Doseganje strateških ciljev policije z boljšim upravljanjem investicij v informatiko

Borut Jereb
Univerza v Mariboru, Fakulteta za logistiko, Mariborska c. 7, 3000 Celje
borut.jereb@fl.uni-mb.si

Izvleček

Obstoječi model upravljanja informatike policije temelji na obravnavi tehničnih in tehnoloških izzivov. Pri tem je prezrt novejši, poslovno orientiran vidik upravljanja, ki temelji na učinkovitem upravljanju investicij v informacijska sredstva in s temi investicijami povezanimi tveganji. V informacijska sredstva in v njihov zaščito ni mogoče ustrezno investirati brez vedenja o njihovi vrednosti, ki jih imajo pri doseganju poslovnih ciljev policije. V prispevku dokazujemo, da je potrebno in mogoče z učinkovitim upravljanjem investicij v informacijska sredstva zagotavljati doseganje poslovnih ciljev policije. To dosežemo prek predlagane razširitve informacijskega varnostnega modela, ki ga predstavlja obstoječa informacijska varnostna politika. Tudi sama implementacija dopolnjenega modela zahteva investicijo – tokrat v dopolnitev organizacije upravljavske piramide in v spremembo obstoječega poslovanja policije. Pri tem gre predvsem za investicijo v človeški kapital in za vzpostavitev okolja, ki omogoča uspešno realizacijo sprememb. S predlaganim modelom, pri katerem v ospredje upravljanja informatike postavimo njihove poslovne vrednosti, ki jih imajo pri doseganju strateških ciljev, so v ZDA na primeru, ki ga povzemamo v prispevku, dokazali izboljšanje ključnih kazalnikov delovanja njihovega oddelka policije.
Ključne besede: upravljanje informatike, investicije v informacijska sredstva, informacijska varnost, informacijska varnostna politika, upravljanje vrednosti, upravljanje tveganj.

Abstract

Achieving the Strategic Goals of Police Service by Improved Management of Investments in Information Technology

The existing model of Police Information Technology (IT) management is based on overcoming technical and technological challenges. At the same time the modern, business-oriented aspect of IT management that is based on effective investments and risk management in IT is largely ignored. Not understanding the value of individual information resources in achieving the business objectives and goals of the Police directly results in an inability to properly invest in them. The paper aims to show that it is necessary and feasible to assure the business objectives of the Police with effective investments management in IT. This can be achieved by proposing an extension of the security model, represented by the existing Information Security Policy. The implementation of the revised model calls for investments, particularly in supplementing the organization of management pyramid and in a modification of the existing performance of the business. The investment in human resources and the establishment of an environment which ensures an effective realization of modifications is of utmost importance. In the USA, the proposed model which is summarized in this paper has been implemented and has shown that by exposing the values that help accomplish strategic goals the key indicators that influence the efficiency of a particular police department can be improved.
Key words: IT management, IT investments, information security, information security policy, value management, risk management.

1 OPREDELITEV PROBLEMA

V vsaki organizaciji je osnovna vloga informatike podpora, vzdrževanje in razvoj poslovnih strategij in ciljev organizacije. Pri tem se pri posameznih poslovnih procesih, ciljih, tveganjih, investicijah in poslovnih varnostnih ciljih srečujemo z informacijskimi procesi, cilji, tveganji, investicijami in informacijskimi varnostnimi cilji. Pri tem praviloma poslovni varnostni cilji definirajo informacijske varnostne cilje. Za informacijska tveganja velja, da jih upravljamo v okviru poslovnih tveganj na taktični in predvsem na strateški ravni. Investicije v informacijska sredstva so podvržena upravljanju v okviru portfelja vseh poslovnih investicij. To je pristop pri upravljanju informatike, ki vključuje potrebe odjemalcev že v osnovi in zagotavlja upoštevanje poslovnih zahtev in pričakovanj zunanjih in notranjih deležnikov organizacije [9].

Vse, kar imamo na razpolago za izvajanje informatike in informacijskih procesov, so informacijska

sredstva. To so informacije, aplikacije, informacijska infrastruktura in ljudje, ki so vključeni v informacijske procese. Ta sredstva so tisto, s čimer imamo opravka v informatiki. Upravljamo jih, investiramo vanje in jih tudi prek investicij varujemo, da bi zagotovili zahtevano razpoložljivost, celovitost in zaupnost informacij. Omenjena sredstva in tri zahteve so osnovni parametri informacijske varnosti. So temelj sodobnega upravljanja informatike, kar običajno izrazimo prek dokumenta informacijske varnostne politike, ki narekuje cilje in načine za doseganje teh ciljev na področju informatike. [10]

Investicije omogočajo vzdrževanje obstoječega poslovanja, njegovo povečanje ali spremembo [8]. V večini primerov je skupni imenovalec investicij to, da pomeni velik ali celo pretežni del poslovne investicije investicija v informacijska sredstva in spremljajočo informacijsko varnost, saj se v večini primerov informatika izrazi kot poslovno kritična komponenta. Zato je pomen konkretnih poslovnih koristi podjetja ob tovrstnih investicijah tako velik. Še več: pomembno je upravljanje investicije v njenem celotnem življenjskem ciklu v okviru upravljanja poslovnih investicij – tako investicije v informatiko naj ne bi obravnavali kot samostojno celoto, temveč le kot investicijo, vpeto v mrežo drugih poslovnih investicij. Vsaka investicija v informatiko in informacijsko varnost mora imeti jasno poslovno korist, mora prispevati k poslovnim ciljem podjetja in mora biti ocenjena skozi prizmo doprinosa k poslovnim ciljem. Imeti mora svojo upravičenost in pričakovano razmerje med vložkom in koristnostjo. Povedano drugače: podjetja dosegajo svojo želeno in pričakovano poslovno korist predvsem z izbiro pravih investicij ter z učinkovitim upravljanjem izbranih investicij – tudi v informacijska sredstva. [11] [13]

Poslovno vrednost je pri storitvah, še posebno v javnem sektorju, težje predstaviti, ker je ocenjevanje uspešnosti investicij v informatiki v javnem sektorju težje, saj gre pri javnih organizacijah za poudarjeno večplastnost ocenjevanja, kar prispeva k povečani kompleksnosti ocenjevanja. Vendar je mogoče in potrebno te vrednosti definirati za uspešno upravljanje investicij v informatiko – tudi pri policiji. Na podlagi siceršnjih znanih nalog policije, njenih strateških ciljev in siceršnjih poslovnih vrednosti in/ali vrednot, ki so v policiji splošno sprejete in znane na vseh ravneh upravljanja, je mogoče izračunati poslovne vrednosti njenih informacijskih sredstev.

