КОМПАНИЈЕ ПРЕПУШТЕНЕ НА МИЛОСТ И НЕМИЛОСТ ИНФОРМАЦИОНИМ ТЕХНОЛОГИЈАМА

COMPANIES AT THE MERCY OF INFORMATION TECHNOLOGIES

Бранко Павловић
Делта Осигурање а.д, Београд

Садржај – *Пословање већине савремених компанија најчешће потпуно зависи од исправног функционисања информатичких ресурса. Проблеми са информационим системом или опремом доводе до прекида рада и великих финансијских губитака. Осигурање пружа једину заштиту од ћуди информационих технологија. У овом раду биће објашњено стање у домаћој пракси у осигурању информационих ресурса и светски трендови.*

Abstract – *Very often the business of the most contemporary companies completely depends on proper functioning of IT. Information system or equipment problems lead to business interruption and great financial loses. Only insurance provides protection from IT caprices. The situation in our IT insurance practice and world trends will be explained in this paper.*

1. УВОД

Информационе технологије се развијају огромном брзином, рачунари постају све бржи и моћнији, а апликације све сложеније. Пословање све већег броја компанија постаје потпуно зависно од исправног функционисања инфораматичких ресурса. Реална опасност од физичких кварова рачунарске опреме, програмерских грешака или намерних саботажа прети да доведе до прекида рада целе компаније и великих финансијских губитака.

Осигурање је привредна, услужна делатност која штити човека и његову имовину од последица бројних опасности (нпр. пожар, удар грома, експлозија, олуја, деловање воде и паре, демонстрације, лом машина, провална крађа). Најважнији циљ осигурања је заштита осигураника и чување његове имовине накнадом штете на уништеним добрима.

Исто као што се осигуравају индустријске машине и опрема, могу се осигурати и информатички ресурси. У пракси је релативно добро развијено осигурање везано за информационе технологије од различитих физичких узрока, утврђивање висине штета и њихова накнада. Наша осигуравајућа пракса, за разлику од светске, не познаје осигурања везана за инф. технологије од нефизичких узрока. Циљ овог рада је да објасни постојећа домаћа осигурања инф. ресурса од физичких узрока и приближи светски тренд у осигурању од нефизичких узрока, с обзиром да ће и код нас у блиској будућности морати да се посвети дужна пажња и овој врсти заштите.

2. ВРСТЕ ОСИГУРАЊА ВЕЗАНИХ ЗА ИНФ. ТЕХНОЛОГИЈЕ У ДОМАЋОЈ ПРАКСИ

Постоје две врсте осигурања од физичких узрока везаних за информационе технологије које се могу срести у домаћој пракси:
-осигурање електронских рачунара и
-осигурање од прекида рада, као допунско осигурање, ако је већ закључено неко основно, нпр. осигурање електронских рачунара.

2.1. ОСИГУРАЊЕ ЕЛ. РАЧУНАРА

Предмет осигурања су електронски рачунари са свом припадајућом опремом и инсталацијама, процесори, персонални рачунари, процесни рачунари за вођење и контролу производње и клима и енергетски уређаји и инсталације. Посебно се може уговорити осигурање вредности носача података (нпр. дискова), вредности података на носачима и трошкова за најам другог рачунара. Нису осигурани делови који брзо троше и хабају, односно често мењају, прибор за погон, одржавање и чишћење, ни трошкови који настају на носачима података због погрешног руковања.

Осигуравајуће покриће обухвата штете настале услед: пожара, удара грома, експлозије, олује, града, деловања воде и паре, пада летилице, манифестација и демонстрација, клизања тла, одроњавања земљишта, снежне лавине, лома машина, провалне крађе и разбојништва. Нису покривене: посредне штете (губитак зараде, прекид рада, итд.), штете које настају у гарантном року за које је одговоран произвођач, ни штете на подацима које настају због немара.

