ТЕМЕ, г. XLI, бр. 3, јул – септембар 2017, стр. 823–837

Прегледни рад DOI: 10.22190/TEME1703823J
Примљено: 6. 6. 2016. UDK 004.738.5
Ревидирана верзија: 6. 2. 2017.
Одобрено за штампу: 15. 6. 2017.

ОСИГУРАЊЕ ОД ИНФОРМАТИЧКИХ РИЗИКА

Слободан Јовановић

Удружење за правно осигурање Србије, Београд, Србија
nsbob@sezampro.rs

Апстракт

У претходне две деценије су свакодневни живот друштва, основна права, друштвене интеракције и привреда постали зависни од континуираног рада информатичке и телекомуникационе технологије. Информатички ризици представљају свакодневну претњу континуираном пословању и пружању услуга у јавном и приватном сектору, а њихово наступање може да проузрокује катастрофалне последице по ствари и људе. То доводи до потребе адекватног управљања информатичким ризицима и дефинисања одговарајућег уговорног оквира осигурања. У овом се раду анализирају различите дефиниције информатичких ризика и поједини појмови у вези са информатичким ризицима, интензитет опасности од информатичких ризика, разлози због којих је неопходно осигурање тих ризика, као и предмет осигурања од информатичких ризика кроз анализу услова осигурања лондонског тржишта.

Кључне речи: информатички ризик, интернет, осигурање, имовина, одговорност.

CYBER INSURANCE

Abstract

Over the previous two decades, everyday life of the society, fundamental rights, social interactions and economy have become largely dependant on the continuous work on the computers and communication technologies. Cyber risks pose everyday threat to the uninterrupted operation and service provision in the public and private sectors, and their occurrence may cause catastrophic consequences to property and people. This necessitates adequate IT risk management and appropriate contract framework of insurance. This paper deals with the analysis of different definitions of the information risks and a few terms connected with information risks, information risk exposure, reasons for cyber insurance, and object of cyber insurance by analyzing insurance policies from London market.

Key words: Information Risk, Internet, Insurance, Property, Liability.

УВОД

У претходне две деценије, интернет је снажно утицао на све делове друштва у свакодневном животу, на основна права, друштвене интеракције и привреду, који данас зависе од континуираног рада информатичке и телекомуникационе технологије (European Commission, 2013, 2). Информатичке и телекомуникационе технологије постале су кичма економског развоја и критичан ресурс на који се ослањају сви сектори друштва. Данас, када су пословне и остале активности зависне од протока података у стварном времену, било који прекид ланца обраде података може да доведе до озбиљног прекида рада који утиче на пословне резултате. Осим тога, намеран или случајан прекид основних услуга у свакодневном животу као што су водоснабдевање, здравствена заштита, снабдевање електричном енергијом или услуге мобилне телефоније могу да имају штетне последице по ствари и лица. Како се технологија развија, старији уређаји који су и даље у употреби такође могу да буду рањиви на информатичке ризике, посебно ако раде са застарелим оперативним системима и рачунарским програмима који више немају подршку (*Allianz Global Corporate & Specialty SE* [Allianz], 2015, 5). Претње могу да буду мотивисане криминалним, политичким, терористичким, државно-спонзорисаним нападима или елементарним непогодама и људским грешкама или пропустима (European Commission, 2013, 3). То доводи до потребе адекватног управљања информатичким ризицима и дефинисања одговарајућег уговорног оквира осигурања.

У овом раду се анализирају различите дефиниције информатичких ризика и поједини појмови у вези са информатичким ризицима, интензитет опасности од информатичких ризика, разлози због којих је неопходно осигурање тих ризика, као и предмет осигурања од информатичких ризика кроз анализу услова осигурања лондонског тржишта.

ДЕФИНИЦИЈА ИНФОРМАТИЧКИХ РИЗИКА

Интензивна примена рачунара и осталих информатичких уређаја (паметни телефон, фаблет, таблет, нови меморијски медији, скенер-миш и друге иновације које се појављују готово свакодневно), као и склоност појединаца злоупотреби, допринели су појави „информатичких ризика". Сваки нови појам односи се на неку врсту друштвених односа, те га је, из разлога научног проучавања, потребно дефинисати.

Дефинисати појам *информатички ризик* значи одредити садржину претње или опасности која, у смислу осигуравајућег покрића, може да проузрокује одређене последице изненадног и ненамерног штетног догађаја. Одређене штетне последице рачунарских ризика

својствене су раду или пословању преко интернета[1], коришћењу рачунара[2], паметних телефона, других информатичких уређаја и електронских – телекомуникационих мрежа.

