

Biljana Cerin, dipl. ing.,
ZAVOD ZA ISPITIVANJE KVALITETE, d.o.o., Zagreb, Hrvatska
mr. sc. Goran Vojković, dipl. iur.

Prenošenje sigurnosnog rizika na osiguratelja kao element sustava upravljanja sigurnošću informacija

SAŽETAK

Suvremeno poslovanje sve se više temelji na raznim oblicima elektroničkog poslovanja. Takav način poslovanja donosi i neke nove rizike za sigurnost informacija: od potencijalnih računalnih prijevара i drugih oblika cyber-kriminala do tehničkih pogrešaka koje uzrokuju nepravilnosti u radu sustava i gubljenje podataka. Najveća opasnost i dalje se krije u samim korisnicima sustava, čijom se pravilnom edukacijom može umanjiti veliki dio sigurnosnih rizika. Ozbiljna institucija će svakako uzeti u obzir ove rizike te će uspostaviti odgovarajuću razinu sigurnosti informacija, najčešće uvođenjem kontroliranog sustava upravljanja sigurnošću informa-

cija u skladu s međunarodno priznatim standardima i najboljim praksama. Opcije za tretiranje rizika svode se na njegovo uklanjanje, smanjivanje, prihvaćanje, ili pak prenošenje na treću stranu, odnosno osiguravajuće društvo. Kako bi osiguravajuće društvo moglo pravilno procijeniti rizik i ponuditi obostrano prihvatljive uvjete (iznos premije i visinu osigurane svote), mora provjeriti razinu informacijske sigurnosti korisnika. U protivnom, osiguratelj se izlaže riziku plaćanja osigurane svote za nekoga čija razina sigurnosti nije bila primjerena. Provjeru razine informacijske sigurnosti osiguravajuće društvo u pravilu će vršiti uz pomoć odgovarajućih vanjskih stručnjaka i specijaliziranih institucija za pita-

nja informacijske sigurnosti. Nadalje, kako bi visina premije trebala biti obrnuto proporcionalna visini rizika, poželjno je da osiguratelj politikom premija potiče podizanje razine informacijske sigurnosti, tj. primjereno snizi premije nekome za koga je provjera ustanovila da mu je stupanj informacijske sigurnosti visok, odnosno povisi premije nekome tko ne polaže dovoljno pažnje informacijskoj sigurnosti. Pri svemu tome, neovisni stručnjaci i društva koja se bave informacijskom sigurnošću pojavljivat će se u dvostrukoj ulozi: razvoja korisnikovog sustava upravljanja sigurnošću informacija te kontrole postojećeg sustava u svrhu procjene njegove kvalitete.

UVODNO O TEMI

Današnje poslovanje bitno je vezano uz informacije. "Način sakupljanja, obrade i uporabe informacija odredit će hoćete li biti pobjednik ili gubitnik."¹ Ostati bez poslovnih informacija bilo koje vrste predstavlja izniman rizik po ugled i poslovanje bilo kojeg gospodarskog subjekta. Stoga će mnogi gospodarski subjekti htjeti taj rizik prenijeti na osiguratelja.

Osigurati od rizika gubitka informacija bilo koje vrste suvremeno trgovačko društvo ili banku koja nema uspostavljen sustav upravljanja sigurnošću informacija ili ne provodi predviđene mjere upravljanja sigurnošću jednako je kao osigurati tehnički neispra-

van automobil: ne postavlja se pitanje hoće li do incidenta doći – već kada će do njega doći.

UVODNO O RIZICIMA UOPĆE

Postoji nekoliko definicija pojma rizik. Tako primjerice E. i T. Vaughan definiraju rizik kao stanje u kojem postoji mogućnost negativnog odstupanja od poželjnog ishoda koji se očekuje.²

Sigurnosni rizici koji se javljaju uvođenjem suvremenog elektroničkog poslovanja mogu se uklopiti u postojeće teorijske podjele rizika prema kojima rizike dijelimo na vanjske (rizici kojima je izvorište u okruženju, te se na njih ne može aktivno utjecati) i

¹ Bill Gates – Collins Hemingway: Poslovanje brzinom misli, Izvori, Zagreb, 1999., str. 5