Вредност осигуране ствари је цена нове ствари, умањена за износ процењене амортизације и увећана за трошкове монтаже. У случају уништења накнада се утврђује према вредности уз умањење за вредност остатка. У случају оштећења признају се трошкови поправке (утрошени материјал, рад, демонтажа и монтажа и нужни трошкови превоза). У случају да није уговорен откуп одбитне франшизе (откуп учешћа осигураника у штети), надокнађује се само део штете који је изнад уговорене граничне вредности.

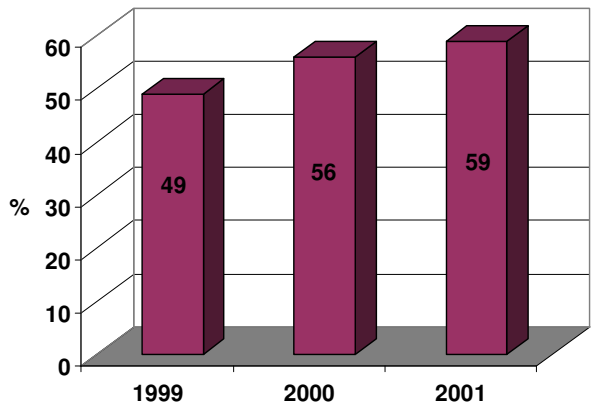
Вредност осигураних података на носачима се споразумно утврђује између уговарача осигурања и

осиг. друштва. Штета се обрачунава према трошковима који су потребни за обнову података, али највише до уговорене вредности на "први ризик". У случају да се подаци паралелно чувају на другом месту, признају се само трошкови потребни за преснимавање.

Осигурана сума за најам другог рачунара и временски период на који се изнајмљивање врши, споразумно се утврђују између уговарача и осиг. друштва. За време квара осигураног рачунара надокнађују се трошкови најма другог рачунара највише до уговорене осигуране суме и уговореног периода покрића. Обавезно се уговара и учешће осигураника у штети у виду временске франшизе, што значи да се не покривају трошкови најма који траје мање од уговореног броја дана.

Конкретне цене се одређују према тарифној групи XVII имовинских осигурања. За персоналне рачунаре цена је скоро двоструко већа него за остале врсте рачунара.

У недостатку домаћих статистичких података послужиће подаци до којих је дошла америчка компанија Columbus [4] анализирајући штете на персоналним рачунарима у САД у последњих неколико година. Најзанимљивији резултат је да се 96% штета догађа на преносним рачунарима (енгл. notebook computer).



Слика 1. Удео штета у осигурању персон. рачунара насталих услед људске непажње

Најчешћи штете на персоналним рачунарима настају услед људске непажње, односно неправилног руковања опремом, као што се види на Слици 1, а међу њима се издвајају по фреквенцији просипање кафе, воде и сокова по рачунарима.

2.2. ОСИГУРАЊЕ ОД ПРЕКИДА РАДА

Предмет осигурања од прекида рада, односно губитка зараде или шомажног осигурања (енгл. Business Interruption Insurance) је изгубљени доходак, који није могао бити остварен услед настанка штетног догађаја и стални трошкови пословања који постоје без обзира да ли се делатност обавља.

У домаћој пракси осигурање од прекида рада се може закључити само као допунско осигурање, што значи да је претходно закључено неко од основних осигурања, најчешће од пожара и других опасности, лома машина или осигурање ел. рачунара.

Осигурана сума се одређује на основу података о реализованом и планираном дохотку и фиксним и варијабилним трошковима осигураника. Може се одредити на два начина: као проценат од фиксних годишњих планираних вредности или као збир одговарајућих динамичних месечних вредности. Осигураник може бити само правно лице које обавља привредну делатност и на основу ње остварује доходак, кога самостално, редовно и трајно утврђује и планира, у складу са законским прописима. Осигурава се по правилу цело правно лице, мада се могу осигурати и само поједини делови уз одговарајућу доплату.

