MODEL DOLOČITVE OPTIMALNEGA OBSEGA VLAGANJ V INFORMACIJSKO VARNOST

dr. Rok Bojanc, Institut Jožef Stefan, Ljubljana in Ekonomska fakulteta Univerze v Ljubljani
dr. Barbara Mörec, Ekonomska fakulteta Univerze v Ljubljani
dr. Metka Tekavčič, Ekonomska fakulteta Univerze v Ljubljani
dr. Borka Jerman Blažič, Institut Jožef Stefan, Ljubljana in Ekonomska fakulteta Univerze v Ljubljani
UDK 519.72
JEL: D890, L860, M150

Povzetek

Informacijska sredstva podjetja so dnevno izpostavljena naraščajočemu številu različnih groženj, ki – če so napadi uspešni – podjetju lahko povzročijo visoko izgubo premoženja. Rast tveganj informacijske varnosti zato podjetja omejujejo z vlaganji v vrsto ukrepov, ki zmanjšujejo uspešnost napadov ali vsaj omejijo njihove posledice. V tem članku je predstavljen postopek, ki podjetju pomaga pri izbiri ekonomsko optimalnega obsega vlaganj v varnostni ukrep, s katerim podjetje zmanjša posamezno tveganje. Vrednostni obseg koristi varnostnega ukrepa in višino stroškov uvedbe ukrepa smo ocenili s pomočjo matematičnega modela, v katerega so vključeni grožnje in ranljivosti sistema, stroški korektivnih in detekcijskih ukrepov, ki izgubo podjetja ob uspešno izvedenem napadu zmanjšujejo, ter stroški preventivnih ukrepov, ki zmanjšujejo verjetnost za varnostni incident. Rezultat modela je ocena varnostnega tveganja pred izvedenim varnostnim ukrepom in po njegovi izvedbi, ki neposredno vpliva na vrednosti kazalnikov donosnosti vlaganja (ROI), čiste sedanje vrednosti (NPV) in notranje stopnje donosnosti (IRR) ter s tem na odločitev o optimalnih vlaganjih v informacijsko varnost. Prispevek končujemo s prikazom empirične uporabe modela.

***Ključne besede**: informacijska varnost, varnostni ukrep, optimalno vlaganje, matematični model*

Abstract

Every day, a company's information assets are exposed to an increasing number of threats, which – if successful – can cause significant losses. The growth in information security risk can be reduced by investments in a number of measures that reduce the effectiveness of attacks, or at least limit their consequences. This paper presents a procedure that helps in selecting an optimal level of investment in security measures. The monetary evaluation of the benefits of increased information security and the cost evaluation of implemented security measures are determined with a mathematical model, which includes threats of attacks and vulnerabilities of current information system, as well as the costs of corrective measures and costs of detection, which minimise the loss of the attack, as well as the costs of preventive measures that reduce the likelihood of an incident. The result is a model of information security prior to and following the implementation of a security measure that directly affects the return on investment (ROI), net present value (NPV) and internal rate of return (IRR) and, consequently, the decision on the optimal investment in information security. We conclude with an empirical application of the model.

***Key words**: information security, security measures, optimal investment, mathematical model*

1 Uvod

Danes podjetja poslujejo hitreje in učinkoviteje kot kadar koli. Pomemben del zaslug za ta razvoj imajo tudi sodobne informacijske tehnologije, ki podpirajo njihove poslovne procese. Razvoju tehnologij, ki podjetjem omogočajo prenos, obdelavo in hrambo podatkov v najširšem smislu, je sledil tudi razvoj spletnega kriminala, pa tudi zlorabe, kraje in prirejanja podatkov s strani samih zaposlenih v podjetju. Vprašanje, kako zagotoviti, da bodo informacije podjetja ali posameznika varne, je zato čedalje pomembnejše (Dhillon in Backhouse, 2000: 125; Whitman, 2003). Negativne posledice napada na informacijske sisteme podjetja so namreč lahko velike, včasih celo pogubne za podjetje. Tako je lahko v podjetju prekinjeno delovanje poslovnih procesov, podjetje lahko utrpi krajo ali izgubo podatkov, njihovo nepooblaščeno spreminjanje, lahko pa jih njegovi zaposleni »le« nepooblaščeno vpogledujejo (Young in Yung, 1996). Odvisno od vrste napada lahko napadeno podjetje utrpi vse od izgube prihodka in/ali padca produktivnosti do izgube ugleda in zaupanja poslovnih partnerjev.

Če se podjetje želi zavarovati pred grožnjami, ki pretijo njegovim informacijskim sredstvom[1], mora vzpostaviti varnostne mehanizme, ki varujejo njegov informacijski sistem. Za uspešno varovanje pa je ključno, da podjetje dobro pozna grožnje, ki mu pretijo (Whitman, 2003). To

[1] Pod pojmom *informacijska sredstva* razumemo fizično računalniško infrastrukturo (strežniki, omrežna infrastruktura in podobno), programsko opremo, pa tudi zbirke podatkov, intelektualno lastnino, znanje in ugled podjetja (FIPS 199, 2004).

poznavanje je namreč temelj pri sprejemanju odločitev, katera informacijska sredstva želi podjetje varovati pred grožnjami, ki pretijo njegovemu elektronskemu poslovanju, in v kolikšnem obsegu jih želi varovati (FIPS 199, 2004). Povečevanje stopnje varnosti je namreč praviloma povezano z dodatnimi stroški, zato je pomembno, da podjetje premišljeno določi zanj ustrezno stopnjo varnosti, sicer lahko za varnost zapravi občutno več sredstev, kot je potrebno.

Čeprav podatkov o dejanski škodi, ki jo povzročajo varnostni incidenti, primanjkuje, pa podjetja z vidika hitrega povečevanja števila varnostnih incidentov veliko vlagajo v rešitve, povezane z varnostjo informacijskih sistemov (CERT, 2008). Pri tem pa se je spremenil tudi pogled na vlaganja v informacijsko varnost: če je še pred leti večina podjetij na to gledala kot na strošek, jih danes večina gleda kot na naložbo (Tordoff, 2006), ki jo je treba tudi ekonomsko upravičiti (Longstaff et al., 2000). Toda raziskave hkrati tudi kažejo, da podjetja (še) nimajo pravega odgovora na vprašanje, kateri od kazalnikov je najprimernejši pri ocenjevanju upravičenosti naložbe v informacijsko varnost (Deloitte, 2004).