Колико је тешко дефинисати наведени појам може се видети из мноштва различитих дефиниција које су прилагођене одређеним наменама или активностима појединих организација. Тако, према дефиницији радне групе *CRO Forum*, информатички ризик представља опасност од употребе електронских података и њиховог преношења, укључујући и технолошка средства као што су интернет и телекомуникационе мреже (CRO Forum, 2014, 5)[3], док се према Институту за управљање ризицима (*The Institute of Risk Management*) из Лондона под информатичким ризиком подразумева финансијска штета, губитак или нарушавање репутације организације због неке врсте квара њених система информатичке технологије (The Institute of Risk Management [IRM], 2014, 8). Са друге стране, неретко се истиче да су у најширем значењу појмови „рачунарски ризици" и „информатички ризици" синоними, што значи да је „пословни ризик повезан са употребом, својином, управљањем, повезаношћу, утицајем и усвајањем информатичке технологије унутар привредног субјекта" (Marsh Ltd, 2015, 8). Према трећој дефиницији, информатички ризик је свака врста офанзивног понашања појединаца или организација – компјутерских програмера усмереног на циљане рачунарске информационе системе, инфраструктуру, рачунарске мреже и/или личне рачунаре ради крађе, измене или уништавања, по правилу, са непознатих локација (Cyber-attack, 2016).

По нашем мишљењу, „информатички ризик" могао би се дефинисати као опасност од штетне употребе и манипулације дигиталним инструкцијама и информацијама које могу да проузрокују финансијску штету на стварима и лицима и штету у вези са испуњавањем законских обавеза. Сматрамо да овако широко постављена дефиниција има смисла јер слични штетни догађаји могу наступити због информатичке технологије без обзира на то да ли је узрок у на-

[1] У смислу Закона о електронским комуникацијама, интернет је глобални електронски комуникациони систем сачињен од великог броја међусобно повезаних рачунарских мрежа и уређаја, који размењују податке користећи заједнички скуп комуникационих протокола (Закон о електронским комуникацијама, 2010, чл. 4, ст. 1, т. 15).

[2] У смислу Кривичног законика, рачунар је сваки електронски уређај који на основу програма аутоматски обрађује и размењује податке (Кривични законик, 2005, чл. 112, ст. 33).

[3] Радна група ове организације окупља чувене осигураваче: Swiss Re, ACE Group, Achmea, Aegon, AIG, Allianz, Aviva, Axa, Generali, Groupama, Legal & General, Lloyd's, Lloyds Banking Group, MAPFRE, Munich Re, NN, Old Mutual, Prudential, Royal & Sun Alliance, SCOR, Unipol и Zurich.

мерном поступку неког лица преко интернета или интерних система. Када говоримо о материјалној штети, она може да се односи, поред директне штете, и на штету због губитка репутације, изгубљену добит због прекида рада или трајне немогућности обављања делатности, кршењу права интелектуалне својине (ауторских права) итд.

Међутим, поред дефинисања горенаведеног појма, у свакодневном животу се јављају бројни информатички и телекомуникациони уређаји, рачунарски програми итд., од чијег дефинисања такође зависи успостављање адекватног и потпуног правног оквира за спровођење осигурања од информатичких ризика. С обзиром на то да домаћа друштва за осигурање још нису донела своје услове осигурања информатичких ризика, добру полазну основу за израду услова за осигурање могу да представљају дефиниције из Кривичног законика Републике Србије (Кривични законик [*Criminal Code*], Службени гласник РС. бр. 85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013 и 108/2014). Кривични законик је у чл. 112 прописао значења различитих појмова који се јављају у вези са употребом информатичких уређаја и технологије као што су: рачунарски податак (Кривични законик, 2005, чл. 112, ст. 17); рачунарска мрежа (Кривични законик, 2005, чл. 112, ст. 18); рачунарски програм (Кривични законик, 2005, чл. 112, ст. 19); рачунарски вирус (Кривични законик, 2005, чл. 112, ст. 20); рачунар (Кривични законик, 2005, чл. 112, ст. 33) и рачунарски систем (Кривични законик, 2005, чл. 112, ст. 34). Поред овог закона, потребно је посебну пажњу посветити и Закону о електронским комуникацијама, који у чл. 4 даје дефиниције одређеног броја појмова који се јављају у контексту електронских комуникационих мрежа, електронских порука и интернета (на пример, чл. 4, ст. 1, т. /1/: *адреса* је низ знакова, слова, цифара и сигнала који је намењен за одређивање одредишта везе; 2) *апликативни програмски интерфејс (АПИ)* је[сте] софтверски интерфејс између апликација пружалаца медијских садржаја и уређаја за пријем тих садржаја; чл. 4, ст. 1 т. 14); *интерфејс* је физичка или логичка веза између два или више уређаја, два [дела] или више делова истог уређаја, или медијума преноса, дефинисана функционалним карактеристикама, карактеристикама сигнала или другим одговарајућим карактеристикама).