Цена осигурања (премија осигурања) се формира на бази пондерисане стопе за основно осигурање у зависности од дужине уговореног гарантног рока и начина закључења осигурања (на најнижи износ или на месечне износе).

У случају прекида рада надокнађује се износ дохотка који осигураник није могао да реализује у периоду прекида рада и осигурани фиксни трошкови пословања (највише до уговореног износа). Гарантни рок се најчешће уговара у трајању од 3 до 12 месеци. Ако прекид траје краће од уговореног броја дана (најчешће 3 дана), не надокнађује се штета. По правилу осигураник учествује у штети, (франшиза је нпр. 10%), што значи да се надокнађује преостали део штете. Када настане осигурани случај, осигураник је дужан да: предузме мере за отклањање и смањење штете и смањење периода трајања прекида рада, представницима осигуравајућег друштва дозволи сва потребна испитивања у вези штете и њене висине и стави на располагање све пословне књиге за текућу и претходне године. Утврђивање накнаде се врши на бази признатих актуарских метода, прилагођених свакој конкретној ситуацији.

Конкретне цене се одређују према тарифној групи IX имовинских осигурања и сматрају се прилично високим.

3. ОСИГУРАЊА ВЕЗАНА ЗА ИНФ. ТЕХНОЛОГИЈЕ ОД НЕФИЗИЧКИХ УЗРОКА

Мала техничка грешка у програмирању, грешка оператера, злонамерни поступак, вирус или хакерски напад могу срушити велики и скуп информациони систем компаније и потпуно или делимично зауставити њено пословање.

Из угла руководства компаније, најбоље би било имати максималну техничку заштиту инф. ресурса, а остатак ризика пребацити на осигуравајуће друштво.

Размотрићемо услове и могућности за осигурање компанија, чије пословање зависи од исправног функционисања информатичких ресурса, од нефизичких узрока, из угла осигуравајућег друштва.

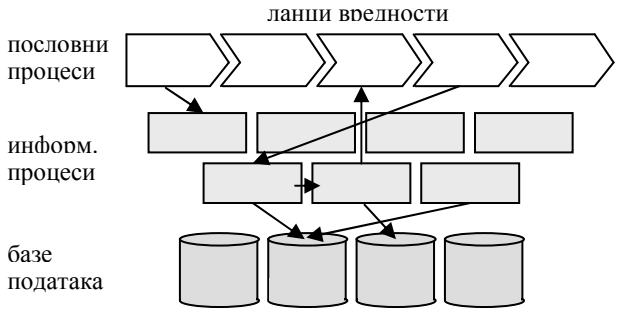
Општа једначина за одређивање цене осигурања:

$$R = p * S \quad (1)$$

Вредност ризика, односно висина премије, коју осигураник плаћа (R) је производ вероватноће да ће се штетни догађај десити (p) и вредности просечне штете (S). Ова општа једначина важи и за осигурања од нефизичких узрока у информатичкој области. Ризици се могу поделити на прихватљиве и неприхватљиве за компанију, а затим се неприхватиљивим ризицима може управљати ограничавањем њихове вероватноће (p) или вредности штете (S). Нажалост, често се овакав начин не може лако применити у пракси.

3.1. ПОСЛЕДИЦЕ ШТЕТЕ

Традиционална индустрија, нпр. челика или текстила, има линеарни производни процес који се састоји од једне или више производне линије, у коме се од сировине долази до финалног производа. Стање магацина и алтернативе у производним линијама су јасно дефинисани, тако да се финансијске последице било ког прекида у раду могу израчунати. Наравно, код већих компанија одређивање финансијских последица прекида рада није нимало једноставно. Неопходно је појединачно анализирати сваки производни процес и вредносни ланац да би се добила реална процена ризика.



Слика 2. Пример производних процеса у информатичкој области

Исти принцип се може применити и на прекиде рада који наступе због проблема са инф. технологијама, али је све много компликованије пошто су производни процеси мање очигледни, број гранања после сваког догађаја је велики, а јављају се и петље. Свеједно, као и код традиционалне индустрије, може се применити анализа вредносних ланаца.