V strokovni literaturi je sicer mogoče najti kar nekaj različnih pristopov za vrednotenje naložb v informacijsko varnost (na primer Huang et al., 2006; Cremonini in Nizovtsev, 2006), vendar je večina predstavljenih modelov osredotočena le na določeno področje (npr. na analizo varnostnih tveganj ali na modeliranje groženj) in zato ne pomenijo celovite rešitve, ki bi jo podjetja lahko uporabila. Če želimo doseči optimalno stopnjo varnosti ob kar najracionalnejši porabi sredstev, moramo varnostna tveganja, ki jim je podjetje izpostavljeno, najprej prepoznati in ovrednotiti (Gordon in Loeb, 2005; ISO 73, 2009). Šele vrednosti posameznih sestavin tveganja (opredeljene z verjetnostjo, da se dogodek zgodi, in mogočo škodo, ki jo bo ob tem lahko imelo podjetje) omogočajo vrednostno oceno primernosti varnostne rešitve: primerjavo vrednosti naložbe v informacijsko varnost in škode, ki bi nastala, če te naložbe ne bi bilo. Pri izbiri optimalnega sistema za zmanjšanje varnostnih tveganj se tako v nadaljevanju pogosto uporabljajo kazalniki *donosnosti vlaganja* (ROI), *čiste sedanje vrednosti* (NPV) in *notranje stopnje donosa* (IRR) naložbe v informacijsko varnost (Sonnenreich et al., 2006).

Članek, ki je pred vami, je sestavljen iz šestih poglavij. Uvodu, v katerem je na kratko orisana problematika vlaganj v informacijsko varnost, sledi predstavitev upravljanja tveganj, ki je temeljni pogoj za zagotovitev optimalne ravni varnosti. Tretje poglavje prikazuje ekonomski pogled na vlaganja v informacijsko varnost, ki temelji na analizi stroškov in dobrobiti (angl. cost-benefit analysis), ki se pojavijo z vlaganjem v informacijsko varnost. V četrtem poglavju je predstavljen matematični model za izbiro optimalnega vlaganja v informacijsko varnost. Model je zasnovan kot standarden postopek, ki podjetje vodi od začetnega vnosa vhodnih podatkov do končnih priporočil za izbiro (glede na potrebe podjetja) optimalne naložbe v informacijsko varnost, ki bo zmanjšala varnostno tveganje. V večini do zdaj predstavljenih modelov za vrednotenje naložb v informacijsko varnost je bil poudarek zgolj na iskanju njihovega optimalnega obsega (Huang et al., 2006; Cremonini in Nizovtsev, 2006), naš model pa omogoča neposredno primerjavo in kvantitativno vrednotenje različnih varnostnih ukrepov. Uporabo modela na primeru vlaganja v protivirusni program smo prikazali v petem poglavju. Sledi sklepna ugotovitev.

2 Zagotavljanje informacijske varnosti

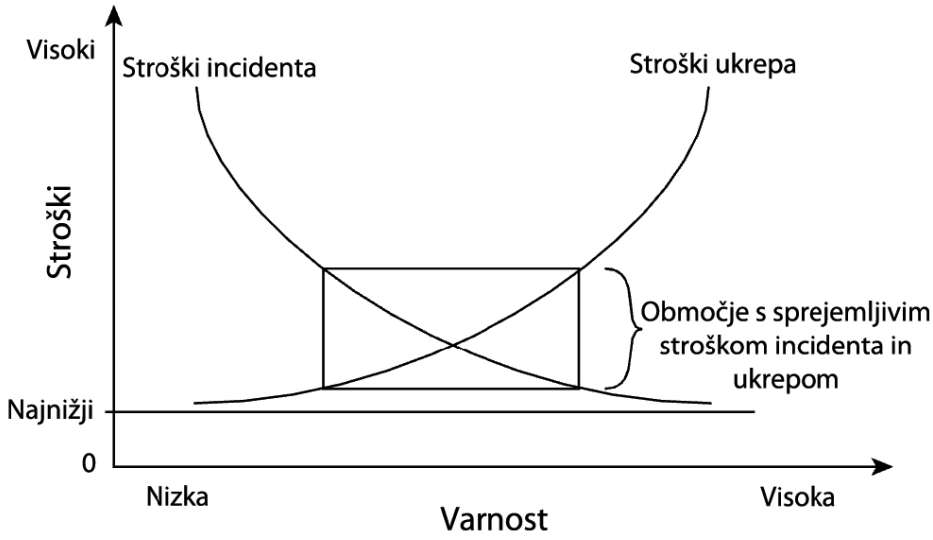
Kako varen bi moral biti informacijski sistem in *kako varen dejansko je?* To sta vprašanji, ki si ju neprenehoma zastavljajo strokovnjaki za varovanje informacijskih sredstev. Na vprašanje, kakšno stopnjo varnosti želimo imeti, Sandhu (2003) enostavno odgovarja, da »*dovolj dobro varnost*«, vendar Geer (2004a) takoj dodaja, da je zelo težko določiti, kaj je dovolj dobro. *Dobro varnost* lahko torej razumemo kot *stopnjo varnosti*, ki je za podjetje sprejemljiva (Schneier, 2003) in je hkrati odvisna od *stroškov varnostnega incidenta* (posledic, ki jih podjetje utrpi, ko pride do napada na njegov informacijski sistem) ter *stroškov ukrepa* (naložbe v informacijsko varnost, ki naj bi ta incident preprečila), kar prikazuje slika 1.

Želeno stopnjo informacijske varnosti pa je le redko mogoče zagotoviti zgolj z vzpostavitvijo neke tehnične rešitve, saj učinkovito odpravljanje varnostnih tveganj praviloma zahteva *procesni pristop* (Schneier, 2004). Ključno namreč je, da podjetje ugotovi in ovrednoti grožnje informacijskemu sistemu, na tej podlagi načrtuje svojo varnostno politiko in šele nato uvede varnostne mehanizme, ki grožnje preprečujejo. V zadnjem koraku podjetje običajno uporabi neko kombinacijo tehničnih rešitev, kot na primer šifrirne tehnike, požarne zidove in sisteme za zaznavanje vdorov (angl. *intrusion detection system*). Toda za zagotovitev ustrezne ravni varnosti so nujno potrebni tudi človeški viri, ki znajo tehnične rešitve pravilno uporabljati (Gordon in Loeb, 2005: 10). Celo več: v razmerah, ko posamezniki niso spodbujeni k spoštovanju varnostnih pravil, celotna varnost odpove kljub vrhunskim tehničnim rešitvam (Dhillon in Backhouse, 2000).