ИНТЕНЗИТЕТ ОПАСНОСТИ ОД ИНФОРМАТИЧКИХ РИЗИКА

Министарство за културу, медије и спорт Велике Британије недавно је објавило резултате анкете о нарушавању рачунарске безбедности, по којој се четвртина великих привредних субјеката суочила са овим проблемом најмање једном месечно, а да се готово 70% свих рачунарских напада на привредне субјекте односило на

вирусе[4], шпијунске програме или контаминантне програме (UK Department for Culture, Media & Sport et al. 2016). Осећај небезбедности и страха од нарушавања приватности приликом коришћења рачунара и интернета били су одлучујући разлози због којих је 45% домаћинстава у САД одлучило да се суздржи од одређених активности на интернету као што су куповина, коришћење друштвених мрежа или управљање својим финансијама (е-банкарство – прим. аут.) (Bolton, 2016). У америчкој теорији недавно се појавио један рад у којем је замишљен и описан најгори сценарио у случају општег информатичког напада на САД, при чему је фикција поистовећена са нападом на Перл Харбор, 7. децембра 1941. године када су постојали сви знаци упозорења на предстојећу опасност, али није било благовремене одбрамбене реакције (Trautman, 2016).

Један од недавних примера рањивости услуга на интернету је и случај финског десетогодишњака који је пронашао начин да избрише коментаре корисника на „Инстаграму" (Griffin, 2016a). Иако се ради о услузи која има више друштвено-забавни карактер, последице неких других рачунарских напада често могу бити катастрофалних размера. О томе говори пример *JPMorgan Chase & Co* у којем су неовлашћеним лицима била доступна имена, адресе, телефонски бројеви и електронске адресе власника рачуна 76 милиона домаћинстава и 7 милиона малих предузећа (Agrawal, et al. 2014) или случај када су неовлашћена лица инсталирала контаминантни компјутерски програм на продајне системе фирме *Home Depot* и пет месеци крали информације о 56 милиона платних картица (Lemos, 2014). Посебно је огромних размера рачунарска провала названа „Операција пацов из сенке", која је отпочела 2006. године и данас траје, у системе седамдесет једне организације, произвођача одбрамбене опреме, пословне системе, укључујући Уједињене нације и Међународни олимпијски комитет (Nakashima, 2011). Али, нису само финансијске институције оштећена лица у рачунарском криминалу. Тако су у САД током 2013. године од 614 случаја крађе података већина оштећених били привредни субјекти, болнице и друге организације здравствене заштите (Insurance Information Institute [III], 2014, 3).

Када говоримо о финансијским последицама рачунарског криминала, очигледно је да су оне значајне висине и да су у непрестаном порасту. Годишњи просечан износ штете у САД, због рачунарског криминала, износи 11,6 милиона долара за 2014. годину, што

[4] Према чл. 112, ст. 20 Кривичног законика Републике Србије, рачунарски вирус је „рачунарски програм или неки други скуп наредби унет у рачунар или рачунарску мрежу који је направљен да сам себе умножава и делује на друге програме или податке у рачунару или рачунарској мрежи додавањем тог програма или скупа наредби једном или више рачунарских програма или података".

представља повећање за 30% у односу на претходну годину, док је појединачни износ штете на узорку од шездесет организација износио од 1,3 милиона долара до 58 милиона долара (III, 2014, 8). У доњој табели дајемо преглед процењених укупних штета услед рачунарског криминала у првих десет светских економија по висини бруто друштвеног производа (даље у тексту: БДП).

Табела 1. Процењена штета од информатичког криминала у 10 водећих светских економија (у милијардама долара)

Државе рангиране према висини БДП		Информатички криминал у % од БДП	Процењена штета
САД	16.800	0,64%	108
Кина	9.500	0,63%	60
Јапан	4.900	0,20%	0,98
Немачка	3.700	1,60%	59
Француска	2.800	1,10%	3
Велика Британија	2.700	0,16%	3
Бразил	2.400	0,32%	7,7
Русија	2.100	0,10%	2
Италија	2.100	0,04%	0,9
Индија	1.900	0,21%	4

Извор: A Guide to Cyber Risk (*Allianz Global Corporate & Specialty SE*, 2015, 7).