Савремени тренд у информатици је умрежавање ресурса. Из угла сигурности такав приступ носи опасност да проблем у једном рачунару може срушити цео систем од више стотина рачунара распоређених по целој земљи. Ипак, пружа се и могућност да се уведу редундантни системи за критичне ланце вредности – у случају проблема резервни систем моментално преузима функцију сервера који је отказао. Дуплирање идеално решава проблем хакерског напада или саботаже, али грешка у програмирању или вирус на главном серверу највероватније постоје и на резервном серверу који је идентичан главном.

Прекид рада, поред губитка зараде, може оставити и трајне последице по пословање компаније. Клијенти могу почети сарадњу са конкуренцијом, без жеље да се врате, после поновног почетка рада компаније. Наравно, друга крајност је ако на тржишту нема конкуренције за дате производе, па су клијенти принуђени да чекају да компанија поново проради.

Природа података и њихове обраде је кључна у одређивању димензије потенцијалне штете пошто подаци могу бити суштинска вредност извесног производа, али информациони систем може бити и само помоћна алатка у производном процесу. Такође, поставља се питање могућности опоравка података са помоћног медијума у случају изненадног нарушавања конзистентности база података. Осигураник се мора обавезати да организује сиситем чувања података (енгл. back-up system) примерен вредности конкретних података и могућим ризицима. Ситуација се додатно компликује у случају да су подаци поверљиви.

Постоје делатности, као нпр. берзе, у којима је немогуће измерити или компензовати изгубљену добит у случају прекида функционисања информационог сиситема. За такве делатности једноставно треба искључити могућност оваквог осигурања.

3.2. КВАЛИТЕТ РИЗИКА

Контрола ризика се побољшава квалитетном анализом следећих фактора ризика:
- **информатика као услужни процес** – информатика је најчешће услужни процес који подржава пословање компаније. У великим компанијама информатички сектор се бави развојем сопственог информационог система. Информатичке услуге се могу пратити као и сви остали пословни процеси помоћу система управљања квалитетом, који информациони систем потпуно документује. Систем квалитета такође организује испитивање задовољства корисника, идентификацију и корекцију грешки. Најважније је увести правило по коме се све процедуре које систем квалитета налаже, морају спровести пре пуштања у

рад нове верзије апликације, пре него што евентуалне грешке могу угрозити рад целог информационог система.

- **управљање сигурношћу инф. ресурса** – с обзиром да комплексност инф. технологија стално расте одговарајући ниво сигурности се може достићи само ако сви заинтересовани активно сарађују. Треба увести управљање сигурношћу инф. ресурса, да би се прецизно одредили задаци у планирању и праћењу извршавања задатака из те области. Осиг. друштво треба да наведе у полиси које мере компанија мора да испуни да би се ефикасно управљало сигурношћу, као нпр: процедура за криптозаштиту података, заштита од вируса, заштитни зид према Интернету (енгл. firewall), систем приступа инф. систему помоћу лозинки, систем управљања и заштите лозинки, надгледање саобраћаја у рачунарској мрежи, надзор приступних тачака мрежи, котрола коришћења инф. ресурса, итд. Нажалост, нема стандардног решења. Свака компанија је случај за себе и мора се посветити велика пажња при успостављању ове управљачке функције, али се ту не сме стати – потребно је стално развијати и усавршавати ову функцију. Такође, осиг. друштва и одитори треба да повремено проверавају функционисање овог значајног сегмента посла у компанији.
- **свест о ризику** – то је важна карика у анализи, пошто она одређује понашање компаније у предупређивању нежељених догађаја. Неопходна је развијена безбедносна свест у корпоративној култури компаније. Следећа питања могу помоћи у одређивању нивоа развоја свести о ризику: да ли је направљен програм заштите инф. ресурса; постоје ли процедуре у управљању ризиком; да ли су сигурносни захтеви имплементирани у пракси? Кључни индикатор добро развијене свести о ризику је постојање плана за наставак пословања у случају губитка података.
- **моралне дилеме** – саботаже су једна од највећих опасности за информациони систем. Бивши или садашњи незадовољни запослени информатичари представљају велику опасност за интегритет података. Додатни проблем је релативна нестабилност и велика флуктуација информатичког кадра, као и велике и честе фрустрирајуће структурне промене у информатичком сектору. Степен мотивисаности и лојалности радника у инф. сектору значајно утиче на димензију ризика.

