**ЭПИГРАФ И ВСТУПЛЕНИЕ номер 1**

«- Дядя Георгий, а что ж, мой папа – вор?

– В старинном смысле этого слова – может, и нет.

Но он украл у нас самое дорогое.

Наше свободное время. Наше вдохновение.

Радость творчества. Это – хуже, чем украсть деньги.

Это называется – компьютерное преступление».

Написал статью про компьютерные преступления: общие убытки по миру + расходы по урегулированию последствий + неполученные доходы по некоторым оценкам достигли 450 миллиардов долл. в 2014.

И тут - жизненная ситуация. Создавала Ассоциация сайт. Записала его на частное лицо, он заплатил деньги за создание сайта. Ассоциация стала привлекать к сайту внимание: двое-трое самых активных стали постить заметки и фото. НЕ формальный создатель - владелец. Ему два года подряд говорили: перепиши сайт на Ассоциацию. Нет.

Собрался "создатель" из Ассоциации выйти. Авторы 95% статей, постов и фотографий говорят ему - "сайт отдай"! Ни в какую.

Пришлось авторам с болью в сердце - они же модераторы - с сайта все стирать. Около 500 постов. На каждый полчаса свободного времени потрачено - 250 часов. За три года - каждый пятый день, по часу. Все стёрто.

Вот и что делать? Называть почтенного отца семейства обычным вором? А что он украл-то, сайт на него записан?

А украл он - радость от того, что делишься с другими впечатлениями и видами. Вдохновение. Чувство гордости от того, что помогаешь людям, экономишь их время.

Да, и ведь украл он просто наше свободное время. Можно было побольше с детьми, с семьями побыть.

Но ведь думалось - "работаем на общее дело"! Чтобы всем было интересно.

И вот интересно: это компьютерное преступление или нет? Как исчислить убытки от него? Входит ли оно в эти 450 миллиардов?

**ЭПИГРАФ И ВСТУПЛЕНИЕ номер 2**

Году в двухтысячном, клянусь я вам, ребята,

Все будут жить прекрасно и богато

И человек, идя под вольтовой дугой

Нести в кармане будет слиток золотой.

Тогда появятся на свет электроворы,

Судить их будут электропрокуроры,

Ловить их будут электромусора,

Кормить их будут электроповара.

Туристские песни, сборник 1959 г.

**ЭЛЕКТРОВОРЫ и ЭЛЕКТРОПРОКУРОРЫ**

Почти все, о чем мечтали туристы в 1959м году, сбылось. Есть электроворы. Есть и прочие – те, кто во второй строфе. Вот только не каждый “несет в кармане слиток золотой”. Этого нет, врать нашим предкам не буду.

Ну что, поговорим о Кибернетической Преступности и ее страховании? И надо (ли?) начинать с цифр про миллионы, украденные у банков и страховщиков?

**Да ведь знаете же все примеры?**

- Отели – Mandarin Oriental, Hilton Group (по богатым бьют) – украдены данные по кредитным карточкам – theft of credit card data.

- Загадочный и всемогущий Биткойн – подвергся Distributed denial of service (DDoS) – атаке, прерывающей оказание услуг по интернету.

- Ransomware – программа кодирует базу данных компаний, ключ к раскодированию выдается за выкуп – ransom.

- Data breach – получение доступа к базе данных – обошлось компании Talk Talk в 35 млн. фунтов.

- APT = Advanced persistent threats = развитые постоянные угрозы – постепенное проникновение в IT систему. Две ОПГ, объединенные под именем Carnabak, смогли «заработать» на APT – cочетая их с кражами из банкоматов – 1 миллиард долларов. Только в 2015м. В основном из российских банков, считает Касперский.

- Dyre group облегчил крупнейшего лоукостера Европы – Ryanair – на 5.5 млн. долл.

- Brute-force attacks – хоть и устарелый, но все еще действующий вид преступлений: подбор сочетания имени и пароля (username & password).

- sophisticated spam, spear-phising, malvertising: Вас просят дать свои данные. Убедительно просят – вроде как, от Вашего банка или страховой. Identity Theft – кража персональных данных, это называется.

- Advance fee fraud – мошеничество с авансовым платежами. Вам предлагается заработать 10,000 – вложив 500. Знакомо же, правда?