Pri tem trčimo na izziv kompleksnosti upravljanja informacijske varnosti, ki je tesno povezana z uspešnostjo upravljanja investicij v varovanje informacijskih sredstev [14]. Vrednosti informacijskih sredstev ne morejo določiti tehnični strokovnjaki sami, saj so vrednosti, ne glede na to, kako so te vrednosti izražene in s čim, domena strokovnjakov, ki so odgovorni za poslovanje policije. Pri tem je ključno spoznanje, da je informacijska varnost ne samo tehnično-tehnološki izziv, temveč tudi in predvsem poslovni [20] [12]. Brez tega spoznanja informacijska podpora delu policije ne more biti učinkovita in uspešna pri doseganju njenih strateških ciljev, kar bomo skušali dokazati v nadaljevanju.

V informacijsko varnostno politiko moramo vnesti dimenzijo poslovnosti, da prek ključnih parametrov informacijske varnosti – razpoložljivosti, celovitosti in zaupnosti – izražamo in postavljamo poslovne zahteve, ki jih mora izpolnjevati informatika [10]. To zahteva poznavanje poslovne vrednosti informacijskih sredstev. Te vrednosti so podlaga za odločanje o tem, koliko investirati vanje in kako ter koliko investirati v njihovo zaščito [7].

V prispevku s pomočjo indukcije in dedukcije, analize in sinteze ter na primeru realnega dogodka dokazujemo, da je policija trenutno vsaj formalno soočena samo s tehničnim vidikom varovanja informacij. Tega bo treba znati nadgraditi tako, da bodo z na novo osmišljeno informacijsko varnostjo dosegli poslovne cilje, ki so zapisani v dokumentih, kot so Temeljne usmeritve za pripravo srednjeročnega načrta razvoja in dela policije v obdobju 2008–2012 [17], Usmeritve in obvezna navodila za pripravo letnega načrta policije v letu 2012 [19] in Srednjeročni načrt razvoja in dela policije za obdobje 2008–2012 [16].

2 ANALIZA OBSTOJEČEGA STANJA UPRAVLJANJA INFORMACIJSKE VARNOSTI PRI POLICIJI

Pri analizi obstoječega stanja v policiji smo se osredinili samo na javno dostopne dokumente, na podlagi katerih smo sintetizirali obstoječe stanje. Pri tem ne vemo, ali so v pripravi morebitni novi, še neobjavljeni dokumenti, ki bi lahko ovrgli naše predpostavke o trenutnem stanju v policiji. Pri analizi stanja bomo uporabili tudi primer izginotja zaseženih elektronskih nosilcev podatkov. Pri deduktivnem pristopu bomo med drugim uporabili primer uspešnega upravljanja investicij v informacijska sredstva, s ka-

terim so na policijski postaji v ZDA dosegli zastavljene poslovne cilje [5].

Po vseh dostopnih formalnih virih sodeč, je pri policiji njena informacijska varnost v »pasivnem načinu upravljanja«. To pomeni, da so informacijski varnostni inženirji praviloma predvsem tehniki in tehnologi, ki se dnevno srečujejo z nevarnostmi, informacijskimi tveganji in kršitvami, novimi tehnologijami in z njimi povezanimi varnostnimi luknjami ter z drugimi težavami. So v nezavidljivem položaju in kot predstavniki relativno mladega področja so soočeni s pomanjkanjem temeljnih raziskav in orodij, s katerimi bi si pomagali pri izboljševanju informacijske varnosti, tako da bi upoštevali tudi njen poslovni vidik. Zagotavljati morajo skladnost z razdrobljenimi zahtevami, ki jih pred njih postavljajo standardi, okviri za delo in zakonodaja. Pri vsem tem jim verjetno ostane prav malo časa, da bi se pri svojem delu ukvarjali z ugotavljanjem vrednosti, ki jih informacijska tehnologija prinaša v poslovnem pomenu, ter z drugimi inovacijami pri upravljanju informacijskih sredstev.

Kot posledica problema nezadostnih kompetenc, ki jih imajo tehniki in tehnologi za samostojno upravljanje investicij v informacijska sredstva, se kaže zahteva po spremembi upravljavskih praks v informatiki. Prakse, ki so bile še do včeraj aktualne, postajajo premalo kompleksne in nezadostne. Še včeraj namreč nismo investicijam v informatiko namenjali tolikšne pozornosti, kot jo zahteva današnji čas. Videti je, kot da postaja proučevanje uspešnosti investicij v informacijska sredstva osrednja tema, s katero se ukvarjajo ali se bodo ukvarjali vodje informatike v organizacijah. [8]

2.1 Poslovni cilji policije

Pri policiji ne gre iskati poslovnega cilja v razmerju med vloženim denarjem in zaslužkom, ki ga prinese vloženi denar, temveč v temeljnih usmeritvah za delo policije, ki se s časom bistveno ne spreminjajo. Na prvem mestu med najpomembnejšimi strateškimi cilji so preprečevanje, odkrivanje in preiskovanje kriminalitete [17]. V usmeritvah [19] so med pomembnejšimi cilji eksplicitno navedeni zmanjšanje gospodarske in kibernetske kriminalitete, informacijsko povezovanje, analize stanj itn. [19]. Vse to so poslovni cilji policije.