3 Ekonomska analiza vlaganj v informacijsko varnost

Gordon in Loeb (2002a) ugotavljata, da podjetja vlagajo čedalje več sredstev v dejavnosti s področja informacijske varnosti. Sredstva, ki so za to na voljo, pa so omejena in se lahko porabijo tudi za druge naložbe. Z naraščanjem sredstev, ki so potrebna za zagotavljanje določene ravni informacijske varnosti, zato vodstva podjetij čedalje pogosteje zahtevajo tudi *ekonomsko utemeljitev* sprejetja odločitve za naložbo v informacijsko

Slika 1: **Iskanje optimalne rešitve med višino stroškov varnostnega incidenta in stroški ukrepa (tj. obsega naložbe v informacijsko varnost)**



Vir: Kaplan, A Matter of Trust, v Tipton & Krause (ur.), Information Security Management Handbook, 6th edition, 2007, str. 304.

varnost. Swire (2001) tudi sicer ugotavlja, da vodstvo podjetja bolje razume predlog, ki je predstavljen tudi s pomočjo ekonomske in ne zgolj tehnične analize, saj si laže predstavlja (ne)pomembnost škode ob varnostnih incidentih, če je ta izražena kot višina finančne izgube (Bojanc in Jerman - Blažič, 2008: 413).

Vsako podjetje mora zase najti *optimalno raven informacijske varnosti*, ki jo določa razmerje med vrednostjo naložbe in koristmi varovanja (zmanjševanja stroškov incidenta), kar je prikazano na sliki 1. Optimalna raven informacijske varnosti je torej odvisna od dveh sestavin, in sicer od stroškov ukrepa in stroškov incidenta. *Strošek ukrepa* je vrednost naložbe v informacijsko varnost, s katero se podjetje želi izogniti posledicam varnostnega incidenta, *strošek incidenta* pa so sredstva, ki jih podjetje porabi, ko odpravlja posledice varnostnega incidenta. Podjetje, ki nameni zelo malo sredstev za informacijsko varnost, bo praviloma porabilo več sredstev za odpravo posledic pogostih varnostnih incidentov, zelo velika vlaganja v informacijsko varnost pa bodo praviloma močno zmanjšala stroške incidenta, saj se bodo ti redko pojavljali in bodo praviloma imeli manjše posledice. Ker koristi večje informacijske varnosti pogosto niso omejene le na podjetje, pač pa se pojavljajo tudi v širšem družbenem okolju, v katerem podjetje deluje, si pri ocenjevanju optimalne stopnje varnosti lahko pomagamo z *analizo stroškov in dobrobiti*.

3.1 Opredelitev analize stroškov in dobrobiti

Analiza stroškov in dobrobiti (angl. *cost benefit analysis*) je sistematičen pristop ocenjevanja primernosti sprejetja nekega ukrepa, ki primerja vse *dobrobiti* (vrednostno izražene koristi ukrepa) in vse *stroške*, ki nastanejo s sprejetjem tega ukrepa (Gordon in Loeb, 2002b). Analiza izhaja iz osnovnega pogoja, ki mora biti izpolnjen za sprejetje katere koli odločitve je (Brent, 2007):

$$B > C \quad (1)$$

pri čemer je *B* dobrobit, *C* pa strošek.

Izhodiščni pogoj v nadaljevanju preoblikujemo takole:

$$P * E > C \quad (2)$$

pri čemer je *P* cena na enoto koristi, *E* pa količina. Sledi le še:

$$P * E / C > 1 \quad (3)$$

Navedeni količnik se imenuje *razmerje med stroški in dobrobitmi* (angl. *Cost-benefit ratio* – CBR). Količnik mora biti večji od 1 – dobrobiti sprejetja nekega ukrepa morajo torej presegati stroške, ki jih bomo imeli z njegovo uvedbo.

Čeprav v praksi to le redko drži, predpostavimo, da lahko zanesljivo ovrednotimo vse pričakovane skupne dobrobiti v podjetju in širšem družbenem okolju ter vse pričakovane skupne stroške za različne ravni dejavnosti informacijske varnosti. Dokler dobrobiti dodatne dejavnosti informacijske varnosti presegajo stroške, je uvedba dejavnosti smiselna. *Optimalna uvedba varnostnih ukrepov* pa je dosežena v točki, kjer je razlika med dobrobitmi in stroški največja. Uvedba dodatne dejavnosti informacijske varnosti, ki bi presegala to točko, namreč pomeni, da so mejni stroški njene uvedbe

večji od mejnih dobrobiti, ki jih s to dodatno dejavnostjo pridobimo.

V praksi se podjetja srečujejo z omejenimi sredstvi za vlaganje v informacijsko varnost (Gordon in Loeb, 2005: 85). Če je višina sredstev, ki je na voljo, manjša od tiste, ki je potrebna za optimalno vlaganje v informacijsko varnost, bo podjetje vložilo vsa sredstva. Če pa je sredstev več, kot bi jih bilo potrebno za optimalno vlaganje v informacijsko varnost, pa bo racionalno podjetje vlagalo le do optimalne ravni.

3.2 Izvedba analize stroškov in dobrobiti

Analiza dobrobiti in stroškov je običajno sestavljena iz teh korakov (Hanley in Spash, 1993):

1. opredelitev predmeta analize,
2. ugotovitev ekonomskih vplivov projekta,
3. količinska ocena vplivov projekta,
4. vrednostna ocena dobrobiti in stroškov,
5. izračun sedanje vrednosti dobrobiti in stroškov (diskontiranje),
6. izračun čiste sedanje vrednosti,
7. analiza občutljivosti.

Čeprav je analiza dobrobiti in stroškov teoretično nadvse jasna in zato tudi široko sprejeta, pa se pri njeni uvedbi v prakso pojavlja vrsta vprašanj. Najpogostejša so:

– Katere stroške in katere dobrobiti vključimo v analizo?
– Kako te stroške in dobrobiti izmerimo?
– Katero diskontno stopnjo uporabimo?