Я перечислил апельсины с помидорами – примеры видов кибератак и названия громких случаев. Как к ним относятся? Кто-то называет их the greatest transfer of wealth in human history = самая большая передача (да скажите уж прямо, «кража») богатства в истории человечества. А другие отмахиваются – “a rounding error in a fourteen trillion dollar economy” = просто погрешность, или округление – в индустрии, насчитывающей 14 триллионов (!) долларов (Интернет имеется в виду).

**Так сколько же денег уносится?**

Компания Mcafee (mcafee.com) перечисляет составные части Злоумышленных компьютерных действий = Malicious cyber activity:

- Утеря интеллектуальной собственности и конфиденциальных данных,

- Компьютерные преступления,

- Утрата чувствительной бизнес-информации, например, манипулирование рынками,

- неполученные доходы = opportunity costs, включая утрату доверия к интернетным продуктам,

- дополнительные траты на обеспечение безопасности сетей, страхование (!) и восстановление систем,

- утрата репутации компании, подвергшейся нападению (the hacked company).

Оценка Макафи – в 2011м - **400 миллиардов долларов по всем 6 направлениям**. Много или мало?

Интересно, по некоторым оценкам, оборот **наркоторговли** в том же 2011м составил **600 миллиардов долларов**. Сравнимо с компьютерными преступлениями и убытками? Только наркодельцы глотают свои субстанции, а компьютерные преступники сидят в чистых офисах или пыльных кухнях…

**ВВП всего мира в 2014м году составил 78 триллионов** долларов.

Тогда, 400 миллиардов – это немного?

Но ведь вся страховая индустрия – **меньше 5 триллионов долларов в 2014.**

Это что же, если страховать компьютерные преступления и прочие убытки – на них уйдет под **10 % доходов** всех страховщиков мира?

**И что, ничего не страхуется?**

**В связи с Кибер-исключениями?**

Поэтому, пока – страхуют мало.

Почти в каждом полисе есть Кибер-исключения. И они иногда очень широки. Ну вот, к примеру, даже перевод приводить не буду, все ясно:

**Cyber Clause**

The coverage given by this Policy does not apply to, and specifically excludes losses of any kind directly or indirectly caused by, arising from, or consisting of, in whole or in part :

a) the use or misuse of the Internet or similar facility ;

b) any electronic transmission of data or other information ;

c) any computer virus or similar problem ;

d) the use or misuse of any Internet address, Website or similar facility ;

e) any data or other information posted on a Website or similar facility ;

f) any loss or data damage to any computer system, including but not limited to hardware or software….;

g) the functioning or malfunctioning of the Internet or similar facility, or of any Internet address, Website or similar facility …; or

h) any infringement, whether intentional or unintentional, of any intellectual property rights (including but not limited to trademark, copyright or patent).

То есть – не отвечают страховщики за: неправильное использование Интернета или похожей услуги (это кто там еще похож на Интернет?), электронной передачи данных, компьютерные вирусы, неправильное использование интернетных адресов или сайтов, информации, нарушения прав интеллектуальной собственности и прочая и прочая.

Или вот, первая часть (из двух) короткой специализированной оговорки **Institute Cyber Attack Exclusion clause – Институтской Оговорки об исключении кибернетических атак, номер 380** от 10/11/03:

Subject only to clause 1.2 below (военные риски), in no case shall this insurance cover loss damage liability or expense directly or indirectly caused by or contributed to by or arising **from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system.**

Не покрывается “использование или оперирование, в целях причинения вреда, любого компьютера, компьютерной системы, программ, кодов, вирусов или процессов….”

**Страхование Кибер-рисков**

Еще одна оценка: в 2014 “интернет-проблемы” 6 видов обходились уже в 445 миллиардов долларов.

А страхование – есть! По оценкам, к 2025му году его оборот достигнет 20 миллиардов долларов.

Ого! Больше, чем теперешний сбор страховой премии во всей России.

Ну да. Но меньше, чем 5 % от объема убытков. К тому же, речь о 2025м – через 10 лет.

**В США**

Там – да, много компаний страхуется. Считается, в 2014м году страховалось 33 % компаний. Больше всего – конечно же, в секторе финансовых услуг - до 82 % компаний. Средний лимит полиса у них был немаленький – 23.5 миллиона долларов.

**А сколько это стоит?**

**Вечный вопрос: сколько стоит страхование?**

Ну примееееерно. Спрашивает меня потенциальный страхователь или мой коллега – брокер.