Poleg tega je v temeljnih usmeritvah podana še splošna zahteva, ki pravi [17]: »Izdelajte celovito strategijo ITK (informatika in telekomunikacije) za zagotavljanje optimalne organizacije in vsebine dela.« Gre za zelo splošno zahtevo, brez nakazanih ciljev na ravni informatike ali nakazanih načinov za dosego teh ciljev. Iz teh dokumentov tako ni razbrati neposrednih zahtev za informacijsko varovanje. Ni razbrati, s katerimi informacijskimi sredstvi bomo podprli poslovne zahteve in kako. Ni nakazane povezave med poslovnimi cilji in cilji informatike, ki bi izhajali iz informacijske varnostne politike.

Dokument, ki prehaja iz strateške na operativno raven, je Srednjeročni načrt razvoja in dela policije za obdobje 2008–2012 [16]. V njem je med mnogimi strateškimi cilji in zahtevami mogoče zaznati dovolj natančno določene programe s področja informacijske tehnologije. Med takšnimi so:

1. posodobitev forenzično-informacijske tehnologije,
2. spremembe in dopolnitve informacijskega sistema s področja kriminalitete,
3. prehod na schengenski informacijski sistem druge generacije (SIS II),
4. informacijsko-telekomunikacijska podpora policijskemu delu (mobilni in stacionarni sistem avtomatske prepoznave registrskih tablic – ANPR, sistem avtomatskega lociranja vozil – GPS/AVL, mobilni dostop do podatkov, digitalni radijski sistem za prikrito kriminalistično delovanje, uvedba digitalnega sprejemnika LEO, termovizija idr.),
5. sprejetje strategije informacijsko-telekomunikacijskega sistema policije,
6. izdelava metodologije prikaza podatkov o varnostnih dogodkih v okviru geografskega informacijskega sistema na intranetu policije in izdelava programa za časovno in prostorsko razporejanje policijskih patrulj na podlagi teh podatkov.

Iz tega (nepopolnega) seznama je razbrati, da je – poleg informacijskih rešitev – v igri tudi izdelava strategij in metodologij. Vendar nikjer ni mogoče zaznati, da bi bila eksplicitno navedena zahteva po izdelavi ali pripravi rešitve, strategije ali metodologije tako, da bo v zvezi z informatiko upoštevan tudi poslovni vidik policije.

2.2 Umeščenost urada za informatiko in telekomunikacije v organiziranost policije in njegove ključne naloge

V katalogu informacij javnega značaja policije [20] je mogoče razbrati, da je v sestavi policije tudi Urad za informatiko in telekomunikacije. To je eden od

sedmih organizacijskih enot na ravni generalne policijske uprave. Takšna organiziranost daje področju informatike pričakovano vplivnost.

Pri pregledu nalog, ki jih izvaja urad, sta dve izmed štirih točk [20]:

1. upravlja z informacijskim in telekomunikacijskim sistemom policije;
2. pripravlja, izdeluje in nadzira izvajanje srednjeročnih in letnih načrtov razvoja ter nabave programske in strojne opreme informacijskega in telekomunikacijskega sistema policije ter elektronske opreme in sistemov tehničnega varovanja.

Iz teh nalog je razvidno, da je urad odgovoren za nabavo (to je investicije) in delovanje informacijskih sredstev policije.

Pri podrobnejšem pregledu nalog, ki jih izvaja urad, največkrat zasledimo besedne zveze in pojme, kot jih prikazuje tabela 1. Ob analizi besedila z opisom nalog lahko ugotovimo, da se beseda nabava, ki jo lahko v našem primeru jemljemo kot sopomenko besede investicija, pojavi samo enkrat. Analizirano besedilo je sicer vsebovalo 393 besed, med katerimi jih je 220 različnih. Za ta prispevek so se nam zdele še posebno zanimive besedne zveze:

1. načrtovanje, razvoj, uvajanje in vzdrževanje,
2. standardizacija,
3. strokovna pomoč,
4. zagotavljanje neprekinjenega delovanja,
5. okrevanja po izpadih,
6. zaščita in varovanje,
7. testiranje,
8. upravljanje z varnostnimi dogodki in incidenti.

Besede iz tabele 1 ter zgornjih osem pojmov in besednih zvez nakazujejo predvsem tehnično ali tehnološko usmerjenost pri določanju (in predpostavljamo tudi izvajanju) nalog. Torej imamo pri investicijah opraviti predvsem s tem, da se v policiji trudijo doseči tehnične zahteve in standarde (zagotovo v okviru obstoječega proračuna), pri čemer poslovne vrednosti niso omenjene. Iz nalog je torej razvidno, da se v policiji sprašujejo:

1. Delamo pravilno? Gre za vprašanje arhitekture informacijske tehnologije.
2. Izvajamo informacijske procese dovolj dobro? Pri tem se sprašujemo o kakovosti servisov.

Smiselno bi bilo, da se sprašujejo še o dveh vprašanjih, in sicer:

1. Delamo prave stvari? So investicije pravilne? Pri tem gre za strateška vprašanja.
2. Kolikšne in kakšne so dejanske koristi od investicije? Kolikšne in kakšne so glede na pričakovanja? Gre za vprašanje poslovne koristi.

