Кибер-риски – глобальная проблема современности

Примеры из практики Chartis в США

Инцидент «Нелояльный сотрудник»

На компанию был подан иск в суд после того, как один из сотрудников присвоил конфиденциальную информацию, поступившую от конкурента.

Выплаты Chartis US по данному инциденту составили порядка $200 000.

Инцидент «Хакерский взлом»

Хакеры получили доступ к компьютерным системам 26 отелей и могли получить имена и номера кредитных карт примерно 480 000 клиентов.

Страховые выплаты Chartis US на урегулирование последствий инцидента составили более $980 000.

Инцидент «Ошибка/Халатность»

Застрахованный непреднамеренно разместил в открытом доступе на своем сайте конфиденциальные данные более 42 000 студентов. Родители одного из пострадавших подали иск в суд о нарушении права на частную жизнь. Кроме того, по итогам инцидента Федеральная Торговая Комиссия (ФТК) начала расследование на предмет соблюдения застрахованным Акта ФТК, запрещающего искажение фактов при обработке конфиденциальных данных.

Выплаты Chartis US на судебные издержки составили порядка $250 000.

Инцидент «Потерянное/украденное оборудование»

Застрахованный потерял носители с информацией о медицинской страховке и номерах социального страхования.

Страховое возмещение на расходы по содержанию call-центра и мониторинга репутации застрахованного составило $400 000.

Кибер-риски – глобальная проблема современности

Статистика киберпреступлений

Страхование кибер-рисков – новое направление на российском рынке страхования, обладающее колоссальным потенциалом развития.

Преступность в киберпространстве становится одной из главных проблем современного мира электронных технологий. Такое мнение высказали участники Всемирного экономического форума, состоявшегося в Давосе в январе 2012 года.

С оценкой лидеров мировой экономики согласны эксперты PricewaterhouseCoopers. За последний год масштабы киберпреступности значительно выросли, отмечается во Всемирном обзоре экономических преступлений, подготовленном PwC. Противозаконная деятельность в глобальном киберпространстве прочно занимает вторую строку в рейтинге экономических преступлений, уступая только такому виду, как незаконное присвоение активов.

На киберпреступления приходится 38% экономических преступлений в секторе финансовых услуг. Жертвами мошенничества признали себя 45% опрошенных экспертами PwC участников рынка.

Киберпреступность не знает географических и государственных границ. Сегодня на планете более 9 миллиардов подключенных электронных устройств, и эксперты прогнозируют рост их числа до 24 миллиардов единиц к 2020 году. По сведениям Европейской Комиссии, нападению киберпреступников ежедневно подвергается более 1 миллиона человек во всем мире. От действий преступников, охотящихся за конфиденциальными данными, пострадали, в частности, 77 миллионов клиентов компании Sony. 600 тысяч пользовательских записей Facebook блокируются каждый день после попыток хакерского взлома.

Мировая тенденция к росту киберпреступности не обошла стороной и Россию. По данным аналитического центра компании Zecurion, в 2011 году в мире было зарегистрировано 819 случаев утечки данных. Суммарный ущерб от них составил $20 млрд, из которых более $1 млрд. пришлось на российские компании. В том же году в России был зарегистрирован 41 инцидент, связанный с утечкой конфиденциальных данных из компьютерных сетей компаний. Данные исследования свидетельствуют о том, что участились случаи обнародования информации о клиентах со стороны российских интернет-магазинов. При этом в России стабильно растет количество публичных инцидентов.

Кибер-риски – глобальная проблема современности

Угрозы, связанные с информационными рисками, так же опасны, как угрозы физическим активам компании. Инциденты, связанные с утечкой данных, как правило, вызывают цепную реакцию и наносят значительный репутационный и финансовый ущерб.

Таким образом, защита информации становится приоритетной задачей для компаний, особенно в связи с текущей тенденцией развития нормативно-правовой базы в сторону усиления ответственности компаний за сохранение конфиденциальности и защиту данных. Так, внесенное в апреле Европейской Комиссией предложение о комплексной реформе закона ЕС о правилах защиты информации 1995 года, в частности, предполагает:

Введение единого пакета правил о защите данных, действительных на всей территории Евросоюза;

Повышенную ответственность и подотчетность для компаний, осуществляющих обработку персональных данных (например, компании и организации обязаны незамедлительно уведомлять контрольные органы в случае серьезных инцидентов, связанных с несанкционированным использованием данных, по возможности, в течение 24 часов);

Наделение независимых национальных органов по защите данных дополнительными полномочиями на применение штрафных санкций в отношении компаний, допускающих нарушения правил (такие штрафы составят до 1 миллиона евро или до 2% от глобального ежегодного оборота компании).