Я всегда отвечаю – “от доллара до ста тысяч”. И среднюю цифру тут не назовешь.

Очень порадовался, найдя подтверждение моим словам на сайте страхового брокера Дата Брич. Посмотрите – лимиты и стоимость Кибернетического страхования по разным компаниям. Я решил рассчитать ставку – в проценте от оборота и в проценте от лимита. Вот что получилось: вид компании / брутто-доход / лимит полиса / премия (все в доллара) / ставка от оборота и от лимита.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **in USD** | **Revenue** | **Limit** | **Premium** | **%of Revn.** | **% of Limit** |
| IT Solutions Integrator | 20,000,000 | 5,000,000 | 41,500 | 0.2075% | 0.8300% |
| Healthcare IT Provider | 4,500,000 | 5,000,000 | 34,600 | 0.7689% | 0.6920% |
| Healthcare Clinic | 400,000 | 1,000,000 | 1,202 | 0.3005% | 0.1202% |
| Call Center | 20,000,000 | 5,000,000 | 19,800 | 0.0990% | 0.3960% |
| Fiber Optics Communications Provider | 35,000,000 | 10,000,000 | 47,000 | 0.1343% | 0.4700% |
| Industry: E-commerce | 50,000,000 | 1,000,000 | 37,000 | 0.0740% | 3.7000% |
| Restaurant | 35,000,000 | 1,000,000 | 10,000 | 0.0286% | 1.0000% |
| Psychologist’s Office | 1,000,000 | 1,000,000 | 649 | 0.0649% | 0.0649% |
| Online Retailer | 500,000 | 1,000,000 | 1,100 | 0.2200% | 0.1100% |
| Data Storage Center | 15,000,000 | 20,000,000 | 120,000 | 0.8000% | 0.6000% |

**Нет средней ставки!**

Вот подтверждение моим словам: НЕТ средних цифр! Средних премий!

От оборота – варьируется от 0.03 % (!) до 0.8 %. В ДВАДЦАТЬ ШЕСТЬ раз!

От лимита – от 0.07 % до 3.7 %. Вообще в ПЯТЬДЕСЯТ раз.

Так что всегда и везде – НЕ спрашивайте, по ком звонит колокол. Равным образом – **сколько стоит страхование**. Для каждой компании - разная цифра.

**От оборота**

Ух, как у нас часто обижаются – “это я Вам, да объем своего оборота / брутто-дохода скажу?! Да налоговики годами хотят это узнать!”

Ну, что делать. Налоговикам – не говорите. Нам, страховщикам – можно. И нужно. Вот подумайте – даже когда мы страхуем огромный завод, стоящий сотни миллионов или миллиарды – мы ставим премию в проценте от страховой суммы. По имуществу – от пожара, наводнения.

А как застраховать Малый и Средний Бизнес = МСБ = SME – у которого порой все имущество – два стола, три компьютера и два айПэда? На чем основываться?

Но – и при страховании больших заводов, как только речь заходит об ответственности перед третьими лицами, о перерыве в производстве = потере прибыли – ставка идет НЕ от стоимости имущества. От ОБОРОТА. Во всем мире.

Так что не волнуйтесь, у нас – как за каменной стеной. Вот ведь и в таблице выше – Вы ж не увидели названий компаний?

**Где страхуем?**

Тот же специализированный брокер – увы, американский, мы УЖЕ спросили, он про Восточную Европу ничего не знает и работать тут не хочет – тот же брокер задает себе и Вам вопрос: «как выбрать правильного страховщика и брокера?»

(1) полис, который Вам продают – составлен ли он **с учетом Ваших потребностей** в покрытии кибернетических рисков и рисков утери данных (cyber and data risks)?

(2) **какие убытки** (what types of breaches – «нарушения») этот полис покрывает?

(3) **что исключено**?

(4) оказывает ли брокер или страховщиков **физическую помощь** по восстановлению базы данных?

**Сервис**

Это – очень интересный вопрос, четвертый. От страховщиков – и брокеров – все больше ждут СЕРВИСА. Не только возмещения убытков – помощи. Мы то, в Оукшотте, знаем – уж 23 года как работаем 24/7/365 (как я всегда сам говорю после этого высказывания – 0.94 %, ну и что?) – работаем все время.

