Осознаем мы это или нет, но все мы – заложники Ассанжа, Мэннинга, Сноудена, а также группы «Анонимус» и им подобных в борьбе с государством. Разоблачая закулисные игры «больших братьев», активисты приставили пистолет к голове каждого гражданина. Заряды, правда, виртуальные: все возможные сведения о любом человеке или юридическом лице, тщательно оберегаемые из самых разных соображений. Что может в такой ситуации сделать отдельный человек или компания?

Обезопасить каждого персонально, подручными средствами почти невозможно, для гарантии придется просто отказаться от любого использования технологий. Частный бизнес всегда был более осмотрителен – количество и разнообразие услуг по защите в виртуальном пространстве растет вместе с ним. Причем многое из этой защиты распространяется на клиентов, а что-то – на клиентов в первую очередь. Миллиарды долларов тратятся на усиление безопасности бизнес-процессов.

Наибольшее внимание пока уделяется технологической составляющей безопасности – работе IT-служб и сервисов, противовирусной и противохакерской защите, многослойному обеспечению бесперебойной деятельности всех структур. Чуть меньше – в силу непредсказуемости – компании защищены от человеческого фактора, как от элементарных ошибок, так и целенаправленных действий изнутри. И, к сожалению, еще реже речь идет о защите на случай, если сбой уже случился и повлек за собой неприятные последствия в виде финансового, а также репутационного ущерба.

Самые свежие данные этого года от NSSLabs, ведущей компании в области информационных исследований, показывают, что рынок киберстрахования пока еще не может считаться развитым. Так, например, даже в США подобные услуги предлагают всего лишь несколько десятков компаний, тогда как всего на рынке страхования работают около 5000 участников. В таком положении виноваты и потребители, и страховщики. Первые с недоверием относятся к подобным услугам, считая, что достаточно технически защититься от всевозможных проблем. У страховщиков же определенное время заняло формулирование своих предложений по страхованию киберрисков в условиях постоянно меняющейся виртуальной реальности.

Многое в этих условиях зависит и от государства. Для начала можно было бы обязать определенные категории бизнеса оформлять страховку от киберрисков. Например, это может касаться компаний, которые хотят вести дела с государственными органами. В скором времени и другие компании тоже начали бы интересоваться подобным

страхованием.

Конечно, страхование каждого отдельного человека, имеющего доступ к высоким технологиям, пусть даже в виде ноутбука – это еще вопрос не слишком близкого будущего. Хотя для сравнения стоит посмотреть, сколько времени прошло от появления первого частного автомобиля до введения обязательного страхования автогражданской ответственности. А ведь сегодня внедрение любых новаций проходит в десятки раз быстрее.

Сейчас существование в виртуальности на собственных условиях вполне реально. Это касается как каждого отдельного гражданина, который может выбирать, с кем ему вести дела, кому доверить свои секреты, так и частного бизнеса. В его интересах и силах обеспечить себе, партнерам и клиентам максимально высокий уровень виртуальной безопасности.

Источник: РБК daily , 18.11.13

Автор: Владимир Кремер, руководитель отдела страхования финансовых рисков AIG в России