

**Экспертные, непредвзятые репортажи из Газы, Израиля и Ближнего Востока.**  
 Попробуйте комплексное покрытие FT всего за 1 фунт

Попробуйте за 1 фунт стерлингов

Специальный отчет кибербезопасности



Кибербезопасность

## Взлом данных и крупные штрафы стимулируют рост киберстрахования

Страховщики рассматривают цифровую безопасность как шанс для расширения, несмотря на неопределенность в отношении рисков



Гостиничная группа Marriott подверглась хакерской атаке, в результате которой были обнародованы данные о 339 миллионах постояльцев © Bloomberg

Оливер Ральф 20 НОЯБРЯ 2019



### Будьте в курсе с бесплатными обновлениями

Просто подпишитесь на Дайджест myFT по кибербезопасности, который будет отправлен прямо на ваш почтовый ящик.

Sign up

Утечка данных может стоить дорого — просто спросите Marriott. В ноябре прошлого года гостиничная группа заявила, что хакеры получали доступ к ее базе данных с 2014 года, скомпрометировав до 339 миллионов записей гостей.

С тех пор компания понесла расходы в размере 100 миллионов долларов, связанные со взломом, и это до потенциального штрафа в 99 миллионов фунтов, взимаемого по правилам ЕС.

Однако эффект был смягчен страховыми полисами, по которым компании было выплачено 102 миллиона долларов.

Киберзащита - одна из самых быстрорастущих составляющих страховой отрасли. Громкие утечки данных и атаки программ-вымогателей, такие как атаки WannaCry и NotPetya в 2017 году, убедили компании в необходимости защиты.

“NotPetya стала огромным стимулом для покупок за пределами США, поскольку [компания] увидели, как на самом деле выглядит прерывание бизнеса”, - говорит Сара Стивенс, руководитель практики кибербезопасности, медиа и технологий в страховом брокере Marsh JLT Specialty.

История киберстрахования берет свое начало в 1990-х годах, когда все большее число компаний электронной коммерции стремились защитить себя от риска того, что хакеры взломают их веб-сайты.

В последнее время этот рост наблюдается в США, где правила защиты данных и штрафы за утечку данных убедили компании покупать страховку.

Эта тенденция распространяется и на Европу, где правила обработки данных GDPR, вступившие в силу в прошлом году, как ожидается, приведут к волне штрафов — например, British Airways была временно оштрафована на 183 млн фунтов стерлингов за утечку данных в 2018 году.

Неясно, могут ли штрафы покрываться страховкой в соответствии с законодательством ЕС, но брокеры говорят, что потенциальные штрафы, с которыми сталкиваются BA и Marriott, повысили осведомленность о рисках, связанных с утечкой данных.

Другой растущий рынок - малые и средние предприятия. Брокеры говорят, что проникновение по-прежнему низкое, но, учитывая их меньшие ресурсы, эти компании особенно уязвимы для кибератак.

“Мы наблюдаем все большее распространение киберстрахования, особенно в отраслях, где мы видим риск утечки данных, таких как розничная торговля, здравоохранение, все, кто занимается анализом данных, и компании, работающие с крупными глобальными фирмами”, - говорит г-жа Стивенс.

# Прогноз стоимости глобального рынка киберстрахования на 2022 год в размере 15 млрд

Полисы киберстрахования выплачиваются клиентам, подвергшимся атаке, во многом так же, как и обычные страховые полисы. Но часто в продукте присутствует и сервисный элемент, который оказывает практическую помощь клиентам, чьи системы подверглись атаке.

Эти службы могут включать судебных следователей, которые исследуют причины и предлагают решения, экспертов по связям с общественностью, которые устраняют ущерб репутации, и даже опытных переговорщиков, которые рассматривают требования о выкупе и организуют его оплату, часто с помощью биткойнов.

Страховые компании рассматривают киберпространство как редкую возможность для роста и спешат выйти на рынок. Почти 200 страховщиков предлагают киберстрахование в

США, в то время как ожидается, что мировой рынок киберстрахования вырастет примерно с \$ 6 млрд премий в год до \$ 15 млрд к 2022 году, по данным RBC Capital Markets.

Но этот рост может повлечь за собой высокие издержки для страховых компаний.

Хотя существуют сложные модели для известных рисков, таких как наводнения и штормы, киберриски бывают разными.

“Кибермоделирование все еще находится в зачаточном состоянии”, - говорит Ребекка Боле, руководитель отдела взаимодействия с отраслью в CyberCube, специалист по кибермоделированию. “Это опасность, сильно отличающаяся от опасностей, связанных с погодой, где научные данные задокументированы и хорошо поняты. Кибер - это опасность, созданная человеком, которая создает много сложностей”.

Страховщикам и разработчикам моделей приходится сталкиваться с постоянно меняющимся характером кибератак, а также с неопределенностью в отношении того, кто их совершает, чего они хотят, какой ущерб они могут нанести и как быстро эффект атаки может распространиться по всему миру.

“Мы знаем о [риске катастроф] больше, чем о кибербезопасности”, - заявил Брайан Дюперро, исполнительный директор страховщика AIG, на недавнем саммите Financial Times / PwC по страхованию. “У плохих парней отдел исследований и разработок лучше, чем у нас”.

Он сказал, что клиенты AIG пользуются большим спросом на страховое покрытие. “Каждый клиент сталкивается с киберугрозами — это самый большой глобальный риск, с которым мы сталкиваемся”.

Возможная стоимость крупномасштабных атак поражает воображение. CyberCube и Гай Карпентер, страховой брокер, смоделировали сценарии, которые могут привести к большим потерям для отрасли. Например, длительный сбой в работе крупного поставщика облачных услуг может привести к выплатам в размере 14,3 млрд долларов, в то время как массовая кража у поставщика услуг электронной почты может привести к убыткам в размере 19,1 млрд долларов.

Lloyd's of London, страховой рынок, также оценил стоимость крупномасштабной кибератаки. Недавно было подсчитано, что одна атака на азиатские порты, в ходе которой компьютерный вирус зашифровал данные о грузах, может привести к экономическому ущербу в размере 110 миллиардов долларов — что эквивалентно половине глобальных потерь от стихийных бедствий в 2018 году — и только 8 процентов будет покрыто страховыми полисами.

“Все признают, что это огромная область роста для страховой отрасли”, - говорит г-жа Боле. “Все больше и больше предприятий будут стремиться к передаче рисков”.

---

[Авторские права](#) на Financial Times Limited 2023. Все права защищены.

---