² Emmett J. Vaughan, Therese M. Vaughan: Rizici i upravljanje rizicima, Poslovni savjetnik, 11-12, 1998., Zagreb, str. 53

INVESTMENTS Check Writing Account? Yes No Portfolio Account? Yes No

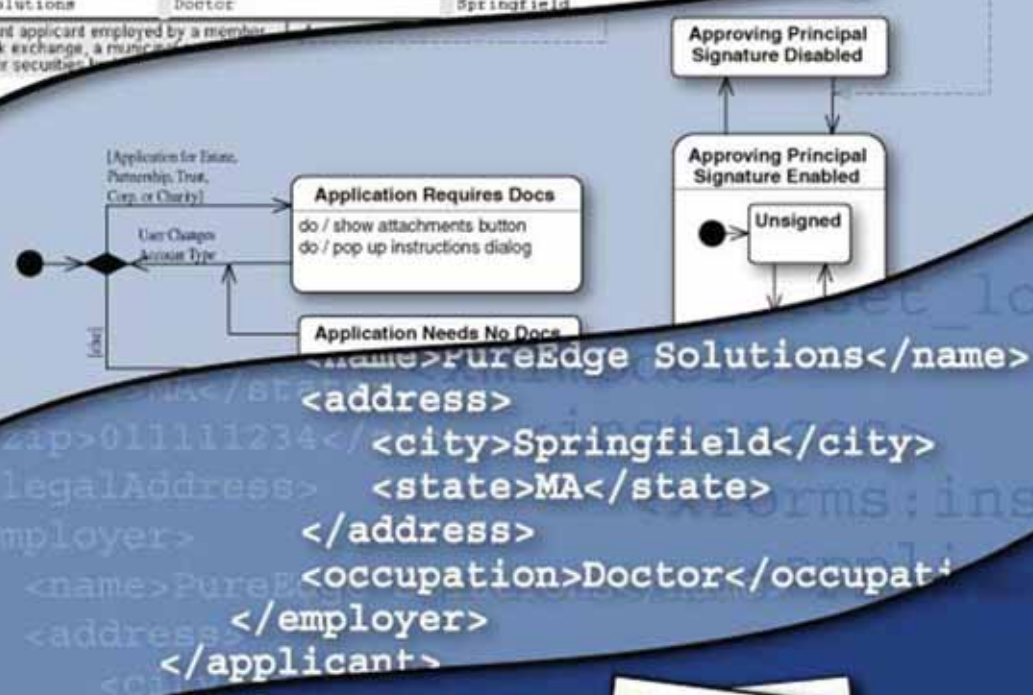
Account Type Individual Estate* Partnership* Custodian for a Minor Collateral *Additional Documents Required
 Joint Tenants Trust* Corporation* Charitable Organization* Investment Club

Applicant Information Required by MSRB Rule C-0(a)(1)(ii) and NASD Rule 2310

First Name: Richard Middle Initial: Last Name: Smith SSN: 999-99-9999 Date of Birth: 04-15-1964 Business Phone: () -
 Mailing Address: 123 Electric Focm Ave City: Springfield State: MA ZIP Code: 01111
 Legal Street Address (Required in Addresses P.O. Box #): 123 Electric Focm Ave City: Springfield State:
 Employer: PureEdge Solutions Occupation: Doctor City: Springfield

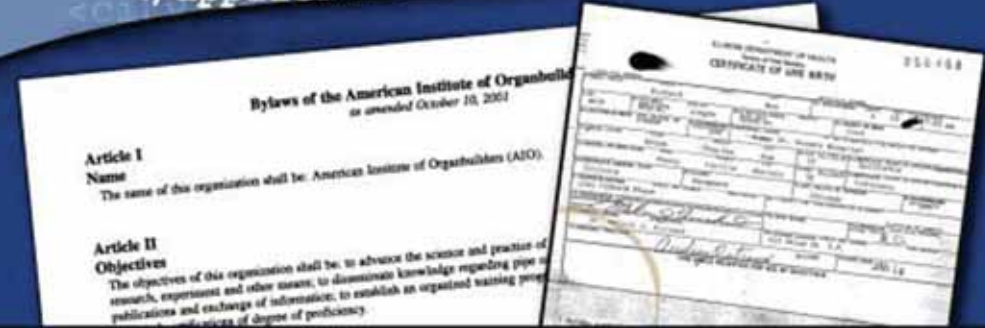
Are you or joint applicant employed by a member firm of a stock exchange, a national securities dealer or other securities...
 Yes, Co