3.3. ТРАНСФЕР РИЗИКА

Данас информатичко пословање великог броја компанија директно зависи од услуга које им пружају друге компаније. Нпр. рад електронске продавнице на Интернету директно зависи од Интернет провајдера. Такође, често компаније изнајмљују или узимају на лизинг скупе апликације или моћне рачунаре. Због тога је зависност једних компанија од других све већа, што повећава ризик од прекида рада и компликује одређивање границе на којој се одговорност осигураника завршава. Уколико се услуге изнајмљују од треће стране, мора се пажљиво анализирати ко ће бити одговоран ако ствари крену лоше. Ситуацију додатно компликују закони неких земаља који не гарантују поузданост комуникационих услуга и тиме ограничавају одговорност компанија које обезбеђују телекомуникационе услуге.

У случају да је до прекида рада дошло због штетног догађаја у другој компанији, од које зависи пословање осигураника, осиг. друштво може прихватити да покрије штету само ако је у полиси наведено и име те компаније. Проблеми са добављачима који нису наведени у полиси не могу бити прихваћени, пошто њихов ризик није урачунат у цену осигурања. Прекид рада у оваквим случајевима представља велику опасност за реосигаравача, јер се може десити да се једна штета акумулира и плати више пута. Модерни информациони ресурси су најчешће преко Интернета вишеструко повезани са другима, тако да је често тешко одредити прецизне границе између њих. Такође, због данашњег високог степена умрежености целе планете, вируси и сличне грешке се шире невероватном брзином. Због превеликог ризика од акумулирања штета најбоље је не прихватати овакве случајеве у осигурање, а нарочито не у реосигурање.

Осиг. друштва још увек имају мало искуства са штетама насталим од нефизичких узрока. Прекид рада настао због инф. техологија поред финансијске штете често носи и ненадокадиво нарушавање имица компаније. Пошто нефизички узроци могу бити врло различити, процес утврђивања и обраде штете је доста тежак. Не може се сваки пад инф. сиситема унапред прихватити као осигурани случај, нпр. штета коју је направила апликација која није тестирана пре пуштања у рад свакако не може бити покривена. Зато је у процесу ликвидације штете најважније откривање правог узрока који је довео до проблема са инф. системом.

У појединим полисама, традиционално осигурање имовине некад покрива и податке или софтвер. Таква пракса је погрешна, јер осиг. друштво покрива нови ризик без доплате на основну имовинску премију – догађаће се више штета, а новац за њихово покриће остаје исти. Неопходно је прецизно дефинисање предмета осигурања у информатичкој области и због избегавања каснијег судског утврђивања основаности за исплату накнаде. За разлику од традиционалних имовинских осигурања, осигурање од прекида рада информационог система мора имати прецизно дефинисане узроке штете. Покриће обухвата губитак добитка и додатне трошкове изазване нефизичким узроцима у информационом систему осигураника. Оваква дефиниција омогућава осиг. друштвима да адакватно процене и тарифирају преузети ризик.

3.4. РЕЗИМЕ

Технологија рада савремених компанија је најчешће постављена тако да је немогуће радити без информатичке подршке. Због тога се компаније суочавају са новом врстом ризика који може довести

до прекида рада, великих финансијских губитака, чак и до губитка удела на тржишту.