Tabela 1: **Najpogosteje uporabljene besede pri opisu izvajanja nalog urada za informatiko in telekomunikacije policije, ki jih je zaslediti v informacijah javnega značaja (statistika je izdelana s spletno aplikacijo Textalyzer [22])**

Beseda	Pojavitev	Frekvenca	Rang
sistemov	17	4,3 %	1
upravljanja	15	3,8 %	2
podatkov	14	3,6 %	3
opreme	13	3,3 %	4
načrtovanja	11	2,8 %	5
uvajanja	10	2,5 %	6
policije	10	2,5 %	6
storitev	8	2 %	7
razvoja	8	2 %	7
vzdrževanja	6	1,5 %	8
varovanja	6	1,5 %	8
drugih	5	1,3 %	9
elektronske	4	1 %	10
zaščite	4	1 %	10
informacijskih	4	1 %	10
sodelovanja	3	0,8 %	11
vseh	3	0,8 %	11
tehničnega	3	0,8 %	11
izvajanja	3	0,8 %	11
standardizacije	3	08 %	11

Iz ciljev in nalog urada (ki je odgovoren za izvajanje informacijske politike v policiji) ni razbrati, da bi se njihovo delo pri investicijah v informacijska sredstva vrtelo okrog poslovnih vrednosti – ni zaznati povezave med poslovnimi cilji in investicijami v informatiki. Ta ugotovitev je podobna, kot je bila opisana pri analizi poslovnih ciljev policije, vendar tokrat z diametralno nasprotnega gledišča.

2.3 Informacijska varnostna politika policije

Informacijska varnostna politika policije [18] je najpomembnejši in glavni dokument, na podlagi katerega policija upravlja z informacijskimi sredstvi in tveganji. Z njo vodstvo policije prevzema pooblastila in odgovornosti za upravljanje tveganj (v bistvu varnosti) njenih informacijskih virov. Eksplicitno se pri definiciji njenega namena v drugem členu sklicuje na standardno zagotavljanje razpoložljivosti, celovitosti

in zaupnosti informacij. Pri ciljih v tretjem členu navaja, da je treba:

1. ugotoviti vrednost informacijskih sredstev (ki pa niso predhodno definirana in lahko le sklepamo, da so avtorji dokumenta imeli v mislih aplikacije, infrastrukturo, informacije in ljudi kot tista informacijska sredstva, s katerimi »izvajamo« informatiko) prek analize informacijskih tveganj;
2. ugotoviti in razumeti ranljivosti teh sredstev ter določiti njihovo izpostavljenost tveganjem;
3. v tretji točki tretjega člena dokument preskoči na splošno upravljanje tveganj (kar že samo po sebi vključuje zgornja dva cilja kot potrebne aktivnosti pri upravljanju tveganj – npr. ISO 31000:2009 [3], ISO 31010:2009 [2], ISO/IEC 27005:2011 [4]).

Kot zadnji, četrti, večji cilj eksplicitno navede deset ciljev, med katerimi so (ponovno) navedeni zagotavljanje razpoložljivosti, celovitosti in zaupnosti informacij in še sedem drugih.

Na koncu se dokument sklicuje na osem področnih informacijskih varnostnih politik, ki niso predmet tega prispevka, vendar se iz njihovega imena in namena da sklepati, da se ne nanašajo na kakršne koli poslovne cilje policije.

Informacijska varnostna politika se tako v nobenem delu ne sklicuje na poslovne cilje policije. Poslovni cilji pri upravljanju informatike niso vključeni. Obravnavan je le tehnološki vidik upravljanja. Še manj so poslovni cilji predstavljeni kot temelj, na katerem bi slonelo upravljanje in s katerimi bi bilo prežeto temeljno poslanstvo in upravljanje informatike v policiji.

Pri upravljanju sistema vedno upoštevamo neko temeljno poslanstvo in takšen pristop se bolj ali manj prenaša tudi na upravljanje njegovih podsistemov. Zato verjamemo, da so poslovni cilji pri upravljanju informatike nekako v ozadju, verjetno v različnih primerih sicer upoštevani različno, vendar niso sistemsko vgrajeni v upravljanje informatike. Ali je takšno stanje zadovoljivo? Po stari, vendar še zdaleč ne zastareli metodologiji ugotavljanja zrelosti takšno stanje spada na prvo raven zrelosti [1], na kateri je aktivnost poznana le *de facto* in ne *de jure*. Z drugimi besedami to pomeni, da v policiji ni aktivnosti, ki bi se ukvarjala z investicijami v informacijska sredstva na podlagi poslovne vrednosti, ki jo prinaša informatika. Vsaj uradno ni (raz)poznane nikakršne dejavnosti v zvezi s tem. Tako tudi ne (pre)poznamo tveganj, ki bi jih bilo treba upravljati v povezavi s to dejavnostjo, in ni notranjega nadzora nad njo – seveda govorimo v kontekstu poslovnega vidika upravljanja informatike v policiji.

2.4 Primer: analiza vrednosti odtujenega zaseženega nosilca elektronskih podatkov

Zasežene elektronske naprave so lahko ključne pri doseganju poslovnih ciljev policije. Ob izgubi ali odtujitvi zaseženih nosilcev elektronskih podatkov (npr. diskov iz računalnika) so načeti temeljni poslovni cilji policije, kot sta »preprečevanje, odkrivanje in preiskovanje kriminalitete« ali »povečevanje ugleda policije«. Pri analizi realnega primera [21] so za tematiko tega prispevka zanimiva predvsem dejstva.