Financial...



```

<name>PureEdge Solutions</name>
<address>
  <city>Springfield</city>
  <state>MA</state>
</legalAddress>
<employer>
  <address>
    <occupation>Doctor</occupati
  </address>
</employer>
</applicant>
  
```



Bez raznih dokumenata i obrazaca normalno poslovanje ne bi bilo moguće jer se u tim formama prikupljaju, strukturiraju i iskazuju sve bitne informacije koje pokreću poslovne procese. Ne samo da u njima biva predstavljena sama tvrtka, njeni proizvodi i usluge, nego su u pravilu prvi korak u poslovnim procesima koji se odvijaju u tvrtki i van nje.

PureEdge eForms i IBM content management rješenja, posebno prilagođena potrebama osiguravajućih društava, omogućuju ubrzavanje poslovnih procesa, veću efikasnost i bolju sigurnost.

unutarnje (poslovni rizici u punom smislu jer na njih unutar organizacije možemo aktivno djelovati). Unutarnji rizici, a u koje neposredno spadaju i sigurnosni rizici³ dijele se na financijske i operativne.⁴ Sigurnosni rizici naravno spadaju u grupu operativnih rizika: dijelom u one koji se nazivaju tehničkim rizicima, a dijelom i u kategoriju namjernih sabotaza i kriminalnih radnji.⁵ Posebno treba napomenuti kako je Republika Hrvatska Zakonom o izmjenama i dopunama Kaznenog zakona⁶ iz 2004. godine, određena društveno neprihvatljiva ponašanja koja predstavljaju sigurnosni rizik (npr. računalno krivotvorenje) kriminalizirala – tj. proglasila kaznenim djelima.⁷

SIGURNOSNI RIZICI

Iako se danas o sigurnosnim rizicima često priča kao o rizicima vezanim uz vezu prema Internetu i elektronička plaćanja – pojam sigurnosnog rizika je puno širi od zaštite organizacija koje imaju razvijeno online poslovanje. Protok velikih količina informacija među informacijskim sustavima pridonosi formiranju "društva bez granica", ali istovremeno otvara informacijske sustave zlonamjernih napadima neovlaštenih korisnika. Napadači prodiru u informacijske sustave uzrokujući velike štete cjelokupnom poslovnoj organizaciji. Unutar samih organizacija, zaposlenici su putem svojih računala spojeni direktno na Internet, što otvara mogućnosti namjernih i nenamjernih otkrivanja povjerljivih podataka kao i otvaranja potencijalnih sigurnosnih ranjivosti sustava. Uzrok tome je često neupućenost, nedovoljna obrazovanost o problemima sigurnosti informacijskih sustava, ili jednostavno nepažnja.

Brzim razvojem informacijskih tehnologija okruženje informacijskih sustava se u velikoj mjeri mijenja. Upotrebom operacijskih sustava opće namjene i distribuiranog procesiranja, te proširenjem izvora pristupa sustavu dodatno se povećavaju i izvori potencijalnih ranjivosti sustava. Kao rezultat ovih pojava, organizacije prepoznaju potrebu za implementiranjem i dokumentiranjem sustava upravljanja sigurnošću informacija.

Sustav upravljanja sigurnošću informacija može se jednostavno protumačiti kao sigurnosna mjera kojom se smanjuju mogućnosti napadača, bilo vanjskog ili unutarnjeg. Sustav upravljanja sigurnošću informacija je isto tako i sredstvo pomoću kojeg više poslovođstvo organizacije prati i nadzire sigurnost informacijskih sustava organizacije, svodeći poslovni rizik na minimum i osiguravajući da sigurnosni zahtjevi poslovanja ispunjavaju korporacijske, kupčeve i pravne obveze.