Po Brentu (2007) so odgovori na ta vprašanja odvisni od tega, čigava dobrobit naj bi se s sprejetjem nekega ukrepa maksimirala. Če naj bi se maksimirala zgolj *dobrobit podjetja*, potem se pri analizi stroškov in dobrobiti upoštevajo samo zasebne dobrobiti in zasebni stroški, torej tiste dobrobiti in stroški, ki vplivajo zgolj na premoženje podjetja (Sugden in Williams,1978). Praviloma pa nas pri analizi zanimajo tudi *dobrobiti širše skupnosti*, zato vanjo vključujemo tudi dobrobiti in stroške, ki vplivajo na blaginjo širše skupnosti. Vlaganje v informacijsko varnost strokovna literatura praviloma obravnava kot skupino odločitev, katerih cilj je povečati premoženje podjetja, zato se v tem članku tudi mi omejujemo zgolj na analizo dobrobiti in stroškov z vidika podjetja. Pri tem se zavedamo, da smo s tem našo analizo omejili na raven analize dobičkonosnosti: za celovito analizo dobrobiti in stroškov bi bilo namreč treba vrednostno oceniti tudi dobrobiti, ki jih ima od povečane varnosti informacijskega poslovanja širša skupnost, ne zgolj podjetje, ki je ukrep povečanja varnosti uvedlo.

V drugem koraku izdelamo seznam vseh posledic (stroškov in koristi), ki izhajajo iz projekta. Pri tem je treba upoštevati morebitne (Miller in Patassini, 2005):

– *dodatnosti* (angl. *additionality*); koliko bo projekt vlaganja v informacijsko varnost dodatno prispeval k npr. številu transakcij, ki jih kupci opravijo po spletu in tako prihranijo čas, koliko bo projekt povečal prodajo naših drugih izdelkov ali zmanjšal naše celotne stroške na enoto (delovanje ekonomije obsega),
– *prerazporeditve dobrobiti* iz drugih projektov; če na primer nov izdelek vključuje varnostno sestavino, utegnejo kupci pogosteje posegati po njem in manj po drugih, ki te sestavine ne vsebujejo.

Merilo ugotavljanja, ali gre za pozitivno ali negativno posledico, je povezano s tem, katere sestavine povečujejo koristi, katere pa pomenijo stroške projekta. Koristi vlaganja v informacijsko varnost so lahko različne in imajo največkrat obliko prihranka stroškov zaradi zmanjšanja verjetnosti ali posledic varnostnega incidenta (Gordon in Loeb, 2005).

Treba je tudi ugotoviti *količinske (fizične) tokove* gibanja koristi in stroškov ter njihov *časovni razpored*. Sestavni del tega koraka je tudi ocena verjetnosti, da se bodo ti tokovi tudi dejansko pojavili in v kolikšnem obsegu. Običajno večina stroškov nastane na začetku življenjskega cikla projekta, koristi pa lahko nastajajo v celotnem življenjskem ciklu naložbe, lahko celo z velikim časovnim zamikom in jih je zato pogosto težko točno napovedati (Gordon & Loeb, 2005, str. 21). Največja težava je, ker gre pogosto za ocenjevanje prihrankov pri stroških odprave posledic varnostnih incidentov, ki se še niso zgodili. Dodatno velja, da bolj je informacijska varnost uspešna, težje je opaziti dejanske koristi. Hkrati dobrobiti in stroški pogosto nimajo fizične oblike. Na primer občutek varnosti sam po sebi nima fizične oblike, lahko pa merimo njegove posledice (opazimo na primer več transakcij prek varnega kanala kot pa prek tistega, ki ni zaščiten). Najtežavnejši del analize pa je *vrednostna ocena* dobrobiti ali stroška. Stroške vlaganja v informacijsko varnost je sicer večinoma mogoče dokaj enostavno določiti, precej teže pa je opredeliti, oceniti ali meriti koristi (Soo Hoo, 2000). Varnostne rešitve (npr. požarni zid in protivirusni program) same po sebi namreč ne prinašajo koristi v taki obliki, da jih je mogoče enostavno izmeriti.

Ker dobrobiti in stroški nastajajo v različnih časovnih trenutkih, moramo v enačbi (1) primerjati njihove *sedanje vrednosti*: Kaldor-Hicksovo načelo tako pravi, da projekt sprejmemo, če je sedanja vrednost dobrobiti večja od sedanje vrednosti stroškov (Munger, 2000). Tu pa se pojavi vprašanje določitve primerne *diskontne stopnje*, ki jo v ta namen uporabimo, saj z njo lahko vplivamo na izid enačbe. Čista sedanja vrednost projektov, kjer tokovi dobrobiti in stroškov časovno niso med seboj usklajeni, je namreč odvisna od višine diskontne stopnje. Tudi zato je *analiza občutljivosti* kazalnikov, ki se najpogosteje uporabljajo za oceno primernosti vlaganj v informacijsko varnost, tj. čiste sedanje vrednosti (NPV), donosnosti

vlaganj (ROI) in notranje stopnje donosnosti (IRR), za spremembe posameznih ocen in predpostavk nujni sklepni del vsake analize stroškov in dobrobiti vlaganj v informacijsko varnost.

4 Izdelava modela optimalnega obsega vlaganja v informacijsko varnost

Za iskanje optimalnega obsega vlaganja v informacijsko varnost smo uporabili kvantitativni model, ki ga je razvil Bojanc (2010). V modelu se za vsako informacijsko sredstvo določijo ter kvantitativno ovrednotijo ranljivosti in grožnje, ki so povezane s tem sredstvom, ter ukrepi, ki ta tveganja zmanjšujejo. Model analize tveganja z varnostnimi ukrepi je prikazan na sliki 2. V njem povzročitelji groženj izvajajo *grožnje (T)* oziroma napade na sistem. Napadi so usmerjeni na *ranljivost* informacijskega sredstva. Uspešno izvedeni napadi za podjetje pomenijo *izgubo (L)*. Pred napadi se podjetje zavaruje s *preventivnimi ukrepi* (s_p), ki zmanjšujejo *verjetnost za varnostni incident (ρ)*, ter *korektivnimi* (s_k) in *detekcijskimi ukrepi* (s_d), ki zmanjšujejo nastalo izgubo.

4.1 Opredelitev parametrov modela

4.1.1 Grožnje, ranljivost in varnostni ukrepi

Verjetnost grožnje (T) opredelimo kot verjetnost, da se zgodi dogodek, ki ima neželene učinke na informacijska sredstva. Na verjetnost grožnje vpliva veliko dejavnikov, kot na primer, kolikšna je vrednost informacijskih sredstev podjetja za napadalca, viri, ki jih ima napadalec na voljo, ali je informacija o stopnji varnosti v podjetju na voljo napadalcu in podobno.

Informacijska sredstva so ranljiva, grožnje pa lahko to njihovo ranljivost zlorabijo. *Ranljivost sredstva (v)* zato opredelimo kot verjetnost, da bo grožnja, usmerjena na neko informacijsko sredstvo, uspešna.

