Исследование Allianz показало, что киберриски вышли за пределы угроз конфиденциальности и репутации.

Бизнес должен быть подготовлен к новому поколению киберрисков, которые очень быстро развиваются и уже выходят за пределы традиционных угроз утечки данных, соблюдению конфиденциальности, репутационного урона и могут привести к операционному ущербу, перерыву в производстве и даже потенциально катастрофическим убыткам.

В новом исследовании «Гид по киберрискам: Управление влиянием возрастающей взаимосвязанности» Allianz Global Corporate & Specialty (AGCS) изучает последние тенденции в сфере киберрисков и возникающие угрозы во всем мире.

Киберриски представляют собой важнейшую и быстрорастущую угрозу для бизнеса: киберпреступления обходятся мировой экономике приблизительно в 445 млрд долларов в год. При этом половина этой суммы приходится на 10 крупнейших экономик мира.

«Не далее как 15 лет назад кибератаки находились еще в зачаточном состоянии и ассоциировались только с хакерами, но с ростом взаимосвязанности, глобализации и коммерциализации мы наблюдаем взрыв киберпреступности как в плане частоты наступления, так и серьезности случаев, – говорит Крис Фишер Хирс, генеральный директор AGCS. – Страхование киберрисков не является заменой надежной IT-безопасности, но создает вторую линию защиты для снижения количества киберпреступлений. AGCS видит возросшую потребность в таких услугах, и мы ответственно подходим к нашей работе с клиентами, чтобы лучше понимать ситуацию и реагировать на растущую подверженность среды киберрискам».

Более жесткий режим регулирования и новые киберугрозы

Растущая осведомленность о киберугрозах, а также законодательные изменения обеспечат бурный рост киберстрахования в будущем. При текущем показателе – менее 10% компаний, приобретающих полисы страхования от киберрисков, AGCS прогнозирует рост премий по киберстрахованию с 2 млрд долларов в год сегодня до более 20 млрд долларов в следующее десятилетие, с комплексным годовым коэффициентом роста свыше 20%.

«Рост востребованности киберстрахования в США уже находится в активной стадии, так как законы о защите данных позволяют сориентировать компании, а регуляторные изменения и возрастающие уровни ответственности обеспечивают ускоренный рост в остальных странах, – комментирует Найджел Пирсон, ответственный за киберстрахование в AGCS. – Мы наблюдаем общую тенденцию установления более строгих режимов регулирования защиты данных, сопряженных с угрозой серьезных штрафов в случае утечки информации». Гонконг, Сингапур и Австралия – среди стран, которые рассматривают или уже внедрили новые законы. ЕС намерен утвердить панъевропейские правила защиты данных. Следует ожидать появления более жестких нормативов в каждой отдельно взятой стране.

Ранее внимание в основном было сфокусировано на угрозе утечки корпоративной информации и вопросах соблюдения конфиденциальности, однако новое поколение киберрисков – более комплексное: будущие угрозы будут исходить из кражи интеллектуальной собственности, кибершантажа и перерывов в производстве, вызванных кибератаками или операционными/техническими неисправностями; данные риски обычно недооцениваются. «Осведомленность о рисках перерыва в производстве и киберстраховании возрастает. В течение последующих 5–10 лет перерыв в производстве будет рассматриваться как ключевой риск и важнейший элемент страховой среды», – комментирует Георгий Пачов, эксперт по киберстрахованию международной группы андеррайтеров AGCS. Применительно к кибер- и IT-угрозам покрытие от риска перерыва в производстве может быть очень широким и включать защиту бизнес IT-систем, а также систем индустриального контроля (автоматизированные системы управления, АСУ), используемых энергетическими компаниями, или защиту роботов, используемых на производстве.

Взаимосвязанность порождает риски

Увеличивающаяся взаимосвязанность каждодневно используемых электронных устройств и растущая зависимость от технологий и получения данных в реальном времени на личном и корпоративном уровнях, известные, как «Интернет вещей»,

создают новые уязвимые места. По некоторым оценкам, к 2020 году триллион электронных устройств будут соединены, в то время как, по прогнозам, не более 50 млрд устройств будут способны обмениваться данными на ежедневной основе. АСУ – это другая область, вызывающая тревогу, т.к. определенное количество систем, используемых сегодня, были разработаны до того, как кибербезопасность стала серьезной проблемой. Атака на АСУ может привести к физическому ущербу, такому как пожар или взрыв, а также к перерыву в производстве.

Катастрофические события

Пока имели место только несколько весьма серьезных случаев утечки данных, однако перспектива катастрофических убытков становится все более вероятной, при этом трудно предсказать, как именно это будет выглядеть. Сценарии включают в себя успешную атаку на базовую инфрастуктуру Интернета, масштабную утечку данных или выход из строя провайдера облачных услуг. При этом массивная кибератака, затрагивающая энергетическую или коммунальную компании, может привести к серьезному выходу из строя услуг, физическому ущербу и даже гибели людей в будущем.

Отдельное покрытие

Allianz также прогнозирует, что объем киберстрахования должен развиваться, чтобы страховщики имели возможность предоставлять более широкую и глубокую защиту, охватывая перерывы в производстве и сокращая разрыв между традиционным покрытием и полисами киберстрахования. В то время как исключения киберрисков в традиционных полисах страхования имущества и ответственности, по-видимому, становятся общим местом, отдельно взятое киберстрахование будет развиваться дальше как основной источник комплексной защиты. Наблюдается растущий интерес со стороны телекоммуникационного, ретейлового, энергетического, коммунального и транспортного секторов, а также финансовых институтов.

