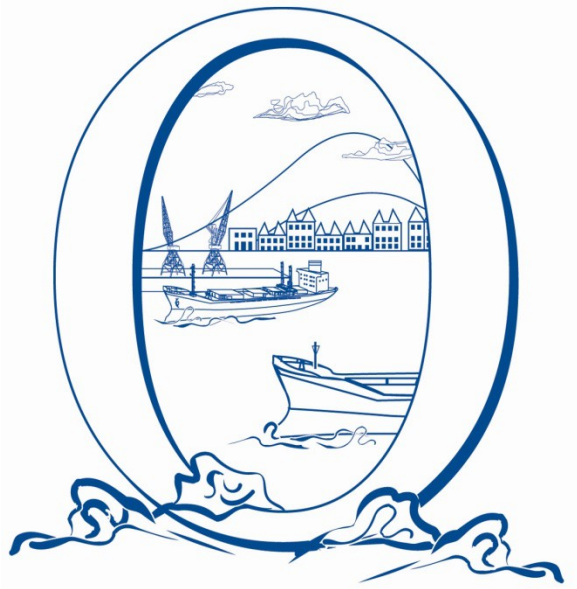

Oakeshott Insurance Consultants Ltd

I n s u r a n c e P r o t e c t i o n o n L a n d & S e a

КИБЕР-РИСКИ:
ЖИЗНЬ В НОВОЙ ЦИФРОВОЙ РЕАЛЬНОСТИ

КИЕВ 2017

Кибер-риски являются угрозой с перспективой дальнейшего роста и влияния на мировоую экономику из-за углубления и распространения цифровой революции (digitisation) в бизнесе и повседневной жизни. В 2016г потери от кибер-атак оцениваются $450 млрд. (*Graham, 2017*). Рынок кибер-страхования оценивается $3-$3.5 млрд. *(Stanley, 2017).* В 2016г рост премий 35%, всего подписано премий $1.35 млрд. *(A.M Best, 2016).*

Ллойд совместно с группой аналитиков проработали несколько сценариев развития кибер-рисков и развития убытков.

Для моделирования были выделены 6 ключевых параметров, которые применили к двум большим группам, сформированным по принципу масштаба последствий кибер-атак.

1. <u>Количество разработчиков</u>:
в 2011 в Linux Kemel участвовали 1 400 чел., 15 млн строк кода.

2. <u>Количество ПО и его сложность</u>:
Apollo 11 использовалось около 145,000 строк кода. Сегодня авто — более 100 млн строк.

3. <u>ПО с открытым доступом:</u>
высокий потенциал уязвимости и неконтролируемое распространение

4. Старое ПО:
чем старее, тем больше уязвимостей выявляются и используются (Wannacry)

5. Многоуровневое ПО:
новые софты имееют приоритетный код, «надстраиваются» над ранее имеющимися программными кодами, сложность в проверке корректности работы программ и их безопасности

6. Генерирующее программирование:
могут модифицировать злоумышленное содержание

Основные сценарии моделирования убытков:

Сценарий 1. Атаки на провайдеров облачных сервисов. Преступные группы "hacktivists" проникают в облачные сервисы, могут обрушить их работу и сервис для пользователей.

Группа делает зловредные модификации к гипервизору (программа управления операционными системами), который управляет облачной инфраструктурой.
Это приводит к «падению» серверов пользователей, ведущее к широкому распространению атаки и BI.

Такой сценарий актуален для различных подгрупп: интернет, облачные сервисы, сервисы доменных имен, платежные процессоры итп

Прямой экономический ущерб для больших и экстремальных убытков - от $4.6 млрд до $53.1 млрд (средний), $121.4 млрд (пессимистический)
Застрахованные убытки — от $620 млн. до $8.1 млрд (13%-17% всех убытков застрахованы)

Исходя из текущей оценки заработанных премий по единичному риску LR отрасли могут вырасти от 19% до 250%. Это иллюстрирует катастрофический потенциал кибер-рисков.

Основные сценарии моделирования убытков:

Сценарий 2. Массовые атаки на уязвимости ПО

Cyber аналитик случайно оставляет в поезде свою сумку с отчетами по уязвимости ОС, имеющие влияние на 45% глобального рынка.
Информация продается на черном рынке неопознаной преступной группе.
Через вредоносный код она атакует уязвимые структуры с целью извлечения финансовой выгоды.

Сценарий актуален для ОС, web-серверы, БД, web-приложения, удаленный доступ итп
(45% мирового рынка страдают от массовых атак, запускаемых через интернет-сайты и соединения, с целью получения финансовой выгоды через уязвимости компьютерных систем и софтов)

Прямой экономический ущерб для больших и экстремальных убытков - от $9.7 млрд до $28.7 млрд
Застрахованные убытки — от $762 млн. до $2.1 млрд (только около 7% всех убытков этой группы застрахованы)

Атаки осуществляются white hat хакерами, киберпреступниками, hacktivists, национальными государствами.