А в киберстраховании – еще важнее, чтобы страховщик был рядом в трудную минуту.

**А что надо страховать? Мнение из России**

Вот пишет нам один из лучших страховщиков России. Видите, **как глубоко копают!**

QUOTE

Для подготовки предварительных предложений клиентам, просьба **уточнить ряд моментов**, касающихся возможного покрытия и исключений.

Ниже перечислены **примеры возможных убытков потенциальных Страхователей** и вопросы, которые просим прокомментировать:

1.**Расходы Страхователя, на консультации** и иные услуги специалистов программно-технической экспертизы, **на  экспертов по оценке восстановления данны**х и т.д. включатся в покрытие. если понесены расходы как оплата **услуг сторонних организаций.**

Если Страхователь привлечет **дочернюю компанию** для восстановления программного обеспечения, такие расходы попадают в покрытие? Аналогично, например, у Компании может быть специализированная **дочерняя компания,** которая в случае кибер-атаки будет привлечена для **консультационных услуг/восстановления данных** и т.п. **Оплата услуг дочерней компании** Страхователя попадает в покрытие?

2.Убытки по причине **несанкционированного раскрытия …** (или передачи персональных данных, в том числе заражения вирусами, уничтожения, модификации или удаления информации, физической кражи или утери аппаратного обеспечения) – что может быть включено в покрытие?

Примеры:

А) в результате **хакерской атаки раскрыты** **персональные данные** сотрудника/физического лица. Он подает **претензию: либо непосредственно Страхователю** (попадает в покрытие?) либо в суд (по решению суда заплатим? Это может быть и моральный вред, и некие расходы/упущенная выгода физ.лица).

Б) в результате хакерской атаки **обнародованы бизнес-планы Страхователя по приобретению какого-либо актива**, в результате чего сделка сорвалась. **Упущенная прибыль** входит в покрытие?

В) в результате хакерской атаки произошел **сбой поставок например, электричества/отопления** и т.д.

Как следствие, может быть **имущественный ущерб** (например, взрыв, пожар, прорыв). Исключение в данном покрытии?

В ряд районов не подали газ - ущерб имуществу третьих лиц. В исключениях? Если сам Страхователь вынужден произвести какие-то расходы – предположим, **закупить газ у сторонней организации** и исполнить тем самым свои обязательства, такие расходы попадают в покрытие?

3. Возможно ли предусмотреть в одном Договоре страхования покрытие как **для Страхователя, так и для дочерних обществ?**

4.В презентациях Западных компаний по защите кибер-рисков есть покрытие **BI** (потери прибыли) **- лимит ответственности доходит до 100 млн.евро.**

Кто сможет поддержать нас в перестраховании с покрытием, включающем эту опцию при необходимости покрытия **с большим лимитом?** И какие есть ограничения в покрытии, временная франшиза и т.д.?

**Не факультативно**

Очень не хочется отказывать в запросах. С этим мы еще поработаем – тут же – портфель целый.

А другой у нас запрос на этой неделе…но сначала пройдемся по **Вопроснику = Proposal Form.**

1. Your business – 2. Claims and incidents – 3. Declaration. Посмотрим на третью позицию, мы же только что изучали **Закон о Страховании 2015** года и о частичном снятии со страхователей ответственности за несообщение всей информации.

Что мы видим? Фразу:

I/We understand that non-disclosure or misrepresentation of a material fact or matter will entitle The Underwriters to avoid this insurance = Я/Мы понимаем, что несообщение или искажение существенного факта или обстоятельств даст Страховщикам право расторгнуть этот договор страхования.

А теперь – что хотят знать страховщики об объекте Кибернетического страхования? C одной стороны, скучновато все это переписывать и переводить. Но если об этом не знать – как мы с Вами организуем- в ближайшем будущем – страхование и перестрахование Кибернетических рисков?

Поехали.

**Your business / Ваша компания**. Мы уже понимаем, что важно: адрес – адрес сайта – год создания – количество работников **– Брутто-доход = Total Gross Revenue, в том числе в США** – и в остальных странах. Доход – в прошлом году, в текущем и оценка на будущий.

Наш запрос – из Африки. Gambling business – интернетные азартные игры. Страховщики сразу же спрашивают: у вас работают 170 человек, а доход в прошлом году только 200,000 фунтов. Маловато-что-то?