Када упоредимо процењене укупне износе штета у односу на бруто друштвени производ, долазимо до закључка да разлике могу настати најмање из два следећа разлога: по основу квалитета заштите рачунарских система и мрежа или услед непостојања поуздане статистике. Због тога није могуће тврдити да су државе са мањим процентом процењеног информатичког криминала и стварно мање изложене том проблему, али је исто тако вероватно да државе са вишом проценом штете од рачунарског криминала воде његову ажурнију статистику. Увиђајући проблем непостојања статистичких података, једна од иницијатива на територији Европске уније за уредно и доследно вођење статистике о информатичким ризицима потекла је од удружења осигуравача *CRO Forum*, које је, у време писања овог рада, радило на успостављању инфраструктуре ради бољег вођења статистичких података о информатичким ризицима и штетама и креира општу класификацију информатичких ризика заједно са општим правилима за њихово пријављивање (European Cybersecurity Industry Leaders, 2016, 17). У САД, Комисија за хартије од вредности и берзе је још у октобру 2011. године донела смернице којима су привредни субјекти чијим се акцијама тргује на берзи обавезани да пријављују значајне примере информатичких ризика и догађаја (Securities and Exchange Commission, 2011), док је енглески Лојд, у сарадњи са одређеним бројем организација, установио опште критеријуме за ин-

форматичке ризике и њихове карактеристике које њихови чланови – осигуравачи и реосигуравачи – морају користити када се ради о информацијама у складу са постојећим шифрама осигурања (Lloyd's Cyber Core Data Requirements, n.d.).

С обзиром на све интензивнију употребу интернета и зависност од информатичких технологија и уређаја[5], као и свеприсутну опасност од настанка штете услед информатичких напада и тој технологији својственим ризицима, потреба за осигурањем од штетних последица расте. То је истакло и Удружење британских осигуравача, које сматра да осигурање од информатичких ризика треба да до 2025. године постане уобичајено, јер су сви привредни субјекти који користе интернет рањиви на нападе лопова и губитак података услед људске грешке. Оно истиче следеће кључне разлоге за ту тврдњу: (1) информатички криминал један је од најбрже растућих облика криминала у свету; (2) информатичке претње су високотехнолошке природе; (3) привредни субјекти су високо зависни од информатичких технологија у свакодневном пословању и (4) информатички напади и кварови могу довести до престанка бављења делатношћу или битног мењања начина обављања делатности (Association of British Insurers, 2015). Коначно, треба истаћи да су опасности из информатичких активности, а посебно употреба интернета, релативно нове многим појединцима и организацијама које немају превише знања и искуства да би их разумели или деловали против њих. Међутим, како истиче лондонски Институт за управљање ризицима, „на основу информација од Владе и специјализованих агенција, нико није безбедан од тих опасности" (IRM, 2014, 10). Из наведених разлога, све више се улаже у безбедност података и комуникације, а један од последњих примера заштите власника паметних телефона је и рачунарски програм који може да открије и пријави свом власнику ако дође до неовлашћеног приступања и манипулисања садржајем (Griffin, 2016b).

ОСИГУРАЊЕ ОД ИНФОРМАТИЧКИХ РИЗИКА

Пре него што пређемо на излагање о осигурању од информатичких ризика, неопходно је да анализирамо које врсте информатичких претњи постоје и које последице они производе. Информатички напади долазе кроз примену „злонамерних компјутерских програма" (енгл. *Malicious software*, *Malware*), који оштећују рачунарски систем тако што неовлашћена лица краду заштићене податке, бришу документе или убацују компјутерске програме без сагласности корисника предметног рачунара (Malicious software, n.d.).

[5] Процене говоре да ће до 2020. године хиљаду милијарди (1 трилион) уређаја бити умрежено (*Allianz Global Corporate & Specialty SE* [Allianz], 2015, 5).

Осигурање од информатичких ризика је нова врста осигурања која се појавила у високоразвијеним државама[6], док код нас, колико је аутору познато, домаћа друштва још увек немају у понуди ову врсту осигурања која би одговарала садржини услова осигурања страних осигуравача. Пре свега, треба имати у виду да ова врста осигурања може да се спроводи као осигурање имовине и као осигурање од одговорности према трећим лицима.

Традиционалне врсте осигурања имовине не покривају ове врсте ризика, иако је могуће да се и по таквим полисама осигурања пружа покриће прилично ограниченог обима. Тако, на пример, традиционално осигурање имовине пружало би осигуравајуће покриће у случају да информатички напад доведе до настанка неког од осигураних ризика као што су пожар или експлозија, који проузрокују материјалну штету на осигураним стварима. У Великој Британији, на пример, могуће је информатичке ризике осигурати на три начина: да се у постојећим полисама осигурања од опште одговорности уговори проширење покрића и на информатичке ризике (у том случају покриће је прилично ограничено и са доста непокривених ризика – прим. аут.), да се закључи полиса осигурања којом ће се покрити празнине у покрићу по постојећим полисама или да се закључи посебна полиса осигурања од информатичких ризика, што је и најсигурније решење за осигураника.