Podjetje tveganja informacijske varnosti zmanjšuje z vlaganjem v *varnostne ukrepe (s)*. Lahko izbira med *preventivni varnostni ukrepi* (s_p), ki zmanjšujejo verjetnost varnostnega incidenta, *korektivnimi varnostnimi ukrepi* (s_k), ki zmanjšujejo izgubo ob varnostnem incidentu, in *detekcijskimi varnostnimi ukrepi* (s_d), ki zmanjšujejo čas za odkritje incidenta ter omogočijo pridobitev informacije o grožnjah. Vlaganje v varnostni ukrep je na splošno opredeljeno s *ceno ukrepa (C)* in *produktivnostjo ukrepa (α)*.

$$s = s(C, \alpha) \tag{4}$$

Cena ukrepa (C) je denarna naložba v varnostni ukrep, ki vsebuje vse izdatke, povezane z uvedbo varnostnega ukrepa, *produktivnost varnostnega ukrepa (α)* pa pomeni vpliv varnostnega ukrepa na zmanjšanje tveganja. Zbirka mogočih groženj se neprestano spreminja in je podjetjem le delno znana (ISO 13335-1, 2004), zato produktivnost zaradi vedno novih groženj s časom konveksno pada, če ni dodatnih vlaganj v varnostne ukrepe.

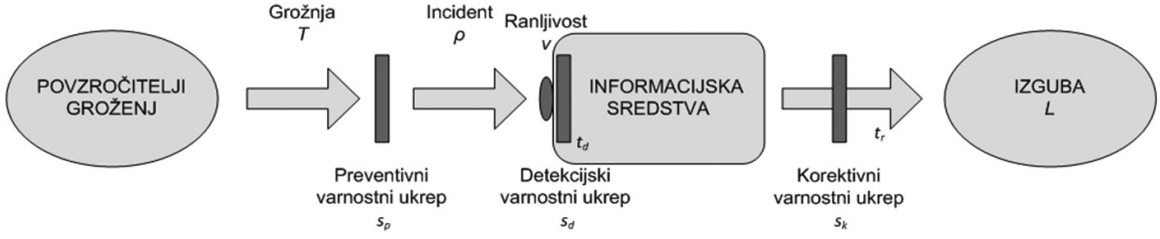
4.1.2 Verjetnost varnostnega incidenta

Nekateri dogodki, ki imajo neželene učinke na informacijska sredstva, so za povzročitelja grožnje uspešni in povzročijo, da se v podjetju zgodi *varnostni incident*. Verjetnost, da bo izvedena grožnja uspešna, oziroma *verjetnost varnostnega incidenta ρ(t)* je odvisna od *verjetnosti grožnje (T)* in *ranljivosti sredstva (v)*. V skrajnih primerih je tako verjetnost varnostnega incidenta $\rho(t) = 0$, če ni nobenega napada (verjetnost grožnje $T = 0$). Enako je verjetnost varnostnega incidenta $\rho(t) = 0$, če informacijski sistem ni ranljiv (ranljivost sredstva $v = 0$). Če verjetnost varnostnega incidenta $\rho(t)$ ni enaka nič, pa se ta lahko zmanjša z uvedbo *preventivnega varnostnega ukrepa* (s_p), ki zmanjšuje ranljivost sredstev *(v)*.

Povzamemo lahko, da verjetnost grožnje (*T*) in ranljivost sredstev (*v*) povečujeta verjetnost varnostnega incidenta (*ρ*), preventivni varnostni ukrep (s_p) pa to verjetnost zmanjšuje. Funkcijo verjetnosti varnostnega incidenta (*ρ*), ki jo navajajo in uporabljajo drugi avtorji (Matsuura, 2008: 2; Gordon in Loeb; 2002b; Bojanc, 2010), lahko zapišemo.

$$\rho(T, v, C_p) = T \cdot v^{\alpha_p C_p + 1} \tag{5}$$

Slika 2: **Model analize tveganja**



Vir: Bojanc, R. Modeli zagotavljanja varnosti v poslovnih informacijskih sistemih, 2010, str. 114.

4.1.3 Izguba ob nastanku varnostnega incidenta

Če se varnostni incident zgodi, podjetje utrpi *izgubo (L)*. Nekatere izgube nastanejo *takoj ob incidentu* ($L_{takojšnje}$), druge pa so *posredne izgube* ($L_{posredne}$), ki imajo lahko dolgoročne posledice. Takojšne izgube ($L_{takojšnje}$) nastanejo tako zaradi zamenjave opreme in popravil, pa tudi zaradi izgubljenih prihodkov, zmanjšane produktivnosti podjetja in zaradi nezmožnosti spoštovanja zakonskih predpisov ali pogodbenih obveznosti.

Nekatere vrste izgub so odvisne od *časa nedelovanja informacijskega sistema* (t_{NA}). Čas nedelovanja je odvisen od *časa detekcije* (t_d), v katerem se odkrije, da se je incident zgodil, in *časa popravila* (t_r), ki je potreben, da se delovanje sistema ponovno vzpostavi. Glede na odvisnost od časa popravila (t_r) in časa detekcije (t_d) lahko izgubo zapišemo:

$$L = L_1 t_r + L_2 t_d + L_3 \tag{6}$$

pri čemer je L_1 izguba, ki je odvisna od dolžine časa popravila (t_r), L_2 izguba, ki je odvisna od trajanja časa detekcije (t_d), L_3 pa izguba, ki nastane neodvisno od časa nedelovanja informacijskega sistema (t_{NA}).

Izgubo, ki nastane zaradi varnostnih incidentov, pa podjetje lahko zmanjša z vlaganjem v korektivni varnostni ukrep (s_k) in/ali v detekcijski varnostni ukrep (s_d). *Korektivni varnostni ukrepi* (s_k) zmanjšujejo čas popravila (t_r), s tem se zato zmanjša čas nedelovanja informacijskega sistema (t_{NA}), kar vodi v zmanjšanje izgube *(L)*, ki jo ima podjetje ob nastanku varnostnega incidenta. Čas popravila (t_r) opišemo s funkcijo, ki je padajoča in konveksna; če je cena varnostnega ukrepa *(C)* neskončna (v varnostne ukrepe vlagamo neskončna sredstva), čas popravila (t_r) limitira proti nič. Funkcija, ki ustreza tem pogojem, je zato (Bojanc, 2010):

$$t_r = t_r^0 e^{-\alpha_k C_k} \tag{7}$$

pri čemer je t_r^0 čas popravila brez uvedenega varnostnega ukrepa.