А теперь – технические вопросы, связанные с кибер-рисками.

|  |  |
| --- | --- |
| **DATA PROTECTION PROCEDURES** | **СИСТЕМА ОБРАБОТКИ ДАННЫХ** |
| Is there a written data protection policy and privacy policy that applies to the company? | Имеется ли в компании письменная Политика (Система) защиты данных и политика сохранения конфиденциальности? |
| Are all employees provided with a copy and any update of the company’s data protection policy which they are required to confirm compliance with? | Имеется ли у всех сотрудников, которые должны ею руководствоваться, распечатанная Политика защиты данных и изменений к ней? |
| When was the company’s data protection policy last reviewed and by whom? | Когда эта Политика последний раз пересматривалась и кем? |
| Does the company’s data protection policy comply with the data protection and privacy legislation applicable to all jurisdictions and industry standards/requirements, in which the company operates? | Соответствует ли указаннная Политика законодательству по защите информации и конфиденциальности, действующему во всех юрисдикциях и отраслях, в которых действует компания? |
| Does the company employ a Chief Compliance Officer, Data Protection Officer and/or In-house Counsel responsible for data protection related matters? | Есть ли в Компании Высший руководитель, отвечающий за Защиту информации и связанные с ней вопросы? |
| **DATA ACCESS & RECOVERY** | **ДОСТУП К ИНФОРМАЦИИ И ЕЕ ВОССТАНОВЛЕНИЕ** |
| Does the company use firewalls to prevent unauthorised access connections from external networks and computer systems to internal networks? | Есть ли у компании защитные системы для предотвращения несанкционированного доступа из внешних сетей и компьютерных систем во внутренние? |
| If “Yes” are all computer systems, mobile devices and websites Firewalled or have intrusion prevention systems on them? | При положительном ответе, все ли системы, мобильные устройства и интернет-сайты имеют защитные системы? |
| Does the company use anti-virus protections and procedures on all desktops, e-mail systems and mission critical servers to protect against viruses, worms, spyware and other malware? | Использует ли компания защиту против вирусов и соответствующие процедуры на всех компьютерах, почтовых системах и серверах для защиты от вирусов, программ-шпионов и иных хакерских программ? |
| Does the company have in place procedures to identify and detect network security weaknesses? | Имеются ли в компании процедуры, позволяющие идентифицировать и обнаружить слабые места систем безопасности? |
| Does the company monitor its network and computer systems for breaches of data security? | Контролирует ли компания свои сети и системы на предмет нарушения безопасности информации? |
| Does the company have physical security controls in place to prohibit and detect unauthorised access to their computer system and data centre? | Есть ли у компании система физического контроля, позволяющая избежать и обнаружить несанкционированный доступ к их компьютерной системе и базе данных? |
| Does the company collect, store, maintain or distribute credit card or other sensitive personally identifiable data? | Получает ли компания, хранит, держит или передает данные о кредитных картах или иную персональную информацию? |
| If “Credit Card” is selected above, does the company comply with Payment Card Industry Data Security Standards? | Если “да”, то отвечает ли компания Стандартам безопасности данных Системы платежных карт (PCI DSS)? |
| Does the company process payments on behalf of others, including e-Commerce transactions? | Осуществляет ли компания платежи за третьих лиц, включая электронную торговлю? |
| If “Yes” please provide the number of clients you process such payments for and an estimated number of transactions per client. | Если “да”, приведите число таких клиентов и примерное количество операций по каждому из них. |
| Does the company have encryption requirements for data-in-transit data-at-rest to protect the integrity of sensitive data including data on portable media (e.g., laptops, DVD, backup tapes, disk drives, USB devices, etc.)? | Пользуется ли компания системой криптографической защиты передаваемых и хранимых данных для защиты конфиденциальных данных, включая хранящиеся на переносных носителях (лэптопах, DVD, лентах, дисках, USB устройствах)? |
| Does the company have and maintain backup and recovery procedures for all:  1) mission critical systems?  2) data and information assets? | Имеет ли компания систему копирования / резервирования:  1) всех важнейших систем?  2) информации и  информационных активов? |
| Does the company perform background checks on all employees and independent consultants? | Проверяет ли компания информацию о всех сотрудниках и строронних консультантах? |
| Does the company require remote users to be authenticated before being allowed to connect to internal networks and computer systems? | Работает ли система опознавания удаленных пользователей перед допуском их во внутренние сети и компьютерные системы? |
| **OUTSOURCING ACTIVITIES** | **ПРИВЛЕЧЕНИЕ СТОРОННИХ РЕСУРСОВ (АУТСОРСИНГ)** |
| Does the company outsource any part of its network, computer system or information security functions? | Использует ли компания аутсорсинг для поддержкания сети, компьюетерной системы или информационной безопасности? |
| If “Yes” who is the security outsourced to? And does the company periodically audit the functions of the outsourcer to insure that they follow the company’s security policies? | Если “да”, кто осуществляет аутсорсинг? Проводит ли компания периодический аудит сторонних фирм для того, чтобы убедиться, что они следуют политике безопасности компании? |
| Does the company outsource any data collection and/or data processing? | Делает ли компания аутсорсинг сбора и/или обработки данных? |
| If Yes”, please provide details of the data collection or data processing functions which are outsourced: | Если “да”, пожалуйста предоставьте описание функций по сбору или обработке данных, передающихся в аутсорсинг. |
| Does the company require the entities providing data collection or data processing functions (outsourcers) to maintain their own data protection liability insurance? | Требует ли компания наличия у таких сторонних фирм их собственного страхования ответственности за защиту информации? |
| Does the company require indemnification from outsourcers for any liability attributable to them? | Обращается ли компания за возмещением к сторонним фирмам, если они несут ответственность за какое-либо нарушение безопасности? |
| How does the company select and manage outsourcers? | Как компания отбирает сторонние фирмы и работает с ними? |
| Does the company require all outsourcers to comply with the terms of the company’s data protection policy? | Требует ли компания от всех сторонних фирм, чтобы они следовали политике защиты данных компании? |