Еврокомиссия также выступила с предложением создать Европейский центр по борьбе с киберпреступностью, входящий в Европейское полицейское ведомство (Европол) в Гааге. Такая структура станет европейским координационным центром по борьбе с киберпреступностью и сосредоточится на организованной незаконной деятельности в сети.

Нередко компании осознают риск, связанный с незаконным доступом к данным, но не располагают достаточными ресурсами для эффективного реагирования на действия преступников. В этом случае мощным заслоном на пути киберпреступности становится система страхования кибер-рисков.

Примеры из мировой практики

Компания Epsilon

В марте 2011 года в международной компании Epsilon, базирующейся в США, был зафиксирован инцидент, когда к блоку клиентской информации Epsilon был получен доступ посредством несанкционированного проникновения в систему электронной почты компании.

На момент инцидента в компании подчеркивали, что «раскрытая информация ограничивалась исключительно адресами электронной почты и/или именами клиентов. Тщательная проверка позволила определить, что угроза распространения любой прочей личной информации отсутствует».

В связи с этим компания Marks&Spencer (M&S), которая является клиентом компании Epsilon, была вынуждена предупредить своих клиентов о возможном использовании их персональных данных в мошеннических целях.

Клиентов предупредили, что они могут получать нежелательные сообщения, однако, как подчеркивалось, в компании «относились крайне серьезно к обеспечению конфиденциальности их личной информации» и намеревались «продолжать прилагать все усилия для защиты личной информации».

Кибер-риски – глобальная проблема современности

На тот момент представители Офиса комиссара по информационным вопросам Великобритании заявили о начале расследования касательно факта нарушения Закона о защите данных Великобритании. Среди прочих клиентов компании Epsilon числятся такие компании, как Hilton Hotels, Best Buy, Barclaycard US и Capital One.

Компания Betfair

В прошлом году компания онлайн азартных игр Betfair признала то, что ее клиенты не были проинформированы о крупной утечке данных. В 2010 году были похищены данные, включающие 3,1 миллиона учетных записей с зашифрованными ответами на контрольные вопросы, 2,9 миллиона имен пользователей, а также почти 90 000 имен учетных записей с данными о банковских счетах.

В компании Betfair также признали то, что об атаке стало известно лишь два месяца спустя, когда вышел из строя сервер в центре обработки данных компании на Мальте. Как утверждали представители компании, необходимость в уведомлении клиентов отсутствовала, так как меры по обеспечению безопасности препятствовали использованию данных в мошеннических целях.

Когда стало известно об утечке, компания Betfair проинформировала Агентство по борьбе с особо опасной организованной преступностью, а также Австралийскую федеральную полицию и немецкие государственные органы. В компании узнали об утечке данных случайно – когда социальный работник, забравший конфиденциальные бумажные документы на дом, был затем ограблен.

Компания Global Payments

В марте 2012 года было объявлено, что процессинговый центр Global Payments, находящийся в Атланте, стал жертвой «несанкционированного доступа» в систему. Об этом были уведомлены правоохранительные органы и финансовые учреждения.

Операторы платежных систем MasterCard, Visa, American Express и Discover Financial Services подтвердили, что они стали жертвами инцидента, наряду с банками и прочими представителями клиентской базы.

После публикации сообщения об инциденте в СМИ акции MasterCard упали на 1,8%, а акции Visa – на 0,8%, даже несмотря на тот факт, что аналитики выражали сомнения в том, что этим компаниям грозили иски со стороны контролирующих органов.

По сообщениям, жертвами могли стать около 10 миллионов держателей карт по всему миру, однако компания незамедлительно сообщила, что количество пострадавших клиентов составило 1,5 миллиона жителей исключительно в Северной Америке. Представители компании сообщили, что были украдены данные Track2, а не личные данные клиентов, и что в компании считали, что утечку данных удалось локализовать.