1. Zaradi neustreznih prostorov, kjer so shranjene zasežene elektronske naprave in elektronski nosilci podatkov na oddelku za računalniško preiskovanje sektorja kriminalistične policije Policijske uprave Ljubljana, bi bilo treba urediti skladiščni prostor z ustrezno tehnologijo, ki bi služila večji sledljivosti in mobilnosti [15]. Avtorja v nadaljevanju pravilno ugotavljata, da ne gre samo za neustrezne prostore, temveč gre za neustrezne pristope v procesu skladiščenja zaseženih predmetov.
2. Seveda se postavlja vprašanje, ali so zasežene elektronske naprave to, kar spada v okvire informacijske varnostne politike (torej veljajo principi upravljanja, ki veljajo za informacijska sredstva). Odgovor je pritrdilen. Pri zaseženih diskih gre za informacije, ki pomenijo enega od štirih informacijskih sredstev, s katerimi izvajamo informacijske procese [6]. Ta sredstva varujemo in investiramo vanje. Torej mora biti skladiščenje elektronskih naprav in nosilcev elektronskih podatkov urejeno v skladu z informacijsko varnostno politiko policije.
3. Zaradi povečanja količine zaseženih elektronskih naprav in elektronskih nosilcev podatkov sektorja kriminalistične policije PU Ljubljana bo v prihodnje prišlo do logističnih zapletov pri njihovem hranjenju in skladiščenju. Na oddelku se zavedajo, da bo treba nekaj storiti z opravili, povezanimi z njihovim upravljanjem. Takšna opravila so evidentiranje, označevanje, hranjenje, sprejem in vračanje zaseženih elektronskih nosilcev podatkov, povezovanje zaseženih elektronskih nosilcev podatkov s spisi, sledljivost zaseženih elektronskih naprav in elektronskih nosilcev podatkov

od zasega do vrnitve itd. Z drugimi besedami: na oddelku se zavedajo, da bo treba investirati v spremembo poslovanja.

Vprašajmo se, ali se je mogoče tovrstnim problemom izogniti z dopolnitvijo obstoječe informacijske varnostne politike in iz nje izhajajočih področnih navodil ali usmeritev. Odgovor je pritrdilen, če je ta zastavljena tako, da bi se v konkretnem primeru vprašali, kolikšna bi bila poslovna škoda v primeru odtujitve ali izgube elektronskega nosilca podatkov. S strogo tehnično-tehnološkega vidika nas poslovna škoda sploh ne zanima in nimamo pripravljenega, dogovorjenega, splošno sprejetega in predpisanega ogrodja za njeno oceno. Zato je ne moremo »izračunati«. Seveda jo posamezniki slutijo, vendar ta slutnja temelji na subjektivnem odnosu posameznika do nje. Samo slutnja pa je premalo, če želimo vrednosti in tveganja, povezana z vrednostmi, upravljati učinkovito. Podobno kot s tehnološkega je treba upravljati tveganja informacijskih sredstev tudi s poslovnega vidika. Seveda v tem primeru delamo z vrednostmi iz poslovnega sveta in ne tehnološkega.

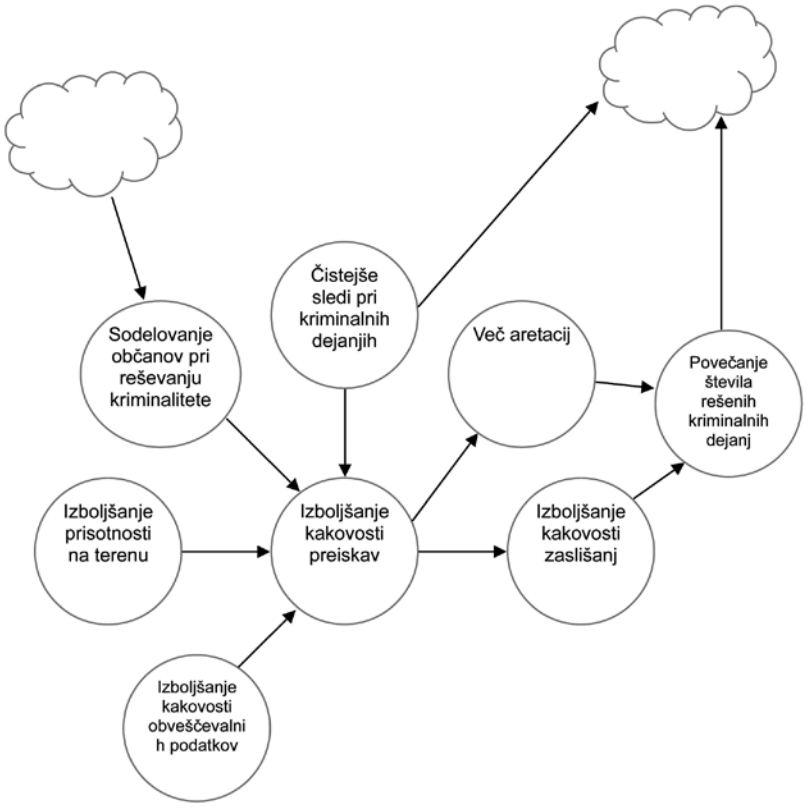
Torej bi morali informacijska varnostna politika in množica dokumentov, ki izhajajo iz nje (področne politike, organizacijska navodila itd.) vsebovati tudi poslovne cilje policije. Če bi bilo tako, bi bilo mnogo manj možnosti, da bi se primeri omenjene odtujitve »izmuznile« sistemskemu pristopu in nas presenetile. Posamezna informacijska sredstva bi imela svojo poslovno vrednost in glede na to vrednost tudi predpisano zaščito. Sedaj, ko se vrednosti vsesplošno ne zavedamo, oziroma ta ni v prvem planu, obstaja večja verjetnost, da sredstva ne bodo ustrezno zaščitena. Ena bodo preveč, druga premalo. Ljudje, ki se ukvarjajo s tehniko, ne morejo vedeti, koliko je treba kaj varovati, če ne upoštevajo poslovnega vidika vrednosti posameznih sredstev.

3 INVESTICIJE V INFORMATIKO NA PODLAGI PRIMERA SREDNJE VELIKE POLICIJSKE POSTAJE V ZDA

Okvir Val IT, ki podaja pristope za uspešno upravljanje investicij v informacijska sredstva [8], je poznan že dolgo. Prve različice tega dokumenta so bile objavljene že leta 2006. Ni pa bilo objavljenih veliko kritičnih analiz o upravljanju tovrstnih investicij. Posebno malo je objavljenih tovrstnih analiz v javnem sektorju. Ena od objavljenih študij investicij v informatiko v javnem sektorju je Val IT Case Study: Value Governance – Police Case Study [5]. V njej je opisano, kako so z osredinjenjem na poslovne cilje v srednje veliki ameriški policijski postaji dosegli zelo dobre rezultate po spremembah njihovega poslovanja. S pomočjo Val IT so upravljali investicije v informacijska sredstva skozi njihov celoten cikel.

