Сбербанк, в рамках своей стратегии развития превращающийся в диверсифицированную IT-компанию, занялся страхованием от кибератак и аудитом информационной безопасности небанковского сектора. Как сообщил старший вице-президент Сбербанка Анатолий Попов на выставке Metro Expo, Сбербанк в марте запустил продажи продукта страхования от киберугроз для своих клиентов, включая малый бизнес, а с мая намерен предоставлять услуги по аудиту информационной безопасности небанковским предприятиям и организациям (интернет-магазинам, телекоммуникационным компаниям и прочим фирмам, работающим с большими массивами клиентских данных; частным клиникам, хранящим персональные и конфиденциальные данные по пациентам; компаниям, проводящим платежи в Интернете и т. д.).

В России на эти услуги есть определенный спрос, обусловленный, в частности, стремительным переходом компаний на работу и предоставление услуг онлайн и, как следствие, активизацией киберпреступников и повышенным вниманием к вопросам информационной безопасности в медиапространстве в последние годы; оба сегмента перспективны, рассказывают опрошенные Банки.ру участники страхового рынка и рынка аудита. Причем если на рынке аудита информационной безопасности Сбербанку предстоит столкнуться как минимум с десятком устойчивых игроков, включая «большую четверку», то в сфере IT-страхования у него почти нет конкурентов.

Ставка на страхование

По данным ФСБ, мировой ущерб от хакерских атак, совершенных за последние годы, составляет от 300 млрд до 1 трлн долларов, или от 0,4% до 1,5% мирового ВВП, «и эти показатели имеют тенденцию к неуклонному росту». По данным «Лаборатории Касперского», в 2016 году 42% российских компаний хотя бы раз за год теряли важную информацию из-за взломов или утечек, еще в трети это происходило неоднократно. На ликвидацию последствий одного инцидента, связанного с нарушением информационной безопасности, крупные компании тратят 11 млн рублей, а средний и малый бизнес — 1,6 млн рублей.

Но в отличие от, например, США, где, по данным PwC, страховки от киберугроз купили уже треть местных компаний, в России спрос на эту услугу остается невысоким. Многие организации по-прежнему не считают нужным покупать страховку, так как недооценивают степень риска киберугроз и не видят в них прямого влияния на основную деятельность, сходятся во мнении опрошенные Банки.ру эксперты. «Все зависит от того, как люди относятся к риску и услугам страховых компаний, каков уровень доверия к страховщикам, — объясняет директор услуг по анализу и контролю рисков аудиторской компании PwC Виктор Морозов. — В российской действительности нет привычки страховать всевозможные риски, в том числе риски нарушения информационной безопасности».

Следствие отсутствия спроса — скромный выбор предложения, неразвитость рынка. «С

информационными рисками работает только несколько страховщиков, в основном «дочки» глобальных страховых компаний. Это очень специфичные риски. Продуктов на рынке и страховых компаний, работающих с ними, не так много, хотя рынок интересный и перспективный», — считает руководитель управления имущественных видов страхования Северо-Западного дивизиона «Ренессанс страхование» Виталий Овсянников. Как следует из данных на сайтах крупнейших в России страховщиков, включая «Росгосстрах», «Ингосстрах», «ВТБ Страхование», «СОГАЗ», «РЕСО-Гарантию», «Согласие», «АльфаСтрахование», они не предоставляют услугу страхования от киберугроз, по крайней мере в массовом порядке. На момент публикации материала указанные компании не ответили на запрос Банки.ру.