Tudi za *čas detekcije* (t_d) lahko veljajo enaki robni pogoji kot za čas popravila (t_r) ob vlaganju v korektivni ukrep (s_k), le da govorimo o vplivu vlaganja v detekcijski ukrep (s_d). Funkcija, ki ustreza tem robnim pogojem, je (Bojanc, 2010):

$$t_d = t_d^0 e^{-\alpha_d C_d} \tag{8}$$

pri čemer je *var* čas zaznave incidenta brez uvedenega varnostnega ukrepa. Ob uvedenem korektivnem ukrepu in ob upoštevanju (7) lahko izgubo zaradi varnostnih incidentov (6) zapišemo:

$$L = L_1 \cdot t_r^0 e^{-\alpha_k C_k} + L_2 \cdot t_d + L_3 \tag{9}$$

Ob uvedenem detekcijskem ukrepu in ob upoštevanju (8) pa izgubo zaradi incidentov (6) zapišemo kot:

$$L = L_1 \cdot t_r + L_2 \cdot t_d^0 e^{-\alpha_d C_d} + L_3 \tag{10}$$

4.1.4 Varnostno tveganje

Na podlagi ocenjene verjetnosti varnostnega incidenta (ρ) in izgubo *(L)* lahko izračunamo *varnostno tveganje (R):*

$$R = \rho \cdot L \tag{11}$$

Tveganje *(R)* pomeni pričakovano izgubo zaradi nastanka varnostnega incidenta, ki jo enako kot *L* merimo v enakih denarnih enotah. Če upoštevamo funkciji verjetnost incidenta ρ (5) in izgube *L* (9 in 10), dobimo:

$$R = T \cdot v^{\alpha_p C_p + 1} \left[L_1 \cdot t_r^0 \cdot e^{-\alpha_k C_k} + L_2 \cdot t_d^0 \cdot e^{-\alpha_d C_d} + L_3 - I \right] \tag{12}$$

4.2 Model optimalnega obsega vlaganja v varnostni ukrep

Za oceno ekonomske upravičenosti uvedbe varnostnega ukrepa smo izračunali kazalnike donosnosti vlaganja (ROI), čiste sedanje vrednosti (NPV) in notranje stopnje donosnosti (IRR), ki so najpogosteje uporabljeni kazalniki v praksi (CSI, 2009).

4.2.1 Donosnost vlaganja

Donosnost vlaganja (ROI) primerja koristi vlaganj v varnostni ukrep s stroški *(C)*:

$$ROI = \frac{B - C}{C} \tag{13}$$

Pozitivna vrednost *ROI* pomeni, da je vlaganje ekonomsko upravičeno. Koristi od vlaganj v varnostni ukrep *(B)* so enake zmanjšanju tveganja zaradi uvedbe ukrepa. Tako lahko zapišemo:

$$B = R_o - R(C) - \delta + \mu \tag{14}$$

pri čemer so:

- R_0 varnostno tveganje pred uvedbo varnostnega ukrepa,
- *R(C)* varnostno tveganje po uvedbi varnostnega ukrepa,
- δ negativni vpliv uvedenega ukrepa na poslovanje. Pričakujemo, da uvedba večje stopnje varnosti zmanjšuje funkcionalnosti sistema, kar vpliva na produktivnost in poslovanje,
- μ posredni pozitiven učinek uvedbe ukrepa (na primer večji ugled in status, samozavest, izpolnjevanje zakonskih obveznosti, …).

Če v (13) vstavimo (14), dobimo:

$$ROI = \frac{R_o - R(C) - \delta + \mu - C}{C} \tag{15}$$

Izračun *ROI* se lahko prilagodi različnim obravnavam tveganja. Če se varnostno tveganje odpravlja (zmanjšuje) z vlaganjem v *preventivni varnostni ukrep* (s_p), lahko za ROI (15) zapišemo:

$$ROI = \frac{T \cdot v(1 - v^{\alpha_p C_p}) \cdot L - \delta + \mu - C_p}{C_p} \tag{16}$$

Če pa se to tveganja odpravlja z vlaganjem v *korektivni varnostni ukrep* (s_k), lahko za ROI (15) zapišemo:

$$ROI = \frac{TvL_1 t_r^0 (1 - e^{-\alpha_k C_k}) - \delta + \mu - C_k}{C_k} \tag{17}$$

Tveganje lahko zmanjšamo tudi z vlaganjem v *detekcijski varnostni ukrep* (s_d) in tako ROI (15) zapišemo kot:

$$ROI = \frac{TvL_2 t_d^0 (1 - e^{-\alpha_d C_d}) - \delta + \mu - C_d}{C_d} \tag{18}$$

4.2.2 Čista sedanja vrednost in notranja stopnja donosnosti

Za dolgoročnejša vlaganja v informacijsko varnost je primernejša uporaba *čiste sedanje vrednosti (NPV)*, pri kateri se upošteva tudi vrednost denarja v času, ki ga kazalnik *ROI* (13) ne upošteva:

$$NPV = \sum_{t=0}^{n} \frac{B_t - C_t}{(1+k)^t} \tag{19}$$

Pri tem je *k* diskontna stopnja, *n* pa časovno obdobje. *NPV* je merjen v denarnih enotah, vlaganje pa je ekonomsko upravičeno, če je *NPV = 0* ali večje od nič. Le tako namreč sredstva, ki so vložena v projekt, prinesejo vsaj zahtevano donosnost *(NPV = 0)* ali donosnost, ki je višja od zahtevane *(NPV > 0)*.

Kolikšna je dejanska stopnja donosnosti projekta, ugotovimo s pomočjo *notranje stopnje donosnosti (IRR)*. Ta je enaka tisti diskontni stopnji, pri kateri je *NPV = 0* oziroma pri kateri se sedanja vrednost prejemkov in sedanja vrednost izdatkov izenačita.

$$\sum_{t=0}^{n} \frac{B_t - C_t}{(1+IRR)^t} = 0 \tag{20}$$

Pri primerjavi dveh ali več alternativnih varnostnih rešitev pa je pogosto treba upoštevati več kazalnikov, ne samo enega, saj lahko posamezni kazalniki dajejo prednost različnim rešitvam. *Ekonomsko optimalen varnostni ukrep* (S_{eko}) je torej tisti, ki ima med izbranimi varnostnimi rešitvami največje vrednosti za *ROI, NPV* in *IRR* (Bojanc in Jerman - Blažič, 2008).

$$S_{eko} = S\big|_{\max(ROI),\max(NPV),\max(IRR)} \tag{21}$$

Zavedati se je treba, da kazalniki med seboj niso vedno usklajeni. V takih primerih je treba pri izbiri ustreznega varnostnega ukrepa upoštevati še druge parametre, včasih tudi subjektivne.