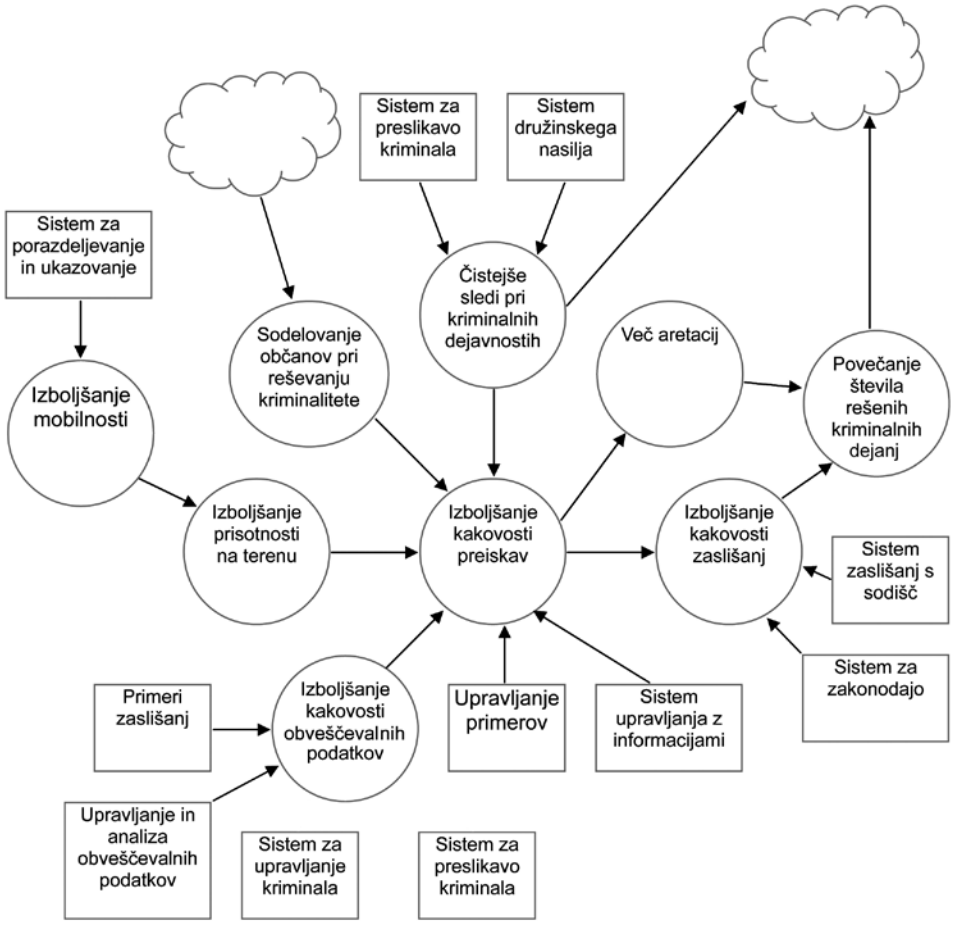
Upoštevali in razpoznali so veliko komplementarnih aktivnosti in dejstev, ki pripomorejo k doseganju strateških ciljev. Med temi so tudi zmanjšanje kriminalitete, povečanje rešenih primerov, zmanjšanje administrativnega dela, zanesljivo delovanje informacijskih sredstev v kritičnih situacijah in podobno. V življenjskem ciklu investicije so vseskozi zagotavljali čisto sliko pri postavljanju odgovornosti in pri meritvah doseženih rezultatov. Študija temelji na petletnih izkušnjah, katerih začetek sega v leto 1999. Šlo je za pomembno investicijo, ki jo je podprla politika in je zahtevala velike časovne in druge nematerialne vložke njihove policije. Izbrati so morali prave investicije v zaostrenih investicijskih pogojih in poročati o poslovni uspešnosti teh investicij političnim predstavnikom, ki so vsako leto posebej odločali o nadaljevanju financiranja.

Poslovno vrednost, ki jo prinaša investicija v informacijska sredstva, so merili z doseganjem poslovnih ciljev in ne z denarnim tokom ali vračilom naložbe. Določali so, kolikšen je tisti del vrednosti, ki ga prinaša informatika pri doseganju posameznega cilja iz njihovega poslovnega načrta. Tako je najprej nastal načrt ciljev, ki so medsebojno povezani. Del tega načrta prikazuje slika 1. V krogih so cilji, usmerjene puščice pa kažejo na njihovo medsebojno povezanost. Smer puščice prikazuje, kateri cilji podpirajo druge pri njihovem uresničevanju. Seveda je treba za dosego vsakega posameznega cilja (to so v bistvu izboljšave obstoječega poslovanja) izvajati neke iniciative.



Slika 1: **Nekatere aktivnosti v procesu kriminaliteta in njihove medsebojne odvisnosti (povzeto po [5])**

Za doseganje cilja *izboljšanje obveščevalnih podatkov* je bilo treba vpeljati *sistem za upravljanje kriminalitete* (ki je informacijski sistem), medtem ko je bilo treba pri doseganju cilja *več aretacij* reorganizirati obstoječe poslovanje in uvesti nov oddelek v policijsko postajo. Že ob tem želimo poudariti pristop, pri katerem se po definiranju poslovnih zahtev lahko začnejo jasneje kazati druge iniciative (to je cel nabor potreb), med katerimi so tudi iniciative za informacijske zahteve. Torej iz poslovnih zahtev prehajamo na iniciative, povezane z informacijskimi sredstvi – informacijskih iniciativ pa ni brez jasnih poslovnih potreb. Slika 2 prikazuje informacijske iniciative za doseganje ciljev s slike 1. V tem prispevku se osredinjamo na informatiko in zato pišemo le o informacijskih iniciativah in ne o drugih, ki tudi obstajajo in se jih moramo zavedati.