Specifikacija samog sustava opisana je u drugom dijelu britanskog standarda BS 7799. Prvi dio standarda, poznatiji pod imenom ISO 17799, predstavlja široki spektar smjernica za implementaciju sigurnosnih kontrola, te pokriva sigurnosne politike, pravne, organizacijske, fizičke i ljudske komponente informacijskih sustava. Drugi dio standarda predstavlja zahtjeve u postupcima korištenja i implementiranja sustava upravljanja sigurnošću informacija, dajući pri tom upute što je sve potrebno napraviti kako bi se uspostavila prihvatljiva razina informacijske sigurnosti unutar organizacije. Implementacija sustava upravljanja

sigurnošću informacija vrlo je specifična za svaku organizaciju i ovisi o organizacijskim karakteristikama i specifičnim poslovnim zahtjevima.

Posebno želimo skrenuti pažnju da postoje područja gdje je odgovarajuća visoka razina informacijske sigurnosti zakonska obveza.⁸ Tako Zakon o zaštiti osobnih podataka⁹ propisuje kako su svi podaci po kojima se može identificirati neka osoba – osobni podaci, a gotovo svaka operacija s takvim podacima jest obrada osobnih podataka te je kao takva podložna odredbama Zakona i pripadajućim uredbama. Ukoliko se prikupljaju neke posebno osjetljive kategorije podataka, među koje spadaju podaci o etničkom podrijetlu, političkim stajalištima, vjerskim uvjerenjima i zdravlje osobe (ne zaboravimo da su podaci o zdravlju bitni za mnoga životna osiguranja!), potrebno je imati odgovarajući pristanak osobe, obavijestiti nadležna tijela o takvoj zbirci podataka, te ispuniti iznimno precizne i složene tehničke uvjete koje propisuje Uredba o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka.¹⁰ Navedena Uredba izričito propisuje u čl. 38.: "Mjere, postupci i osobe ovlaštene za osiguranje, pohranjivanje i zaštitu sustava određuju se, ostvaruju i provjeravaju prema planu kojeg donosi voditelj zbirke osobnih podataka, a u skladu s međunarodnim preporukama za to područje (ISO 17799)."

Stoga ovoj problematici treba pristupiti iznimno ozbiljno i uz suradnju s odgovarajućim stručnjacima jer posljedica nedovoljnog obraćanja pažnje informacijskoj sigurnosti može, osim gubitka podataka i uz to vezanih materijalnih troškova, kao posljedicu imati i odgovornost sukladno Zakonu o zaštiti osobnih podataka.

OBVEZA INFORMIRANJA O ZNAČAJNIM OKOLNOSTIMA

Ugovor o osiguranju po svojoj pravnoj prirodi spada u konsensualne ugovore, dakle ugovore koji nastaju kao rezultat suglasnosti dvaju volja: ugovaratelja osiguranja i osiguratelja. Pri tome na volju ugovaratelja osiguranja hoće li sklopiti ugovor i pod kojim uvjetima odlučujuće utječu pravila odnosno uvjeti osiguranja. Zbog toga Zakon o obveznim odnosima¹¹ (ZOO) u čl. 902. st. 3. propisuje: "Osiguratelj je dužan upozoriti ugovaratelja osiguranja da su opći i posebni uvjeti osiguranja sastavni dio ugovora i predati mu njihov tekst, ako ti uvjeti nisu tiskani na samoj polici." Obveza osiguratelja da informira ugovaratelja osiguranja odgovara obveza ugovaratelja osiguranja o prijavi svih okolnosti značajnih za procjenu rizika, tako ZOO u čl. 907. propisuje: "Ugovaratelj osiguranja dužan je prijaviti osiguratelju, prilikom sklapanja ugovora, sve okolnosti koje su značajne za ocjenu rizika, a koje su mu poznate ili nisu mogle ostati nepoznate."¹²

ZOO u čl. 908. st. 1. izričito sankcionira namjernu netočnu prijavu ili prešućivanje bitnih okolnosti od strane ugovaratelja osiguranja: "Ako je ugovaratelj osiguranja namjerno učinio netočnu prijavu ili namjerno prešutio neku okolnost takve prirode da osiguratelj ne bi sklopio ugovor da je znao za pravo stanje stvari, osiguratelj može zahtijevati poništenje ugovora."