Получился длиннющий вопросник, правда? Обратите внимание **на три основные позиции:**

- Системы обработки данных,

- Доступ к информации и

- Аутсорсинг.

И ведь мы взяли вопросник только одной компании – AIG. Посмотрели у другой, у Ллойдовского синдиката – там еще вопросов 10, не включенных выше. Но, наверно, пока хватит – направленность вопросов ясна?

**Что застраховать?**

Итак, что мы с Вами можем застраховать по полису от Кибернетических Преступлений?

**Для начала, как мы его назовем?**

Используются термины cyber risk, information security, data risk, privacy insurance, media liability cover. Стандартной формы для страхование рисков пока не создано.

**Первые и третьи лица**

Разделы? По-американски, first-party and third party coverage: интересы «первых» и третьих лиц. «Первых» - это собственно страхование имущества, а вернее, расходов в связи с этими рисками. Третьих – ответственность перед третьими лицами.

**“Первые” лица – убытки и расходы страхователя**

Возможные застрахованные риски:

- **гибель или повреждение имущества**, компьютерных данных или программ (digital assets: data or software programmes).

- **кража и мошенничество** = theft & fraud, включая кражу денежных средств и информации,

- **расходы по расследованию** = forensic investigation –по расследованию причины потери информации,

- **перерыв в производстве** = network / business interruption – потери дохода и дополнительные расходы по восстановлению сети. Имеется временная франшиза и максимальный период покрытия, как в обычном BI,

- **вымогательство** = (cyber) extortion – выплата выкупа мошенникам, угрожающим раскрыть конфиденциальную информацию,

- **утрата и восстановление информации** = data loss and restoration – не всегда предлагаемый вид покрытия, с достаточно высокой франшизой. Иногда включает не только расходы по восстановлению информации, но и по диагностике и исправлению систем,

- утеря репутации = reputational damage вследствие утраты данных,

- расходы в связи с утечкой данных = **breach costs** – обобщенный термин, включающий большинство из перечисленных позиций?