Уровень образования – как в части понимания представителями бизнеса возможных рисков, так и знаний андеррайтеров, должен повышаться, если страховщики смогут ответить на возрастающий спрос. Кроме того, как с любым другим новым риском, страховые компании также сталкиваются с трудностями в связи с ценообразованием, непроверенными формулировками в полисах и аккумуляцией рисков.

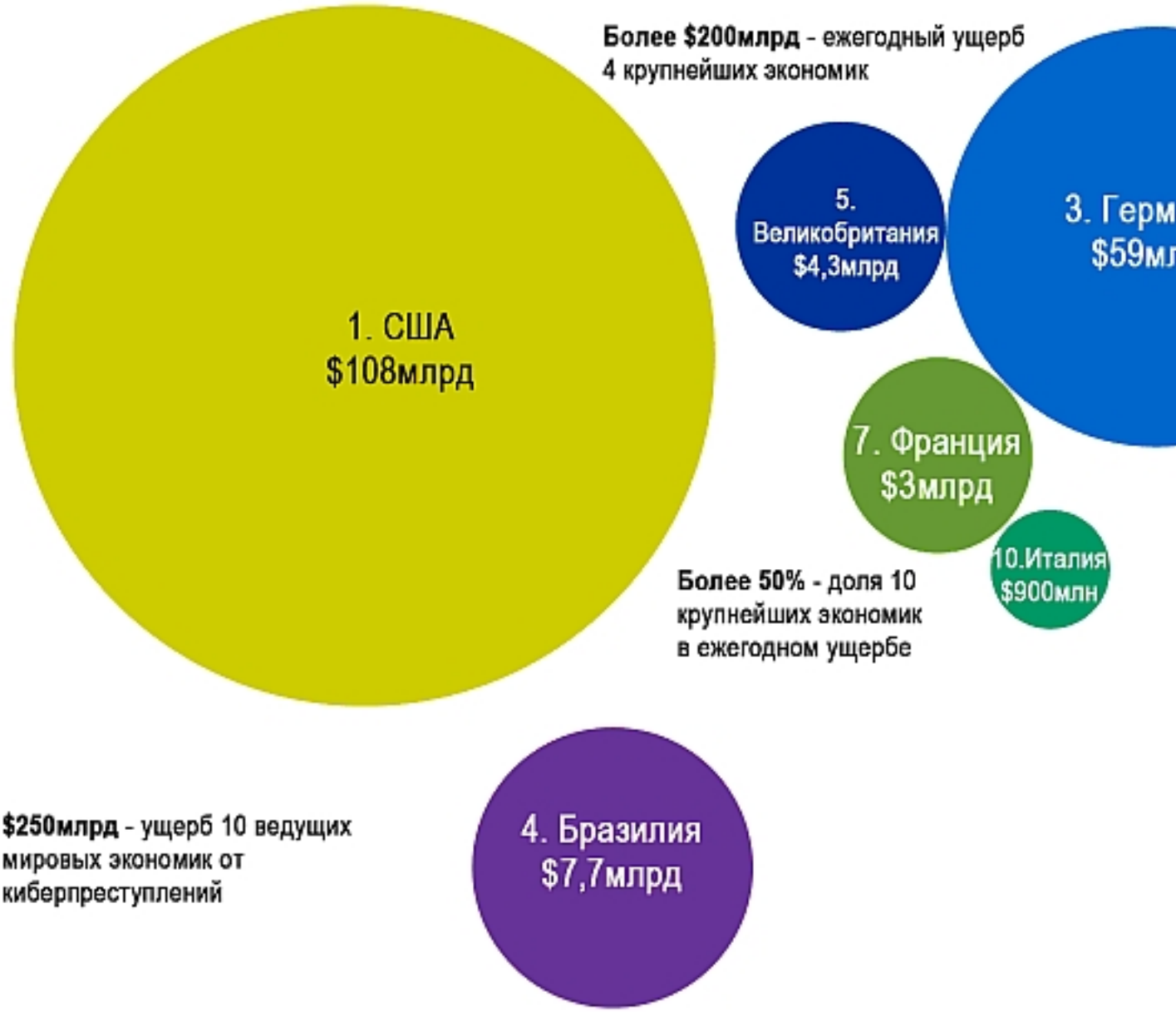
Реагирование на киберриски

В исследовании AGCS говорится о шагах, которые должна предпринимать компания в отношении киберрисков. Страхование может быть лишь частью решения совместно с комплексным управлением рисками, которое является основой для киберзащиты. «Если вы приобрели полис страхования от киберрисков, это еще не означает, что вы можете игнорировать IT-безопасность. Технологический, операционный и страховой аспекты идут рука об руку, – поясняет Йенс Крикхан, эксперт по киберрискам AGCS в Центральной и Восточной Европе. – Управление киберрисками – слишком комплексный процесс, чтобы быть прерогативой какого-то одного сотрудника или департамента, поэтому AGCS рекомендует привлекать разные заинтересованные стороны бизнеса для обмена опытом и знаниями».

В этой связи должны разрабатываться разные альтернативные сценарии развития событий. Например, риски, вызванные изменениями в компании, как то сделки слияния/поглощения, или же связанные с использованием «облачных» или внешних служб. К тому же такое вовлечение разных подразделений компаний очень важно для выявления основных активов, подверженных риску, и, что наиболее значительно, для разработки и тестирования тщательно проработанных планов кризисного реагирования.

Ущерб 10 ведущих экономик мира от киберпреступле

В графике AGCS представлена общая оценка ущерба мировой эконом
нем за год, с детализацией по по 10 крупнейшим экономикам мира по



Рэнкинг стран по размеру ВВП[1]		Киберпреступле-ния, доля к ВВП[2]	Оценочный ущерб[3]
1	США	$16,8 трлн	,64%	$108млрд

Информация предоставлена компанией Википедия страхования, 15.09.15