³ Širokom definicijom sigurnosni rizike bismo mogli gledati dijelom i kao vanjske rizike – primjerice u slučaju da je zbog loše sigurnosne politike došlo do prekida komunikacijskih kanala (mobilne komunikacije, Internet i sl.), no takav stav ne bi bio metodološki ispravan: u pitanju je samo posljedica nečijeg sigurnosnog propusta, dakle unutarnjeg rizika druge organizacije.

⁴ V. opširnije: Josip Kereta: Upravljanje rizicima, Osiguranje, 9, 2004., Zagreb, str. 26-27

⁵ Popis operativnih rizika v. u Ibid. str. 26

⁶ NN105/04

⁷ Opširnije: Goran Vojković: Lov na IT krimose, Mreža, 11, 2004., Zagreb, str. 22-23

⁸ Opširnije: Goran Vojković: Čuvanje privatnih digitalija, Mreža, 11, 2004., Zagreb, str. 23-26

⁹ NN103/03

¹⁰ NN139/04

¹¹ NN 53/91, 73/91, 111/93, 3/94, 7/96, 91/96, 112/99 i 88/01. U ovom tekstu koristiti ćemo tekst postojećeg ZOO, a ne novog koji stupa na snagu 1. siječnja 2006. godine (NN 35/05).

¹² Marijan Čurković: Ugovor o osiguranju = obveza informiranja o značajnim okolnostima, Osiguranje, 11, 2002., Zagreb, str. 12-13

Međutim, kako je kod prosječnog gospodarskog subjekta prisutno dosta slabo poznavanje informacijske sigurnosti, mogući su (pa čak i vjerojatni!) nenamjerni pogrešni odgovori na pitanja koja prije sklapanja ugovora postavlja ugovaratelj osiguranja. Primjerice: "Da, imamo antivirusnu zaštitu!" – ali bez spominjanja da je pretplata za identifikatore novih virusa istekla; "Da, pa mijenjamo šifre svaki tjedan!" – bez spominjanja da zbog pretjerane izmjene korisničkih zaporki korisnici iste zapisuju na Post-it papiriće; "Da, imamo zaštitne mehanizme na bežičnoj vezi!" – bez spominjanja da su zbog uštede ostavljeni na tvorničkim postavkama.

Da zaključimo: kod ugovaranja osiguranja gdje je informacijska sigurnost bitna, ugovaratelj osiguranja mora biti iznimno oprezan, te izvršiti provjeru ili tražiti procjenu od strane odgovarajućih stručnjaka. Jedino u slučaju da potencijalni osiguratelj ima implementiran neki od sustava informacijske sigurnosti, primjerice po standardu BS 7799-2, treba držati kako je njegova razina informacijske sigurnosti odgovarajuća.

SIGURNOSNI RIZICI KAO BITAN ČIMBENIK OSIGURANJA FINACIJSKIH GUBITAKA TVRTKAMA KOJE SE ZASNIVAJU NA ONLINE POSLOVANJU

Jedno od najsloženijih osiguranja je svakako osiguranje financijskih gubitaka trgovačkog društva (šomažno osiguranje). Naime, do financijskih gubitaka osim pogrešnih poslovnih odluka dolazi i ostvarenjem različitih opasnosti koje mogu uzrokovati zastoj u proizvodnji ili prodaji i potpuni prekid poslovanja u dužem vremenskom razdoblju. Takav zastoj će naravno dovesti do gubitka prihoda, a razumna uprava društva koje želi ostvariti dobit (ili osigurati opstanak na tržištu) i u ovakvim uvjetima svoje će interese zaštititi osiguranjem.

Ukoliko se pojavi zahtjev za takvim širokim osiguranjem financijskih gubitaka nekog gospodarskog subjekta koji je snažno prisutan na Internetu (od banke koja snažno koristi online poslovanje do trgovina elektroničke opreme koje većinu poslova obavljaju online narudžbama), osiguratelj mora uzeti u obzir jedan iznimno bitan sociološki element kojeg donosi Internet i ostali suvremeni načini komunikacije: loše vijesti se iznimno brzo šire, a iznimno velika ponuda usluga kao posljedica ima to da će korisnici usluga ili kupci na duži rok zaobilaziti gospodarski subjekt kod kojeg se ostvario sigurnosni rizik koji spada u domenu sigurnosti informacija, npr. krađa brojeva kreditnih kartica. Online trgovina se od jednog jedinog takvog incidenta gospodarski neće oporaviti. Stoga ugovaranje šomažnog osiguranja za bilo koji subjekt koji koristi online poslovanje bez odgovarajuće uspostave i provjere sustava sigurnosti informacija – znači iznimno poslovni rizik za osiguravajuće društvo.