Са друге стране, домаћа друштва за осигурање продају „Комбиновано осигурање електронских рачунара, процесора и сличних уређаја", које пружа покриће само од тзв. пожарних ризика, својствених осигурању имовине.

У наставку излагања анализираћемо садржину услова осигурања информатичких ризика (комбиновано осигурање имовине и одговорности) два осигуравача са лондонског тржишта: *Hiscox PLC* и *QBE Insurance (Europe) Limited*.

Предмет осигурања имовинских ризика

Према условима осигурања друштва за осигурање *Hiscox PLC*, предмет имовинског осигурања су штете и трошкови специфични за информатичке ризике.

[6] Тржиште осигурања од информатичких ризика у САД је са мање од 100 милиона долара премије током 2002. године нарасла на око 800 милиона долара у 2011. години (Beck, Siemens, 2012, 2); Према процени друштва за осигурање *Allianz Global Corporate & Specialty SE* из Минхена, светско тржиште осигурања од информатичких ризика тренутно се процењује на око 2 милијарде долара премије, од чега око 90% чини премија у САД. Међутим, у наредним годинама очекује се његов раст у двоцифреном износу и могао би да достигне више од 20 милијарди долара у наредних десет година (Allianz, 2015, 6).

По основу осигурања имовине, осигуравач покрива трошкове: (1) неовлашћене манипулације подацима; (2) прекида рада; (3) замене или поправке рачунарских програма и података чуваних у електронском облику и (4) информатичке уцене.

У првој врсти имовинског покрића ради се о покрићу трошкова насталих када осигураник открије или посумња да је дошло до неовлашћене манипулације подацима. То су трошкови: (1) форензичне рачунарске анализе ради потврде настанка осигураног догађаја и идентификације власника личних података; (2) адвокатски трошкови управљања реакцијом осигураника према оштећеном лицу; (3) обавештавања оштећеног лица о неовлашћеној манипулацији подацима; (4) обавештавања надзорног органа на основу закона; (5) коришћења корисничког центра трећег лица ради одговарања на питања оштећених лица после њиховог обавештавања; (6) бесплатне контроле свим оштећеним лицима за период од годину дана и (7) сопствене штете (осим оних које су изричито искључене условима – прим. аут.), као и све горенаведене трошкове настале због неовлашћене манипулације подацима које је проузроковао добављач осигураника. Код последње врсте покрића ради се о надокнади штете у случају када осигураник поверава своју документацију и податке на архивирање некој специјализованој фирми. У том случају за осигураника може да представља проблем ако осигуравачи одбију да покривају такву врсту ризика, јер се ради о ситуацији која није под контролом осигураника (Rawlings, 2015, 21).

За разлику од друштва за осигурање *Hischox*, *QBE Insurance (Europe) Limited* изричито оставља могућност посебног уговарања покрића трошкова односа са јавношћу, управљања кризом, форензичних и осталих специјализованих услуга, укључујући и привремено складиштење електронских података осигураника код трећег лица ако се процени да су осигураникови рачунарски и телекомуникациони системи и даље рањиви (QBE Insurance (Europe) Limited [QBE], n. d., чл. 2.3.3.).

У другој врсти имовинског покрића ради се о надокнади штете настале услед губитка зараде, укључујући и штете настале због губитка репутације и увећаних пословних трошкова директно проузрокованих прекидом пословања током периода осигурања, а који траје дуже од уговореног периода мировања (каренца). Ради се о ризику електронског блокирања осигураниковог рачунарског система, рачунарских програма или података у електронском облику, због чега осигураник не може да послује. Да би овај ризик био покривен, није битно да ли с ради о анонимној блокади или о блокади неовлашћеног лица чији је идентитет познат. За разлику од друштва за осигурање *Hischox*, *QBE Insurance (Europe) Limited* изричито искључује из свог производа осигурања информатичких ризика штете на-

стале услед делимичног или потпуног прекида рада, али оставља могућност да се посебно уговори осигуравајуће покриће и за тај ризик, по основу Одељка Д, чл. 5.

У трећој врсти имовинског покрића ради су о штети коју проузрокује неовлашћено лице (енгл. *Hacker Damage*): (а) оштећењем, уништењем, изменом, ремећењем или злоупотребом рачунарског система, рачунарских програма и електронских података осигураника и (б) копирањем или крађом рачунарских програма или података. У случају настанка овог ризика, наведени осигуравачи надокнађују све разумне и неопходне трошкове замене или поправке рачунарског система, рачунарских програма или података чуваних у електронском облику према истом стандарду и са истим садржајем пре оштећења, уништења, измене, поремећаја, копирања, крађе или злоупотребе.

