыва в деятельности.
— Возможно ли участие РНПК в перестраховании наряду с зарубежными партнёрами цедентов?
— Возможно точно. В рамках обязательной цессии в размере 10% так точно. Но мы заинтересованы в адаптации международной практики кибер-страхования к потребностям российских клиентов и в увеличении вовлеченности РНПК в перестрахование таких проектов.
— Каким может быть место ВСС в этом проекте?
— Все, что может быть выработано рабочей группой страховщиков, которая сейчас действует на базе РНПК, может быть растиражировано на общей площадке ВСС. Мы собственно и не разделяем эти площадки.
— Кто является основным конкурентом РНПК в проекте развития направления кибер-страхования?
— Нам нужно рынок создать. Когда будут клиенты у страховщиков, когда страховщики будут нуждаться в емкости, когда за эту емкость будут бороться перестраховщики – только тогда можно будет говорить о конкурентах РНПК. Пока мы все партнеры. Надеюсь, что так будет и дальше.
— Когда стоит ждать первых контрактов?
— Скоро.

korins.ru, 29.08.2017