Разумљиво, компаније желе да се код осигуравајућих друштава где су осигуране и од осталих, традиционалних врста ризика, осигурају и против ове врсте ризика. Наравно, пре осигуравања, компанија треба да одреди које ризике може поднети сама, помоћу процеса управљања ризиком који се састоји из неколико познатих корака:
- идентификација ризика,
- анализа,
- смањење потенцијалних ризика,
- пренос преосталог ризика на осиг. друштво и
- контрола ризика.

Улога осигуравајућег друштва је да поднесе ризик. С обзиром да ризик потиче из релативно новог, информатичког сектора, суштинско питање за осиг. друштво је шта се може сматрати непредвидивим, односно случајним догађајем. Најчешћи узроци проблема са информационим технологијама су грешке у софтверу и губици података. Ови нефизички узроци прекида рада компанија захтевају нови начин обраде ризика.

Могући разлози за прекид рада не леже само унутар компаније. Вируси, хакерски напади и саботаже најчешће долазе споља. Високи степен умрежености инф. ресурса и присуство свих озбиљнијих компанија на Интернету отежавају и поскупљују управљање сигурношћу. Такође, често се поједине информатичке и телекомуникационе функције поверавају спољним сарадницима, од чије поузданости зависи нормалан рад компаније.

Нови ризик захтева нове методе обраде у самој компанији, али и у осигуравајућем друштву. Мора се обратити пажња на следеће факторе:
- управљање процесима обраде информација,
- управљање сигурношћу инф. ресурса,
- процес управљања ризиком,
- план за наставак пословања у случају губитка података и
- корпоративна култура, односно понашање запослених у компанији.

Набројани фактори су индикатор фреквенције могућих штета. Висина штете неког догађаја се одређује по томе како он утиче на целу компанију, иако је то изузетно компликовано због компексности инф. сиситема. Анализа пословних процеса, ланаца вредности и њихових међузависности, као и у традиционалним имовинским осигурањима, помаже у одређивању изложености ризицима.

Нефизички узроци штета, као што су вируси, хакери или грешке у софтверу, често имају епидемијски карактер. Покривање акумулираних штета може представљати велики проблем за осиг. друштво и реосигураваче. Очигледно, неопходно је прецизно формулисати и раздвојити од осталих предмет осигурања у једној команији, да би осиг. друштва могла да преузму ризик и поуздано сервисирају могуће штете.

У принципу, прекид рада који настаје због нефизичких ризика у информатичкој области може се осигурати под следећим условима:
- темељна процена ризика (последице штетног догађаја и квалитет ризика),
- прецизно формулисан предмет покрића, и
- адекватна цена за преузети ризик.

4. ЗАКЉУЧАК

Пословање савремених компанија се не може замислити без јаке информатичке подршке, што носи нове, непознате ризике по несметано функционисање основне делатности компаније. Осигуравајуће компаније у свету су већ развиле програме заштите од прекида пословања због информатичких проблема, било да су узроци за прекид физички или нефизички. Домаћа осигуравајућа друштва имају добар путоказ у светској пракси, тако да ће се неминовно, и код нас, ускоро појавити програми комплетне заштите пословања компанија од ћуди информационих технологија.

ЛИТЕРАТУРА

[1] Ацин Ђ., Цвејић Ђ., *Приручник за праксу у осигурању и реосигурању*, ДДОР Нови Сад а.д., Нови Сад, 1996.

[2] Swiss Reinsurance Company, *Business interruption risks*, Swiss Re Sigma Publication No. 5/2002, Zurich, 2002.

[3] Делта Осигурање а.д., *Услови за осигурање имовине*, Београд, 2000.

[4] Insurance Networking News, *With PCs, Accidents Will Happen*, www.insurancenetworking.com, 2002.

[5] Маровић Б.., Жарковић Н., *Лексикон осигурања*, ДДОР Нови Сад, Нови Сад, 2002.