У четвртој врсти имовинског покрића осигураника ради се о трошковима информатичке уцене (енгл. *Cyber Extortion*) ако током периода осигурања током обављања делатности или рекламирања осигураник прими претњу ради прибављања ствари или услуга, осигуравач надокнађује њихову тржишну вредност, као и трошкове овлашћеног консултанта ради саветовања о преговарању са уцењивачем и крађе новца намењеног за исплату уцене. За разлику од наведеног, друштво за осигурање *QBE Insurance (Europe) Limited*, у својим условима осигурања детаљно дефинише садржај претње информатичком уценом. Тако, информатичка уцена означава претњу неовлашћеног лица да ће: (а) оштетити, уништити, изменити, преметити, копирати, украсти или злоупотребити информације, рачунарски и телекомуникациони систем, укључујући и контаминацију рачунара вирусом, црвом, логичком бомбом или тројанским коњем; (б) преметити безбедност која штити информације, рачунарски и телекомуникациони систем; (в) напасти информације, рачунарски и телекомуникациони систем ради ограничавања или спречавања овлашћених лица или организација да им приступају; (г) открити информације, рачунарски и телекомуникациони систем у јавност, што може да проузрокује комерцијалну или финансијску штету и (д) искористити информације или рачунарски и телекомуникациони систем са циљем да проузрокује штету трећем лицу или осигуранику (QBE, n. d., чл. 10.8).

Према условима осигурања оба друштва за осигурање, осигуравач ће надокнадити штете осигураника које је имао ради спречавања информатичког напада, поправке оштећеног информатичког система, спасавања или дешифровања података, под условом да је осигураник од њега тражио сагласност. Међутим, у пракси је у једном случају искрсао проблем тумачења околности и поступака чувене лондонске Галерије Тејт, којој су 1994. године, на изложби у Франкфурту, украдене две слике Џозефа Тарнера. Поставило се пи-

тање да ли се стварно радило о уцени, давању мита или откупу, док је директор Галерије Тејт тврдио да се радило само о награди посредницима за информацију где се налазе платна, јер Галерија Тејт није имала директне контакте са лоповима (Cumming, 2011). Овде вреди напоменути да је у једном преседану енглеског суда, поводом спора из области поморског осигурања, истакнуто „да не постоји универзална моралност у вези са исплатама за уцене, јер се не ради о акту агресора, већ жртве пиратских претњи, акту који се предузима ради очувања имовине и слободе или живота талаца".[7] Такође треба истаћи да би осигураник, у случају ризика уцене, могао остати без покрића ако би уцењивачима открио да има осигурање.

Предмет осигурања ризика од одговорности према трећим лицима

Према условима осигурања друштва за осигурање *Hiscox PLC*, предмет осигурања пружаоца информатичких услуга од одговорности према трећим лицима су штете и трошкови настали по основу писмених одштетних захтева, грађанских пресуда, одлука надзорног органа или арбитражног суда или било којег процесног средства против осигураника пред надлежним судом. Према Институту за информације из осигурања из Њујорка, број парница у САД у вези са заштитом података и приватности стално се увећава (III, 2014, 16).

У анализираним условима осигурања лондонских осигуравача пружа се покриће у случајевима: (1) одговорности због повреде приватности личних података и поверљивости комерцијалних информација и (2) медијске одговорности.

У првом случају, осигуравач покрива одштетне захтеве које према осигуранику поставе трећа оштећена лица због цурења, кршења или повреде права на приватност на основу прописа о заштити личних података, укључујући податке о потрошачима, кршења обавезе одржавања безбедности или поверљивости личних података и комерцијалних информација.

У другој врсти осигуравајућег покрића од одговорности, осигуравач покрива трошкове који током периода осигурања настану због постављања одштетног захтева трећих лица према осигуранику због: (1) кршења права интелектуалне својине[8]; (2) клевете, укључу-

[7] *Masefield AG v Amlin Corporate Member Ltd* [2012] 1 WLR 2012 at 2033-34.

[8] У погледу права интелектуалне својине, друштво за осигурање *QBE Insurance* таксативно наводи, што је далеко повољније за осигураника, да се у том случају ради о покрићу: права интелектуалне својине, укључујући ауторска права, дизајн, наслов, слоган, пословну тајну, трговачку марку, трговачко име, трговачку униформу, ознаку услуге, назив услуге, назив домена или метатага, кршење моралних права, плагирање, пиратерију и друге непоменуте примере у вези са мултимедијским пословима (QBE, n. d. чл. 2.1, т. (i)).