5 Empirična preveritev modela

Predstavljen matematični model za oceno optimalnega vlaganja v informacijsko varnost smo jeseni 2009 s pomočjo srednje velikega slovenskega podjetja, ki deluje na področju informacijske tehnologije, tudi praktično preizkusili. Podjetju, ki ima 40 zaposlenih, se je v tem času iztekala naročnina za protivirusni program. Želeli so preveriti, ali naj obdržijo obstoječi protivirusni program in podaljšajo naročnino ali pa naj se odločijo za katero drugo varnostno rešitev. S pomočjo modela in podatkov, ki smo jih pridobili iz različnih virov (javni podatki o podjetju, interni podatki podjetja, seznam informacijskih sredstev, ocena tveganja idr.), smo preverili ekonomsko upravičenost različnih varnostnih rešitev. Ker bi bilo navajanje izračunov za vse ukrepe preobsežno za ta prispevek, tu prikazujemo uporabo modela le na primeru ocene upravičenosti vlaganja v podaljšanje naročnine za obstoječi protivirusni program.[2]

Vsi zaposleni pri delu dnevno uporabljajo računalniško opremo, zato okužba z virusom lahko vpliva na vse poslovne procese. V tabeli 1 so prikazani ključni procesi v podjetju in želena stopnja varnosti za vsak proces.

Tabela 1: **Prikaz ključnih poslovnih procesov in želene stopnje varnosti za vsak proces**

Poslovni proces	Želena stopnja varnosti
razvoj projektov po naročilu	visoka
razvoj internih projektov	srednja
opravljanje storitev za zunanje stranke	visoka
skrbništvo nad projekti po naročilu	visoka
skrbništvo nad projekti za neznanega kupca	visoka
podporni proces prodaja	srednja
podporni proces nabava	nizka
podporni proces zagotavljanje delovanja infrastrukture	visoka

Vir: Bojanc, R. Modeli zagotavljanja varnosti v poslovnih informacijskih sistemih, 2010, str.153.

[2] Celoviti izračuni za različne varnostne rešitve skupaj z obsežnimi pojasnili so objavljeni v Bojanc (2010).

Zaposleni se lahko z računalniškim virusom okužijo na različne načine: lahko pri prenosu okuženih datotek prek spleta, pri ogledu spletnih strani z zlonamerno kodo, pri sprejemu e-pošte z okuženo datoteko in prek programov za takojšnje sporočanje (angl. *instant messaging*). Ker je podjetje želelo proučiti obstoječo protivirusno zaščito, smo pri uporabi modela privzeli stanje, da trenutno ni uvedena nobena zaščita pred tveganjem okužbe z računalniškim virusom, in smo kot mogoč ukrep privzeli sedanjo rešitev.

Podjetje je ocenilo pogostost prejema okuženih datotek na enkrat na teden (*T*) in da bi glede na trenutno ozaveščenost zaposlenih in v okolju brez protivirusne zaščite virus z okuženo datoteko aktivirali dve tretjini zaposlenih (*v*). Zaradi okužbe z virusom sicer ni treba zamenjati opreme, zato stroška zamenjave opreme ni. Čas nedelovanja sistema je ocenjen na 10 ur (t_{NA}): podjetje potrebuje 2 uri, da se okužba ugotovi (t_d^0), ter 8 ur, da se odpravijo posledice incidenta (čiščenje virusne okužbe in morebitna povrnitev okuženih dokumentov iz varnostnih kopij). Posledice bi odpravila dva sistemska administratorja, katerih bruto plača znaša 11,56 € na uro (*p*). Ocenjeno je, da okužba z virusom bistveno ne vpliva na prihodek podjetja. Ob upoštevanju vseh navedenih podatkov in da bi se zaradi okuženosti računalniške opreme zmanjšala produktivnost desetine zaposlenih za 25 %, je varnostno tveganje (*R*) tako ocenjeno na 35,15 € na dan.

Če bi se podjetje odločilo za uvedbo osnovne protivirusne zaščite za 40 delovnih postaj, ki ne zahteva letnega podaljševanja, bi ga nakup licenc stal 1.350 € (C_p), namestitev in preizkušanje pa še dodatnih 416 € (C_i). Skupno začetno vlaganje bi tako znašalo 1.766 €, k čemur pa bi bilo treba vsako leto prišteti še stroške vzdrževanja v višini 693 € (C_m). Produktivnost ukrepa (*α*) je izračunana s pomočjo podatkov o učinkovitosti rešitve (*u*), ki jih objavlja *The Independent IT-Security Institute* v AV-Testu, in določa, za koliko % se z uvedbo osnovne protivirusne zaščite zmanjša ranljivost sistema. Učinkovitost za to rešitev je po AV-Testu znašala 65,5 %, kar pomeni, da ima podjetje od uvedbe te rešitve koristi v višini 2.391 € na leto. Ker se je podjetje ob sprejemanju odločitve o podaljšanju osnovne protivirusne zaščite lahko zadolžilo po 2,7-odstotni letni obrestni meri, bi donosnost vlaganja v to rešitev znašala 111 %, čista sedanja vrednost (NPV) 4.591 € in notranja stopnja donosnosti (IRR) 89 %.

6 Sklepna ugotovitev

Ocena optimalnega obsega vlaganj v informacijsko varnost in izbira ustrezne varnostne zaščite zahtevata, da podjetja potrebo po informacijski varnosti tudi kvantitativno ovrednotijo. Kvantitativno je treba ovrednotiti ranljivost in grožnje, ki so povezane z nekim informacijskim sredstvom, ter ukrepe, ki ta tveganja zmanjšujejo. Zgolj tako lahko vlaganja v informacijsko varnost presodimo tudi z vidika njihove ekonomske upravičenosti.