<u>Отсутствие единого стандарта в покрытии:</u>

? Компьютерная система: включает аутсорсинг (облачных провайдеров с базой данных клиента) или только то, что под контролем клиента и в его пользовании;
? Условия: согласно законодательства или добровольные

Общие условия страхования:

- Security and privacy liability включает расходы на защиту, урегулирвание и судебные издержки
- Data breach costs (законодательство по защите персональных данных действует в 47 штатах Америки, ЕС и Австралии): оплата специалиста IT для определения масштаба взлома; юридического советника; письменных уведомлений потенциально пострадавших контрагентов/потребителей; консультанта по связям с общественностью; кредитного мониторнига, мониторинга кражи персональных данных (длительность мониторинга широко варьируется в полисах); услуги call-центра для запросов от потенциально пострадавших потребителей.

- Network business interruption - простои и сбои в работе цифровой среды компании, т. е. необходимые оперативные расходы, дополнительные расходы и потеря прибыли от прерывания работы сети. Временная франшиза 8-12 часов. Разные подходы для временного BI из-за проблем у провайдера (исключается, почасовой сублимит или полное покрытие). BI по причине "системный отказ" или "ошибка администратора" может включаться дополнительно к покрытию от злоумышленных действий извне.
- Regulatory action costs
- Extortion самый популярный вид - вымогательство через зловредные программы, разрушающие компьютер, кодирующие данные (ransomware).

- <u>Digital asset replacement:</u> расходы на восстановление данных. Если бекап не возможен, покрываются расходы на пересохранение, сбор или создание данных, насколько это возможно.

Для TPL полисов может включаться The Information Security Protection Endorsement, BP 15 07 03 15 для рисков: 1) только взлом 2) взлом и ответственность 3) взлом, ответственность, BI, вымогательство.

Terrorism Risk Insurance Act, War как правило исключены.

Эффективная защита — это комплекс действий:

1) технологических компаний с их продуктами, технологиями и экспертизой;

2) компаний-пользователей с продуманными политиками безопасности и обучением сотрудников;

3) государства по образованию и централизованному оперативному информированию, например, в случае с WannaCry - Национальный центр кибербезопасности Великобритании, Petya — Национальная полиция Украины и СБУ

4) самих пользователей - в digital эпоху базовые принципы компьютерной гигиены игнорировать невозможно.

+) страхование для минимизации потерь бизнеса и государственных учреждений.

КИБЕР-АТАКИ НАЦИОНАЛЬНЫХ ГОСУДАРСТВ С ЦЕЛЬЮ ДОСТИЖЕНИЯ ПОЛИТИЧЕСКИХ ЦЕЛЕЙ ИЛИ ШАНТАЖА

(дополнительное вложение)

Майкл Голловей, американский аналитик, "Как Россия превратила соцмедиа в Крыму на оружие" для военного издательства США Realcleardefense: Во время аннексии Крыма, российское правительство потратило более чем 19 млн долларов на финансирование работы 600 человек, которые постоянно комментировали статьи, писали блоги и проводили деятельность в социальных медиа с целью изменить мнение общественности и международного сообщества, перекрыть голоса диссидентов в онлайн медиа, создать впечатление, что население поддерживает аннексию. При этом российские интернет-войска распространили ряд лживых историй, чтобы разделить население.

При этом работа украинских правительственных сайтов в Крыму была заблокирована, на новостные сайты в Крыму осуществлялись нападения, коммуникация ВМС Украины подавлялась - это создало информационный вакуум в регионе и сторонники аннексии быстро завоевали информационное преимущество, что позволило России уменьшить расходы на аннексию полуострова.»

Важно отметить, что аналог этой операции уже был осуществлен Россией в период 20 июля - 14 августа 2008г. Подробно об этом изложено в английской Википедии, статья Cyber attacks during the Russo-Georgian War. Сначала был атакован сайт президент Грузии, который перегружался с фразой “win+love+ Rusia”.

Затем были атакованы СМИ, трубопровод (завуалированная атака на систему контроля и безопасности для увеличения давления, приведшая к взрыву). Атаке подверглись также новостное агентство в Азербайджане, российская газета Scandaly.ru, освещавшие события в Грузии.

Специалисты по кибер-безопасности отмечали организацию ботовых сетей перед вторжением, которые затем были активированы одновременно. В России был создан сайт StopGeorgia, где любой желающий мог поучаствовать в DDoS атаках, при этом велся список правительственных сайтов Грузии, которые уже легли и указывались адреса для атак «еще живых».

Нет прямых доказательств, что атаки выполнялись или санкционировались правительством России, как и нет сведений, что оно пробовало их остановить. Кибер-атаки 2008г стали первым случаем, когда виртуальные атаки совпали с реальными военными действиями.

Эти примеры наглядно демонстрируют серьезность и реальность кибер-угроз для Украины. Конечно, страховщики смогут нивелировать только часть и только экономических потерь.

Кибер-страхование расширяет свои географические пределы и Украина уже может быть вовлечена в этот процесс.

В презентации использованы материалы отчета Lloyd's and Cyence

COUNTING THE COST CYBER EXPOSURE DECODED, 2017

РЕКОМЕНДАЦИИ:

Статья Г.Гришина и презентация LABB по кибер-страхованию

на сайте oakeshott.com.ua

СПАСИБО ЗА ВНИМАНИЕ!

ВСЕГДА РАДЫ ПОМОЧЬ!

WE CAN HELP!