Slika 2: **Nekatere aktivnosti v procesu kriminaliteta, njihove medsebojne odvisnosti in podpora z informacijskimi sistemi (povzeto po [5])**

Na podlagi slike 2 (ki v tem prispevku prikazuje le del ciljev in informacijskih iniciativ za doseganje le-teh) je mogoče opredeliti portfelj posameznih informacijskih projektov, ki jih je treba preslikati v delež zadovoljevanja posameznih poslovnih ciljev. Upoštevamo tudi, da lahko z enim informacijskim projektom podpremo več posameznih poslovnih ciljev, kar dodatno uteži takšen projekt. V primeru policijske postaje, ki jo opisujemo, so za vsak posamezni projekt ocenjevali:

1. njegov neposredni prispevek k doseganju posameznih poslovnih ciljev; ta prispevek so razvrstili glede na pomembnost v več razredov;
2. pomembnost, ki ga ima posamezen poslovni cilj (ki ga sicer podpira opazovani projekt) za poslovanje policije v celoti;
3. poleg prispevka, ki ga ima posamezni projekt za doseganje poslovnih ciljev, so projekt ocenili še s klasičnimi ocenami, ki so:
   a) prihranek časa, ki ga bo omogočila izvedba projekta pri delu na policijski postaji v enem letu;
   b) prihranek vloženega dela (ljudi), ki ga bo omogočila izvedba projekta pri delu na policijski postaji v enem letu;
   c) prihranek denarja.

S pomočjo točkovanja so nato odločili o pomembnosti projektov (kar pomeni pomembnost razpoložljivosti, celovitosti in razpoložljivosti informacij) in s tem posledično o pomembnosti investicij (ki omogočajo spremembo, razširitev ali le vzdrževanje obstoječega stanja) v informacijska sredstva (informacije, aplikacije, infrastruktura in ljudje).

Z osredinjanjem na poslovne cilje pri vodenju investicij (projektov) v informacijska sredstva in s sistematičnim pristopom pri njihovem upravljanju so dosegli zastavljene kratkoročne cilje, medtem ko za doseganje nekaterih dolgoročnih ciljev v omenjeni

analizi primera ni opisa, ker je za analizo njihovega doseganja potrebna časovna distanca. V študiji je povzet način upravljanja projektov in za investicije pomembnejših projektnih mejnikov. Na kratko so opisani postopki za razvrščanje projektov po prioritetah in za merjenje učinkovitosti. Pri tem so sledili navodilom, ki izhajajo iz procesov, ki jih definira Val IT. Med temi so pomembnejša navodila za določanje odgovornosti in pooblastil – tabela RACI (glej Val IT [5] in COBIT 5 [9]).

Verjetno so strateški cilji na področju kriminalitete vseh policijskih postaj v razvitem svetu podobni. Te cilje predpisujejo na državni ravni, same policijske postaje pa ravnajo skladno z njimi. Upoštevaje dejstvo, da se strateški cilji policije in cilji v opisanem primeru v veliki meri prekrivajo, lahko sklepamo, da opisani primer daje dovolj trdno podlago za upoštevanje smiselnosti upravljanja investicije v informacijska sredstva na podlagi smernic, ki nam jih ponuja Val IT tudi pri policiji. Izzivi in cilji so tako v opisanem primeru kot pri slovenski policiji v bistvu identični. Investicije na podlagi resnične vrednosti posameznih informacijskih sredstev bi, kot kaže primer, lahko tudi pri slovenski policiji pripomogle k temu, da bi bilo njeno poslovanje uspešnejše ob sočasnem zmanjšanju dela, ki ni tisto, kar pričakujemo od policistov. Tako torej na podlagi raziskave in primerjave predlagamo, da tudi slovenska policija pristopi k upravljanju investicij v informacijska sredstva na podlagi priporočil Val IT.

4 SKLEP

Model poslovnega upravljanja informacijske varnosti je nedvomno bistveno kompleksnejši in pomembnejši, kot smo ga bili vajeni videti in sprejemati pri modelu tehnično-tehnološkega upravljanja. Po eni strani gre za evolucijo, prek katere spoznavamo in priznavamo nove elemente vpliva, ki jih ima informatika na poslovanje, po drugi strani pa gre za dejstvo, da postaja informatika vse večji in pomembnejši del poslovanja, s tem pa se močno veča tudi njen vpliv na poslovanje.

Posledično se ta proces evolucije kaže tudi v zahtevi po spremembi upravljavskih praks. Prakse, ki so bile še do včeraj aktualne, postajajo premalo kompleksne in nezadostne. Še včeraj namreč nismo poslovnemu vidiku informacijske varnosti namenjali tolikšne pozornosti, kot jo zahtevajo današnje razmere. Videti je, kot da postaja proučevanje uspešnosti investicij v informacijska sredstva osrednja tema, s katero se ukvarjajo ali se bodo ukvarjali tako vodje informatike v podjetjih, kako tudi sam vrh upravljavske piramide. Pri tem gre tako za zasebni kot za javni sektor, kamor spada tudi policija. Med obema sektorjema je razlika samo v tem, da je ocenjevanje poslovne uspešnosti investicij v informacijska sredstva v javnem sektorju težje, saj gre pri javnih organizacijah za poudarjeno večplastnost ocenjevanja, kar prispeva k dodatni kompleksnosti ocenjevanja.