Zavedati pa se je treba, da je ekonomski pristop ocenjevanja optimalnih vlaganj v informacijsko varnost obsežen in zamuden projekt ter predvsem za mala podjetja pogosto prezahteven ter stroškovno neupravičen. Zahteva namreč poglobljeno analizo in vrednotenje informacijskih sredstev in z njimi povezanih groženj, posledic nedelovanja informacijske tehnologije, verjetnosti uspešno izvedenega napada, učinkovitosti izvajanja varnostne prakse ter oceno stroškov in pridobitev, ki so posledica vlaganj v informacijsko varnost. Veliko podjetij nima ustreznega znanja, pa tudi ne dovolj sredstev, da bi lahko to oceno izdelala. Ekonomskega pristopa ocenjevanja optimalnega obsega vlaganj se bodo tako lotila le tista podjetja, pri katerih sta verjetnost grožnje in ocenjena izguba ob uspešno izvedenem napadu zelo veliki, hkrati pa cena ukrepa pomeni pomemben delež sredstev, s katerimi podjetje razpolaga. Zaradi tega je nujno treba znižati stroške uporabe modela ocene optimalnega obsega vlaganj v informacijsko varnost, da bi se povečala njegova uporabnost. Ker se zaradi poenostavitve uporabe modela ne smeta zmanjšati njegova napovedna moč in natančnost, bo vprašanje oblikovanja modela določitve optimalnega obsega vlaganj v informacijsko varnost še naprej pomemben izziv za strokovnjake informacijske in ekonomske znanosti.

Literatura in viri

Bojanc, R., in Jerman - Blažič, B. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management*, 28, 413–422.

Bojanc, R. (2010). *Modeli zagotavljanja varnosti v poslovnih informacijskih sistemih*. Doktorska disertacija. Ljubljana: Ekonomska fakulteta Univerze v Ljubljani.

Brent, R. J. (2007). *Applied cost-benefit analysis.* Cheltenham: Edward Elgar Publishing.

Computer Emergency Response Team (CERT). (2008). *CERT Statistics 1988–2008*. Dosegljivo na: http://www.cert.org/stats (13. 9. 2009).

Computer Security Institute (CSI). (2009). *CSI Survey 2009*. The 14th Annual Computer Crime and Security Survey. Dosegljivo na: http://www.gocsi.com/survey (2. 3. 2010).

Cremonini, M., in Nizovtsev, D. (2006). *Understanding and Influencing Attackers' Decisions: Implications for Security Investment Strategies*. Workshop on the Economics of Information Security (WEIS 2006). Dosegljivo na: http://

weis2006.econinfosec.org/prog.html (15. 11. 2006).

Deloitte (2004). *Cracking the IT value code*. Deloitte Research Report, London.

Dhillon, G., in Backhouse, J. (2000). Information System Security Management in the New Millennium. *Communications of the ACM*, 43(7), 125–128.

Geer, D. (2004a, 20. oktober). *Q&A: Dan Geer on security of information when economics matters. SearchDataManagement.com*. Dosegljivo na: http://searchdatamanagement.techtarget.com/news/interview/0,289202,sid91_gci1139680,00.html (4. 12. 2007).

Gordon, A. L., in Loeb, P. M. (2002a). Return on Information Security Investments: Myths vs. Reality. *Strategic Finance*, november 2002, 26–31.

Gordon, A. L., in Loeb, P. M. (2002b). The Economics of Information Security Investment. *Communications of the ACM*, 5(4), 438–457.

Gordon, A. L., in Loeb, P. M. (2005). *Managing Cybersecurity Resources: A Cost-Benefit Analysis*, New York: McGraw Hill.

Hanley, N., in Spash, C. L. (1993). *Cost-benefit analysis and the environment*. Edward Elgar Publishing, England.

Huang, C. D., Hu, Q., in Behara, S. R. (2006). *Economics of Information Security Investment in the Case of Simultaneous Attacks*. Workshop on the Economics of Information Security (WEIS 2006). Dosegljivo na: http://weis2006.econinfosec.org/prog.html (15. 11. 2006).

International Organization for Standardization (ISO). (2004). *ISO/IEC 13335-1:2004. Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management*. Geneva: International Organization for Standardization (ISO).

International Organization for Standardization (ISO). (2009). *ISO/IEC Guide 73:2009. Risk management – Vocabulary*. Geneva: International Organization for Standardization (ISO).

Kaplan, R. (2007). *A Matter of Trust*. V H. F. Tipton & M. Krause (ur.). Information Security Management Handbook, 6th edition (str. 295–310). Boca Raton, Florida: Auerbach Publications.

Longstaff, T. A., Chittister, C., Pethia, R., in Haimes, Y. Y. (2000). Are We Forgetting the Risks of Information Technology? *Computer*, 33(12), 43–51.

Matsuura, K. (2008). *Productivity Space of Information Security in an Extension of the Gordon-Loeb's Investment Model*. Workshop on the Economics of Information Security (WEIS 2008). Dosegljivo na: http://weis2008.econinfosec.org/program.htm (2. 9. 2008).

Miller, D. H., in D. Patassini (2005). *Beyond Benefit Cost Analysis-Accounting for Non-Market Values in Planning Evaluation*. Aldershot: Ashgate.

Munger, M. C. (2000). *Analyzing Policy*. New York: W.W. Norton.

National Institute of Standards and Technology (NIST). (2004). *Federal Information Processing Standards (FIPS) publication 199. Standards for Security Categorization of Federal Information and Information Systems*. Dosegljivo na: http://csrc.nist.gov/publications/PubsFIPS.html (16. 4. 2009).

Sandhu, R. (2003). Good-Enough Sercurity: Toward a Pragmatic Business-Driven Discipline. *IEEE Internet Computing*, 5(3), 66–68.

Schneier, B. (2003). *Beyond Fear: Think Sensibly about Security in an Uncertain World*. New York: Copernicus Books.

Schneier, B. (2004). *Secrets & Lies, Digital Security in a Networked World*. New York: Wiley Publishing.

Sonnenreich, W., Albanese, J., in Stout, B. (2006). Return On Security Investment (ROSI) – A Practical Quantitative Model. *Journal of Research and Practice in Information Technology*, 38(1), 45–56.

Soo Hoo, K. J. (2000). *How Much Is Enough? A Risk-Management Approach To Computer Security*. Palo Alto, CA: Stanford University.

Sugden, R., Williams, A. H. (1978). *The principles of practical cost-benefit analysis*. Oxford University Press.

Swire, P. P. (2001, 24. september). *What Should be Hidden and Open in Computer Security: Lessons from Deception, the Art of War, Law, and Economic Theory*. The Computer Research Repository (CoRR). Dosegljivo na: http://arxiv.org/abs/cs.CR/0109089 (17. 2. 2009).

Tordoff, P. (2006). UK Information Security Breaches Survey. *ENISA quarterly*, 2(2). 15–17.

Whitman, E. M. (2003). Enemy at the Gate: Threats to Information Security. *Communications of the ACM*, 46(8), 91–95.

Young, A., in Yung, M. (1996). Cryptovirology: Extortion-based security threats and countermeasures. The IEEE Symposium on Security and Privacy (str. 129–140). Washinghton, DC: IEEE Computer Society.