PROBLEMI KOD ODREĐIVANJA CIJENE PREMIJE

"Stručne službe osiguratelja moraju uskladiti obujam pokrivenosti s cijenom osiguranja – premijom. Iznos premije osiguranja mora biti dovoljan da se, uz pretpostavku zaključivanja određenog broja ugovora o osiguranju, mogu naknaditi nastale štete oštećenima ili isplatiti osigurana svota, te pokriti troškovi koje je osiguratelj imao za određenu vrstu osiguranja. Budući da su društva za osiguranje – društva koja su osnivali dioničari (s ulogom u temeljni kapital), poželjno bi bilo da u premiji osiguranja bude sadržan i dio za ostvarenje dobiti osiguratelja."¹³

¹³ Vice Barbir: Uvjeti i cjenici u osiguranju, *Osiguranje*, 11, 2003., Zagreb, str. 28

¹⁴ Zvonimir Vlahov: Regres i osiguranje, *Osiguranje*, 4, 2005., Zagreb, str. 31

¹⁵ NN105/04

¹⁶ Drago Klobučar: Risk menadžment proces, *Osiguranje*, 3, 2003., Zagreb, str. 26-27

¹⁷ V. opširnije: *Ibid.*, str. 28-29

Uvjete osiguranja treba sastavljati interdisciplinarno, u tom poslu trebaju sudjelovati aktuari, pravnici, ekonomisti, a u ovom slučaju i stručnjaci za informacijsku sigurnost. Ono što se može pojaviti kao problem je da u informacijskoj sigurnosti ne postoje odgovarajući povijesni podaci koji trebaju pomoći aktuarima u određivanju visine premije. To se dijelom može ispraviti korištenjem podataka država koje u većoj mjeri koriste elektroničko poslovanje, te imaju više iskustva u informacijskoj sigurnosti od nas, ali svakako će trebati dijelom koristiti i predviđanja naših stručnjaka za informacijsku sigurnost, jer strana iskustva ne moraju u potpunosti biti primjenjiva na naše prilike.

REGRESNA PRAVA OSIGURATELJA

Regres u pravnom smislu označava odštetu, obeštećenje za pretrpljeni gubitak na imovini, odnosno satisfakciju za nematerijalnu štetu.¹⁴ Tako čl. 939. st. 1. ZOO-a propisuje: "Isplatom naknade iz osiguranja prelaze na osiguratelja, po samom zakonu, do visine isplaćene naknade sva osiguranikova prava prema osobi koja je po bilo kojoj osnovi odgovorna za štetu."

U području informacijske sigurnosti mogućnost naplate regresa svakako je povećana stupanjem na snagu Zakona o izmjenama i dopunama Kaznenog zakona¹⁵ iz 2004. godine. Naime, tim Zakonom propisana su nova kaznena djela koja se tiču takozvanog cyber-kriminala, od kojih su za ovo izlaganje bitna: "povreda tajnosti, cjelovitosti i dostupnosti računalnih podataka, programa i sustava" (već postojalo s drugim nazivom, osuvremenjeno); "računalno krivotvorenje" (novo) te "računalna prijevara" (novo). Kazneni progon za sva navedena djela pokreće se po službeno dužnosti.

Ovakvo rješenje iznimno je pogodno za osiguratelje, jer je posao pronalazanja počinitelja zadatak odgovarajućih državnih organa – policije i Državnog odvjetništva. Ukoliko počinitelj bude pronađen i pravomoćno osuđen – moći će se relativno jednostavno pokrenuti postupak naknade štete.