јући и гласине, увреде, клевете конкуренције, омаловажавања производа или лажи и (3) немарног преношења вируса. Горенаведени ризици покривени су ако су директно проузроковани садржајем осигураникове електронске поруке, интранета, екстранета или интернет стране, укључујући и ризик да је то учинило неовлашћено лице. Овде треба напоменути да друштво за осигурање *QBE Insurance (Europe) Limited* покрива горенаведене ризике прве и друге врсте осигуравајућег покрића од одговорности само ако су они настали као последица радњи или пропуста директора или пословних партнера осигураника, али не и радње или грешке лица запослених код осигураника. Покриће за последице радњи или грешака лица запослених код осигураника овај осигуравач нуди као допунски ризик (QBE, n. d., чл. 2.3.1.).

ЗАКЉУЧАК

Информатичке претње су стално присутне, често се извесно време непримећено одвијају из бројних мотива, а могу долазити из земље и света, без обзира на временски тренутак. Због тога би све организације јавног и приватног сектора требало да процене своје информатичке ризике и да се интересују за осигуравајуће покриће код домаћих осигуравача. Без обзира на то што домаћи услови осигурања информатичких ризика још нису донети, одговарајућа иницијатива и повећана тражња свакако би приморали домаћа друштва за осигурање да размисле о увођењу ове врсте осигурања у своју понуду.

Страна искуства показала су да осигурање од информатичких ризика може да буде драгоцено средство за смањивање губитака због информатичких напада. Међутим, увидом у предмет осигурања само два осигуравача са лондонског тржишта, можемо да констатујемо да се њихови услови разликују јер су неки ризици или трошкови већ у основном покрићу код једног осигуравача, док код другог покриће истих ризика и трошкова мора да се посебно уговара. Због тога је веома важно да осигураници одреде своје потребе и жеље за осигурањем, затим да траже осигуравача који им то може пружити, а када добију услове осигурања да их пажљиво прочитају и схвате шта је тачно предмет осигурања које им нуди осигуравач. Свакако је далеко боље благовремено, пре закључења полисе осигурања, да осигураник уочи неслагања између својих потреба и жеља и понуде осигуравача и да одмах преговара са осигуравачем о могућности проширења покрића и његовог усклађивања са сопственим очекивањима.

ЛИТЕРАТУРА

Agrawal, T., Henry, D. & Finkle, J. (2014, October 2). JP Morgan hack exposed data of 83 million, among biggest breaches in history. *Reuters*. Retrieved from http://www.reuters.com/article/us-jpmorgan-cybersecurity-idUSKCN0HR23T20141003.

Allianz Global Corporate & Specialty SE. (2015). *A Guide to Cyber Risk*. Munich: Allianz Global Corporate & Specialty SE.

Association of British Insurers. (2015). Cyber insurance to become a business essential within the next decade. Retrieved from https://www.abi.org.uk/News/News-releases/2015/05/Cyber-insurance-to-become-a-business-essential-within-the-next-decade.

Beck, D., Siemens, R. (2012). Cyber Insurance – Mitigating Loss from Cyber Attacks. *Perspectives on Insurance Recovery Newsletter*. New York: Pillsbury Winthrop Shaw Pittman LLP. Retrieved from http://www.pillsburylaw.com/publications/cyber-insurancemitigating-loss-from-cyber-attacks.

Bolton, D. (2016, May 16). Hackers and Government surveillance are making people abandon the Internet, survey finds. *Independent*. Retrieved from http://www.independent.co.uk/life-style/gadgets-and-tech/news/hacking-cybersecurity-cyberattack-surveillance-nsa-cia-gchq-internet-use-effect-a7031926.html.

CRO Forum. (2014). *Cyber resilience: The cyber risk challenge and the role of insurance*. Amsterdam: CRO Forum & KPMG Advisory N.V.

Cumming, L. (2011, July 17). Art Theft and the Case of the Stolen Turners by Sandy Nairne – review. *The Guardian*. Retrieved from https://www.theguardian.com/books/2011/jul/17/art-theft-case-stolen-turners-review.

Cyber-attack. (2016, April 17). In *Wikipedia, the free encyclopedia*. Retrieved May 20, 2016, from https://en.wikipedia.org/wiki/Cyber-attack.

European Commission. (2013, Ferbuary 7). *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, JOIN(2013) 1 final. Brussels: European Commission.

European Cybersecurity Industry Leaders. (2016). *Recommendations on Cybersecurity for Europe.* Forum International de la Cybersécurité. Lille: European Cybersecurity Industry Leaders.

Griffin, A. (2016a, May 4). Instagram hacked by 10-year-old, who wins $10,000 prize for finding way to delete comments. *Independent*. Retrieved from http://www.independent.co.uk/life-style/gadgets-and-tech/news/instagram-hacked-by-10-year-old-who-gets-10000-prize-for-finding-way-to-delete-users-comments-a7012496.html.