- убытки **от хакерских атак** = hacker damage.:

**Ответственность перед третьими лицами**

- **Ответственность за раскрытие** конфиденциальной информации = privacy liability coverage – покрываются случаи раскрытия информации вне зависимости от их причин. Встречаются более узкие варианты покрытия – только преднамеренных раскрытий информации = intentional breach,

- действие **регулятивных органов** = regulatory actions. Для нас покрытие таких позиций странно – защита от расследования регулятором. Но если Вам “продадут” такое покрытие – обращайте внимание на то, с какого момента покрываются расходы: когда регулятор направляет первичный запрос – или когда получено официальное предписание. Существенно, что страхуются штрафы и иные денежные санкции,

- расходы **по извещению об утрате** данных = notification costs – извещать порой приходится огромный круг лиц,

- **кризисные расходы** = crisis management – создание рабочей группы по урегулированию последствий утечки информации, включая PR-аспекты, назначение юристов,

- **колл-центры** = call centres – важный момент покрытия, расходы сродни crisis management,

- контроль за **восстановлением конфиденциальной** информации = credit/identity monitoring,

- **распространение вирусов,** троянов и пр. = transmission of viruses / malicious code,

- ответственность в связи **со средствами массовой информации** = media liability – нарушение в мейлах или на сайтах авторских прав, клевета и дифамация,

- защита **конфиденциальной информации** = privacy protection – термин, относящийся ко всем или большинству из перечисленных убытков и расходов.

**Вид полисов – claims made**

Как и во многих видах страхования ответственности, покрытие порой предоставляется на базе **claims-made** – заявленных убытков.

Проблемы могут возникнуть в страховании ответственности, где покрытие начинается **(the cover is triggered)** после начала судебного дела, а не заявления претензии. О каком страховом событии тогда надо извещать страховщиков? Утечке информации или получении иска в связи с утечкой?

**Каких юристов использовать?**

В автомобильном страховании требуется использовать авторизованные мастерские. В кибернетическом – одобренных страховщиком юристов. Надо быть уверенным, насколько широк круг юристов – how wide is the choice of counsel.

**Ретроактивное покрытие – retroactive coverage**

Конечно, оно не работает в полисах claims-made. В полисах на базе даты убытка покрытие может распространяться на случаи, произошедшие ДО начала действия страхования.

**Действия третьих лиц**

Acts or missions of third parties – помните вопросы про аутсорсинг? Ведь небольшие компании часто используют услуги сторонних компаний для ведения своих баз данных. Некоторые кибернетические полисы могут исключать убытки, связанные с действиями или упущениями третьих лиц.

**Отсутствие криптозащиты**

Иногда покрытие не распространяется на информацию,утерянную из незащищенных компьютеров – no coverage for unencrypted devices.

**Место страхового случая**

Иногда покрытие ограничивается офисом страхователя. Это неправильно, ведь location of security failure – место утраты информации – может быть самым различным, если данные теряются вместе с лэптопом или домашним компьютером сотрудника компании.

Также важны географические ограничения – порой исключаются претензии и иски третьих лиц в США и Канаде как «самые дорогие».

**Исключения дефектов в системе**

Часто встречаются exclusions for generalized acts or omissions – например, не покрываются известные страхователю недостатки в системе. Или более общо – непринятие страхователем мер по разработке, поддержанию и обновлению мер безопасности = insured's failure to take reasonable steps to design, maintain and upgrade the secutiy system.

Вот так, коротенько. А можно ли реально эти риски застраховать у нас, в Восточной Европе, или перестраховать в Западной? Приходите к нам в Оукшотт, и мы [wecanhelp@oakinsur.com](mailto:wecanhelp@oakinsur.com)

Георгий Гришин

Май 2016

Использованные ресурсы:

<http://www.computerweekly.com/news/4500260419/Top-10-cyber-crime-stories-of-2015>

<https://securityintelligence.com/2015-cybercrimes-epic-year/>

<http://www.forensicscolleges.com/blog/resources/cybercrime-on-rise-2015>

<http://science.opposingviews.com/examples-cyber-crime-1544.html>

<http://www.mcafee.com/es/resources/reports/rp-economic-impact-cybercrime.pdf>

<https://databreachinsurancequote.com/cyber-insurance/cyber-insurance-data-breach-insurance-premiums/>

<http://www.statista.com/topics/2445/cyber-insurance/>

<http://www.businesswire.com/news/home/20150909005336/en/Generation-Cyber-Risks-Pose-Increasing-Challenges-Businesses>

<http://www.riskandinsurance.com/analyzing-cyber-risk-coverage/>

<https://www.hiscox.co.uk/business-insurance/cyber-and-data-insurance/>

<https://www.hiscox.co.uk/shared-documents/business/13388-cyber-and-data-policy-summary.pdf>

<https://www.abi.org.uk/Insurance-and-savings/Products/Business-insurance/Cyber-risk-insurance>