UPRAVLJANJE RIZIKOM

"Risk menadžment ne smije biti izjednačen s menadžmentom u osiguranju. Risk menadžment je širi pojam i razlikuje se od menadžmenta u osiguranju u nekoliko aspekata. Prvo, risk menadžment više pažnje posvećuje identifikaciji i analizi čiste izloženosti riziku gubitaka i tehnikama za sprječavanje takvih gubitaka. Drugo, kao dodatak osiguranju upravljanje rizikom upotrebljava druge tehnike za obradu izloženosti riziku koje uključuju izbjegavanje, kontrolu gubitaka, samopridržaj, osiguranje te neosigurani transfer rizika."¹⁶

Jedna od metoda za upravljanje izloženosti riziku je izbjegavanje rizika – tako trgovačko društvo može primjerice potpuno odbaciti elektroničko poslovanje. No, to u današnjem svijetu znači i sve veće smanjenje prihoda, što je također neprihvatljivo (a i u "klasični sef s podacima se također može provaliti!). Stoga je poslovno prihvatljivija metoda kontrola šteta: trgovačko društvo prihvaća određenu izloženost riziku, ali se želi smanjiti učestalost i ukupna visina šteta. To se postiže raznim mjerama, među koje spadaju provođenje sustava kvalitete, te uvođenje sustava informacijske sigurnosti. Jedna od metoda upravljanja rizicima (i svakako najraširenija) je osiguranje. Ono se obično provodi u situacijama relativno male vjerojatnosti za nastanak štete, ali uz vjerojatnost da šteta, ako nastane, bude velika.¹⁷

Pristup koji smatramo da je sa stano-
višta upravljanja rizikom u sustavu koji
koristi elektroničko poslovanje u bilo
kojem obliku optimalan, jest kombinacija
kontrola šteta (uvođenjem odgovarajućeg
sustava informacijske sigurnosti) i osigu-
ranja.

MOGUĆNOST KORIŠTENJA VANJSKIH USLUGA ZA OSJETLJIVE POSLOVE S PODACIMA

Zaštita informacijskih sustava za sobom
povlači i odgovarajuće financijske troš-
kove. Velike korporacije mogu sustavno
planirati zaštitu, te djelovati preventivno
i kurativno. Samo dobro planirana zaštita
na svim razinama osigurava nesmetan rad
sustava, a ako i dođe do problema, omo-
gućava njihovo brzo otklanjanje i smanji-
vanje štete na minimum.¹⁸

Što je s malim korisnicima? Za njih
je svakako bolje (pa i jeftinije!) da za
osjetljive poslove (npr. elektroničko plaća-
nje) koriste usluge velikih specijaliziranih
društava, nego da sami razvijaju sustav.
U Hrvatskoj već postoje takve moguć-
nosti – tako je primjerice za neku Inter-
net-knjižaru za usluge plaćanja svakako
bolje rješenje koristiti usluge drugih, nego
održavati i plaćati vlastiti sustav. Slično je
i s čuvanjem osobnih podataka, posebno
ako oni ulaze u posebne kategorije osob-
nih podataka; mali sustav jednostavno
neće moći ispuniti sve potrebne uvjete
za čuvanje i obradu tih podataka, a već
sam Zakon o zaštiti osobnih podataka
omogućava povjeravanje tih poslova speci-
jaliziranim osobama.

LITERATURA

1. BS ISO/IEC 17799, Information tech-
nology – Security Techniques - Code
of practice for information security
management, First edition, Internatio-
nal Organization for Standardization,
Geneva, 2005.
2. BSI, BS 7799-2:2002, Information
security management systems – Speci-
fication with guidance for use, British
Standards Institution, London, 2002.
3. Information Security Magazine, Kolo-
voz 2004., str. 50 – 55 "Just in Case",
Lamont Wood ■

Razvoj informatičke tehnologije u sferi obrade, prikupljanja i distribucije podataka
(koji je dodatno potenciran ekspanzijom Interneta) postavio je pred sudionike tog
procesa niz novih zadataka. Jedan od većih problema koji se danas javljaju je
postizanje sigurnosti informacijskog sustava i njegova okruženja.¹⁹

