740 млн конфиденциальных файлов было украдено или незаконно просмотрено киберпреступниками в 2013 году. 2013 год стал худшим по этому показателю за все время. Такие данные приводит исследование, подготовленное страховой компанией Zurich Insurance Group совместно с аналитическим агентством Atlantic Council.

В исследовании говорится, что порядка 2,5 миллиарда человек – почти треть всего населения земли – регулярно пользуются Интернетом и в среднем на каждого человека приходится по 6 гаджетов, подключенных к мировой Сети. Каждую минуту отправляются 204 млн электронных писем, передаются 640 терабайтов данных и публикуются 100000 твитов.

При таком объеме циркуляции данных конфиденциальная информация находится в весьма уязвимом положении, которое может стать причиной серьезных экономических потрясений. На сегодняшний момент в мире нет достаточных технологий, способных защитить частных лиц и организаций от всех киберрисков. Если компания не способна смягчить эти сложные и взаимосвязанные риски, то возрастает вероятность внезапного потрясения, сопоставимого по масштабу с крахом Lehman Brothers на ипотечном рынке в 2008 году.

Проведенное исследование выделяет четыре источника киберрисков – это преступники, хакеры, шпионы и военные.

Преступники обычно используют похищенную информацию с целью ее продажи. Чаще других от них страдают организации, работающие с персональными данными своих клиентов. Хакеры действуют масштабнее – они нарушают работу сетей компаний или похищают информацию, которая может скомпрометировать организацию или человека.

Третьей традиционной киберугрозой является шпионаж, целью которого становятся исследования компаний, новейшие разработки, стратегии переговоров и бизнес-планы. Ярким примером может служить история прошлого года, когда китайские хакеры похитили чертежи нового здания разведывательного управления Австралии. Четвертая группа – военные. Они специализируются на обрушении целых сетей и систем, включая инфраструктурные и индустриальные. Такое, правда, случается довольно редко.

Перечень этих рисков уже завтра может дополниться новыми – вторжением в облачные технологии, в систему автомобилей «без водителей», медицинские аппараты и интеллектуальные энергосистемы (smart grid). Все более тесная связь Интернета с реальной экономикой и обществом может привести к широкомасштабному потрясению, даже более серьезному, чем готовы признать риск-менеджеры и интернет-специалисты. Подвергнуться атаке могут банки, системы водоснабжения, автомобили, медицинские устройства, плотины гидроэлектростанций.

Выходом в этой ситуации может стать создание альтернативных сетей на случай кибератак, а также повышенное внимание топ-менеджмента компаний к защите информации. На сегодняшний день в подавляющем большинстве компании не фиксируют факты кибератак и зачастую даже не знают, что их конфиденциальные данные уже стали достоянием киберпреступников.

При существующей динамике нарастания киберугроз страхование от киберрисков в самом ближайшем будущем может перейти из категории экзотики в категорию стандартных страховых опций, а область деятельности риск-инженеров пополнится мониторингом систем эффективной электронной информации.

Информация предоставлена компанией

Источник: Википедия страхования , 19.05.14