

Как стало известно РБК daily, страховая компания «Чартис» будет предлагать российским клиентам новую услугу – страховку ответственности за сохранность информации. Страховщик рассчитывает, что услуга будет востребована компаниями, имеющими дело с обработкой и хранением больших объемов информации, но не располагающими собственными службами кибербезопасности.

Руководитель отдела страхования финансовых рисков «Чартис» Владимир Кремер сообщил РБК daily, что компания намерена предложить клиентам в России страхование киберрисков. «Его суть в страховании ответственности операторов данных за вверенную им информацию, – сообщил он. – Компании смогут защитить себя от возможных финансовых потерь, связанных с обработкой данных». Также они страхуют свою ответственность перед клиентами.

Подобный продукт известен за рубежом как CyberEdge. В США им активно пользуются клиенты, которым по роду бизнеса приходится обрабатывать большие объемы информации. В Европе этот сервис появился лишь год назад. По словам г-на Кремера, полис страхования киберрисков дает возможность компании получить компенсацию, если в результате атаки хакеров она потеряла данные и понесла убытки.

«У оператора могут быть расходы, связанные с восстановлением IT-платформ и юридическими услугами в связи с возможными исками от третьих лиц, интересы которых пострадали», – говорит топ-менеджер. В качестве примера в «Чартис» приводят недавний случай с одним российским сотовым оператором, SMS-сообщения которого оказались в открытом доступе в Yandex. «В этом случае компания несет репутационные потери, а также вынуждена тратить средства на поиск причин утечки данных, создание новой системы защиты, – говорит Владимир Кремер. – Услуги профессиональных IT-специалистов стоят недешево».

В «Чартисе» не раскрывают, во сколько обойдется страховка от потери информации. По словам представителя страховщика, оценка стоимости полиса будет производиться на основе нескольких факторов: наличия и эффективности работы систем защиты данных, качества IT-систем, размера компании и наличия подобных прецедентов. «Понятно, что у

крупной компании вероятность подобного инцидента выше, потому что она оперирует большими объемами информации, – пояснил Владимир Кремер. – Но у нее, как правило, есть своя служба безопасности, свой штат юристов и IT-специалистов. Поэтому мы больше ориентируемся на средний и малый бизнес, для которого киберстрахование открывает возможность получения всех этих возможностей на аутсорсинге».

Управляющий директор Optima Infosecurity Неманья Никитович считает, что страхование подобных рисков может быть востребовано рынком, особенно финансовыми институтами, которые предлагают онлайн-сервисы и потому более других подвержены кибератакам. «Страхование поможет покрыть расходы на бэкап и восстановление утраченной информации, – говорит он. – DDOS-атаки являются самыми распространенными угрозами, однако страховые компании, скорее всего, посчитают необходимым временем для наступления страхового случая выведение системы из строя на срок не менее 12 часов. Более краткое воздействие не будет считаться достаточно серьезным, так как не представляет угрозы для бизнеса».

Как считает директор центра технологий безопасности IBS Дмитрий Романченко, предоставлять такую услугу с полным покрытием прямых потерь и упущенной выгоды конечного заказчика для какой-либо страховой компании в отношении крупного бизнеса крайне рискованно. «Дело в том, что IT-инфраструктура таких компаний сейчас подвергается постоянным атакам злоумышленников и гарантировать ее работоспособность все время достаточно сложно», – пояснил он. По мнению г-на Романченко, любой такой сбой может привести к значительным потерям для клиента и, следовательно, росту страховых выплат.

Представители финансового рынка скептически в оценке перспектив киберстрахования. Глава Национального бюро кредитных историй Александр Викулин говорит, что компания давно застраховала себя. «Наши базы данных копируются и хранятся в двух и даже трех различных местах, то есть если бомба упадет в одно место, то информация никуда не денется», – уверен он.

По мнению председателя правления банка «Авангард» Валерия Торхова, потеря базы данных будет колоссальным репутационным ударом. «Стоит ли платить в такой ситуации страховую премию, сказать сложно. Может быть, лучше позаботиться о мерах по дополнительной защите своих баз данных», – рассуждает банкир.

«Если такое произойдет, я никакой страховкой не откуплюсь, разом останусь без заказов и без работы, – говорит гендиректор Агентства по возврату долгов Станислав Федоровичев. – Нельзя застраховаться от потери репутации. Понимаете, когда человек умирает, ему все равно, в каких тапочках похоронят – белых или черных».

Источник: [РБК daily](#) , 31.10.12

Авторы: Кошкарров А., Петлевой В., Старостина Н.