По мнению собеседника Банки.ру на аудиторском рынке, в текущих условиях у Сбербанка есть все шансы стать лидером сегмента IT-страхования. «Возможно, если страхование от киберугроз будет закреплено законодательно, либо если рынок поймет, что это выгодно, полезно, что это помогает решению каких-то проблем и задач, или же если покупка страховки будет условием какого-либо договора, то, конечно, рынок создастся, а в противном случае — зачем?» — рассуждает он. Так или иначе Сбербанк, по его мнению, сможет поспособствовать развитию этого рынка. «Во-первых, Сбербанк — первый из банков, кто владеет страховой компанией, причем активно развивающейся. Во-вторых, у него есть мощное технологическое подразделение — «Сбертех». Это дает Сбербанку большие технологические возможности. Ни у одной независимой страховой или аудиторской компании подразделения такого уровня нет», — говорит собеседник Банки.ру.

Ставка на аудит

В отличие от рынка страхования, рынок аудита информационной безопасности более развит — спрос на оценку соответствия различным стандартам безопасности и на оценку фактической защищенности информационных систем выше, чем на страховку, причем он постепенно растет, говорят собеседники Банки.ру. Так, в 2016 году количество запросов в международную IT-компанию Group-IB (один из лидеров отрасли) на проведение оценки фактической защищенности выросло вдвое. Число аналогичных заявок в аудиторскую компанию «КСК» от среднего и малого бизнеса увеличилось на 32%. «Это связано с повышенным вниманием СМИ к вопросам кибербезопасности: «русские хакеры», которые помогли Трампу стать президентом, запуск в действие законов «пакета Яровой», DDoS-атаки. Все эти вопросы заставляют всерьез задуматься о защите бизнеса и коммерческой тайны организаций», — объясняет руководитель практики «IT-безопасность» «КСК групп» Алексей Работягов.

Рынок довольно узкоспециализированный — в открытом доступе нет рейтингов крупнейших игроков. По словам собеседника Банки.ру из международной компании, предоставляющей услуги IT-аудита, лидерами отрасли можно назвать как минимум десять компаний, включая Group-IB, Positive Technologies, «Лабораторию Касперского», Digital Securities, компании «большой четверки» (PwC, KPMG, E&Y и Deloitte). По словам руководителя направления «аудит и консалтинг» Group-IB Андрея Брызгина, в целом на рынке работает много компаний, так как, по его словам, рынок оценки фактической защищенности информационных систем «не особо зарегулирован».

Сбербанк обладает богатым опытом участия в противодействии инцидентам в информационной безопасности, но, выходя на небанковский рынок, он может столкнуться с «резонными возражениями» со стороны потенциальных клиентов,

предполагает топ-менеджер международной IT-компании, предоставляющей услуги IT-аудита. «Например, промышленная компания может задаться вопросом: вы знаете о банках, а о нас вы что знаете? Как вы можете проводить аудит промышленного предприятия? Подход к оценке информационной безопасности компаний схож, но на клиентском рынке определенные вопросы об экспертизе так или иначе появятся. Порог входа в промышленность достаточно высокий — компания должна уверить, что обладает необходимой экспертизой», — рассуждает он.

Привести данные оборота российского рынка аудита фактической защищенности собеседники Банки.ру отказались. По мере развития информационных технологий и перехода компаний на работу и предоставление услуг в режиме онлайн рынок аудита информационной безопасности будет расти, причем «сегмент оценки фактической защищенности будет обгонять по темпам роста комплаенс (внутренний контроль. — Прим. Банки.ру)», считает Брызгин.

Российский рынок аудита кибербезопасности с высокой вероятностью будет постепенно приближаться к рынку Европы и Северной Америки, что прежде всего выражается в повышении заинтересованности в оценке киберрисков со стороны руководства компаний, эволюции восприятия аудита кибербезопасности в качестве услуги для IT к ее восприятию как услуги для бизнеса, говорит руководитель направления по управлению Cyber-рисками «Делойт» (СНГ) Денис Липов. «В результате фокус сместится с малоэффективных попыток тотальной защиты всей IT-инфраструктуры на защиту критически важных для деятельности информационных активов, определенных исходя из потребностей бизнеса, а также на непрерывный мониторинг внешних и внутренних киберугроз», — считает он.

Источник:Банки.ру, 05.05.2017