Osiguranje je dio ukupnog upravljanja sigurnosnim rizikom. Bez obzira na to koli-
ko se potrudili tehnologijom zaštititi informacijske sustave, rizik ne može nestati
jer on nije pitanje samo tehnologije, već međusobno usko povezanih aktivnosti
koje uključuju ljude, procese i tehnologiju. Uloga osiguranja je da podrži maksi-
malne napore u postizanju odgovarajuće razine sigurnosti u organizaciji i suoči
se s događajima koje je nemoguće spriječiti ili izbjeći uz ulaganje razumnog
napora. Glavni službenik za informacijsku sigurnost nije u mogućnosti izjaviti da
informacija on će moći slobodno izjaviti da je učinio sve što je bilo u njegovoj
moći da umanjí rizike, a one na koje ne može utjecati, prenio je na osiguratelja.
Ovdje je zaista bitno posvetiti dužnu pažnju riziku. Potrebno je precizno naglasiti
na što se osiguranje odnosi, pri čemu je jako važno regulirati pitanje neizravnih
šteta koje se pojavljuju kao posljedica ostvarenja rizika. Naime, u današnjem
dinamičnom okruženju izmakla dobit može biti iznimno fleksibilan pojam, a gubi-
tak "snage" nekog branda uvjetovan krađom informacija o poslovnim partnerima
ili brojeva kartica iznimno je teško novčano izraziti. Kao dodatna otežavajuća okol-
nost može se pojaviti i nedostatak odgovarajuće pravne prakse: kako sudske,
tako i arbitražne i miriteljske.

Na osiguratelju ostaje zadatak da odredi koliko je dobro organizacija uspostavila
svoj sustav upravljanja sigurnošću informacija. Možemo još reći da usklađenost
sa zahtjevima standarda BS 7799-2 daje dovoljno dobro uvjerenje, no to ne bi
trebalo sprječavati osiguratelje da izvode provjeru sustava osiguranika. Štoviše,
u Velikoj Britaniji, otkud i potječe ovaj standard, već se sve češće čuje rečenica
"BS 7799-2 is just a baseline". Samo osnova. Ono što se danas uvodi u ozbiljne
organizacije su napredni modeli sigurnosnih arhitektura, poput SABSA modela
(System and Business Security Architecture), koji se ne natječe sa standardom
BS 7799-2, već služi kao njegova nadogradnja kroz model upravljanja sigur-
nošću informacija usmjeren specifičnim poslovnim zahtjevima.²⁰

Kako će osiguratelj procijeniti razinu sigurnosti informacija u ciljanj organizaciji,
ovisi o visini police osiguranja. Za police relativno male vrijednosti vjerojatno će
biti dovoljno poslati upitnik na kojeg će organizacija odgovoriti u smislu samo-
provjere, te će osiguratelj vrednovati kvalitetu odgovora i na temelju toga odrediti
visinu premije. Nezavisni prosuditelji usklađenosti sa BS 7799-2 standardom
uveleke će pomoći kod procjene sigurnosti onih organizacija koje su odlučile svoj
sustav uskladiti upravo s ovim standardom. Međutim, postoje i organizacije koje
razvijaju svoje vlastite sigurnosne standarde. Za takve slučajeve, ili za veće izno-
se police, osiguratelj će ići u nezavisnu provjeru sustava upravljanja sigurnošću
informacija, te moguće i dodatno provjeriti sigurnost pomoću provjera ranjivosti
sustava i ispitivanja njegove probojnosti. Za ove usluge je bitno raditi s kvalitet-
nim dobavljačima stručno specijaliziranim u području sigurnosti računalnih mreža
i sustava, nerijetko i socijalnog inženjerstva – ovisi o dubini testa kojem se organi-
zacija treba podvrgnuti.

Republika Hrvatska je u posljednjih par godina donijela gotovo zaokružen zakon-
ski okvir koji omogućava elektroničko poslovanje. Za očekivati je da se relativno
brzo taj okvir počne koristiti u praksi, kako u jačanju elektroničke trgovine, tako
i u prenošenju klasičnih uredskih procesa i raznih baza podataka u elektronički
oblik. U pitanju je pravno, tehnološki pa i socijalno iznimno složeno područje (i
potencijalno novo tržište!), za koje se osiguravajuća društva trebaju na odgova-
rajući način ozbiljno pripremiti. U tome im stručnjaci za informacijsku sigurnost
mogu pružiti dragocjenu stručnu pomoć.

¹⁸ V. opširnije: Ibid. str. 43

¹⁹ Anto Bilobrk: Sigurnost na WWW, Osiguranje, 10, 2002., Zagreb, str. 41

²⁰ Više o SABSA modelu na <http://www.sabsa-institute.org>