Griffin, A. (2016b, May 10). iPhone app tells users if phones have been hacked into or secretly jailbroken. *Independent.* Retrieved from http://www.independent.co.uk/life-style/gadgets-and-tech/news/iphone-app-tells-users-if-phones-have-been-hacked-into-or-secretly-jailbroken-a7022236.html.

Hiscox PLC. (2015). *Cyber and data Policy wording*, WD-PIP-UK-CD(2) 13388 05/15.

HM Government & Marsh Ltd. (2015). *UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk*. London: Marsh Ltd.

Insurance Information Institute. (2014). *Cyber Risks: The Growing Threat*. New York: Insurance Information Institute.

Кривични законик [*Criminal Code*], Службени гласник РС. Бр. (85/2005), 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013 и 108/2014.

Lemos, R. (2014, September 19). Home Depot estimates data on 56 million cards stolen by cybercriminals. *Ars Technica*. Retrieved from http://arstechnica.com/security/2014/09/home-depot-estimates-data-on-56-million-cards-stolen-by-cybercrimnals/.

Lloyd's Cyber Core Data Requirements. (n.d.). Retrieved from http://www.lloyds.com/news-and-insight/risk-insight/emerging-risks-team/cyber-core-data-requirements, May 26, 2016.

Malicious Software (Malware). (n. d.). In *Techopedia*. Retrieved May 26, 2016, from https://www.techopedia.com/definition/4015/malicious-software-malware.

Nakashima, E. (2011, August 3). Report on 'Operation Shady RAT' identifies widespread cyber-spying. *The Washington Post*. Retrieved from https://www.washingtonpost.com/national/national-security/report-identifies-widespread-cyber-spying/2011/07/29/gIQAoTUmqI_story.html.

QBE Insurance (Europe) Limited. (n. d.). *QBE Cyber Response: Cyber and Data Security Insurance Policy*, PCYB020414 QBE Cyber Response (QBE PI 14 CR).

Rawlings, P. (2015). Cyber Risk: Insuring the Digital Age. Legal Studies Research Paper No. 189/2015. London: Queen Mary University of London, School of Law.

Securities and Exchange Commission. (2011). *CF Disclosure Guidance: Topic No. 2 – Cybersecurity*. Retrieved from http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

The Institute of Risk Management. (2014). *IRM Cyber Risk: Executive Summary*. London: The Institute of Risk Management.

Trautman, L. (2016, March 25). Is Cyberattack the Next Pearl Harbor? *North Carolina Journal of Law and Technology*, Vol. 18, 2017 Forthcoming. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2711059, May 27, 2016.

UK Department for Culture, Media & Sport and Ed Vaizey MP. (2016). *Two thirds of large UK businesses hit by cyber breach or attack in past year*. London: UK Department for Culture, Media & Sport and Ed Vaizey MP. Retrieved from https://www.gov.uk/government/news/two-thirds-of-large-uk-businesses-hit-by-cyber-breach-or-attack-in-past-year.

Закон о електронским комуникацијама [*Electronic Communications Act*], Службени гласник РС. бр. (45/2010).

CYBER INSURANCE

Slobodan Jovanović
Association for Insurance Law of Serbia, Belgrade, Serbia

Summary

Over the previous two decades, everyday life of the society, fundamental rights, social interactions and economy have become dependant from the continuous work on the computers and communication technologies. Cyber risks pose everyday threat to the operation and service provision in the public and private sectors without interruption, and their occurrence may cause catastrophic consequences to property and people. This necessitates adequate IT risk management and appropriate contract framework of insurance.

This paper deals with the analysis of different definitions of the information risks and a few terms connected with information risks, information risk exposure, reasons for

cyber insurance, and object of cyber insurance by analyzing insurance policies from London market.

How difficult it is to define the term "cyber risk" can be seen from the handful of different definitions adapted to the certain purpose or activity of the organization. In the author's opinion, "cyber risk" is a danger from harmful use and manipulation with digital instructions and data that may cause financial loss to the assets and people and expenses relating to legal obligations.

The author recommends national organizations from public and private sectors to assess their cyber risks. Although there is no insurance company selling cyber insurance policy in Serbia at the moment, in the author's opinion organizations should start seeking insurance, which should necessitate insurers to think over introducing this new line of business.

Experience, so far, has shown that the cyber insurance can be a valuable tool for reducing losses due to the cyber attack. However, insurance policies differ and what is covered by one insurer, the policyholder needs to negotiate adequate extensions with the other. This is why it is important that the policyholders determine their insurance needs and objectives, seek insurer who may meet those, and when they get terms and conditions, to read them carefully and understand what exactly is the subject of insurance that is being offered by the insurer. Furthermore, it is far better that the policyholder notices discrepancies between his / her needs and objectives and the insurance offer, and start negotiating with the insurer about possible cover extension and / or its adaption against his / her expectation.