Pogoj za določanje poslovne koristi investicije v informacijska sredstva je, da najprej pri odgovornih za poslovne investicije (to je poslovodstvo) dosežemo, da ti razumejo, kako informatika prispeva k doseganju zastavljenih nalog na področju preprečevanja kriminalitete. Nato je treba doseči to razumevanje na vseh ravneh upravljanja policije. Na vseh ravneh upravljanja mora biti jasno, kako in koliko lahko neka investicija v informacijska sredstva omogoči realizacijo posamezne naloge policije. To je običajno izvedeno z dobrim načrtovanjem komuniciranja z internimi javnostmi in presega okvire tega prispevka.

V prispevku smo opozorili, da se običajno najprej sprašujemo ali počnemo stvari pravilno, vendar kmalu presežemo to stanje in se začnemo spraševati o koristih, ki jih prinaša naše delo. Pri informacijski varnosti to pomeni, da začenja poslovni del upravljati z informatiko in ne govorimo več o upravljanju informatike s strani informatikov tehnikov. Tako zagotovimo neposredno povezavo med tem, kar se dogaja na področju informatike, in med tem, kar se dogaja na poslovnem področju. S tem presežemo predsodek, da informacijski projekti stanejo, poslovni projekti pa prinašajo. Takšen pogled sploh ni nov, že velikokrat je preizkušen v praksi, a na področju informacijske varnosti je tokrat uporabljen na novo. Tudi pri policiji smo ali pa bomo kmalu na točki, ko se bo treba odločiti, kdaj dvigniti kakovost njenega poslovanja z dopolnitvijo obstoječega modela upravljanja njenih informacijskih sredstev in kako.

Učinkovitosti v tem prispevku predlaganega modela ni mogoče dokazati, dokler ta ni pravilno implementiran v konkretnem primeru z vsemi potrebnimi predpostavkami za njegovo implementacijo. Tudi sama implementacija modela zahteva investicijo z vsemi tveganji, ki spremljajo vsako investicijo. Vendar brez investicij ni mogoče nadaljevati v nedogled. Investicija v dopolnjen model informacije varnosti

bi, glede na izkušnje od drugod, povečala kompetence in ugled policije.

LITERATURA

[1] Humphrey, W. (1988). Characterizing the software process: a maturity framework. IEEE Software 5 (2), 73–79.

[2] International Organization for Standardization. (2009). IEC/ISO 31010: Risk management – Risk assessment techniques; Edition 1.0.

[3] International Organization for Standardization. (2009). ISO 31000: Risk management - Principles and guidelines; First edition.

[4] International Organization for Standardization. (2011). ISO/IEC 27005:2011; Information technology - Security techniques - Information security risk management, Second edition.

[5] IT Governance Institute. (2006). Enterprise Value: Governance of IT Investments, The ING Case Study, Rolling Meadows: IT Governance Institute.

[6] IT Governance Institute. (2007). COBIT 4.1, Rolling Meadows: IT Governance Institute

[7] IT Governance Institute. (2008). Enterprise Value: Governance of IT Investments, Getting Started With Value Management, Rolling Meadows: IT Governance Institute.

[8] IT Governance Institute. (2008). Enterprise Value: Governance of IT Investments, The Val IT Framework 2.0, Rolling Meadows: IT Governance Institute

[9] IT Governance Institute. (2011). COBIT 5, Rolling Meadows: IT Governance Institute

[10] Jereb, B. (2007). Informatika in računalništvo. Celje: ABakus in Jereb.

[11] Jereb, B. (2008). Val IT - Upravljanje IT investicij. Zbornik referatov. Ljubljana: Slovenski inštitut za revizijo.

[12] Jereb, B., & Brumen B. (2010). Upravljanje IT tveganj s pomočjo Risk IT. Dnevi slovenske informatike. Uravnotežite naložbe, tveganja in razvoj za uspeh. Ljubljana: Slovensko društvo Informatika.

[13] Jereb, B., Cvahte, T., & Rosi, B. (2012) Managing logistics investments by using experience from IT. XII. znanstveni skup s međunarodnim sudjelovanjem Poslovna logistika u suvremenom menadžmentu, Osijek: Ekonomski fakultet.

[14] Jereb, B., Cvahte, T., & Rosi, B. (2012). Val IT v logistiki. Dnevi slovenske informatike. Ustvarimo nove rešitve! Ljubljana: Slovensko društvo Informatika.

[15] Matjašič, K., & Jereb, B. (2012). Študija primera upravljanja zaseženih nosilcev elektronskih podatkov. 13. slovenski dnevi varstvoslovja, Zbornik povzetkov (str. 24). Ljubljana: Fakulteta za varnostne vede.

[16] Republika Slovenija, Ministrstvo za notranje zadeve. (2007). Srednjeročni načrt razvoja in dela policije za obdobje 2008-2012. Pridobljeno na http://www.policija.si/images/stories/O_Policiji/NacrtiPorocila/nacrtDela2008-2012.pdf.

[17] Republika Slovenija, Ministrstvo za notranje zadeve. (2007). Temeljne usmeritve za pripravo srednjeročnega načrta razvoja in dela policije v obdobju 2008Ð2012. (2007). Pridobljeno na http://www.mnz.gov.si/fileadmin/mnz.gov.si/pageuploads/SOJ/word/2011/temeljne_usmeritve_2008-2012.doc.

[18] Republika Slovenija, Ministrstvo za notranje zadeve. (2010). Informacijska varnostna politika Policije – krovna politika, Različica 1.1. Pridobljeno na http://www.mnz.gov.si/fileadmin/mnz.gov.si/pageuploads/JAVNA_NAROCILA/PRILOGA_7-Varnostna_politika.pdf.

[19] Republika Slovenija, Ministrstvo za notranje zadeve. (2011). Usmeritve in obvezna navodila za pripravo letnega načrta dela policije v letu 2012. Pridobljeno na http://www.mnz.gov.si/fileadmin/mnz.gov.si/pageuploads/DPDVN/Nadzor/Usmeritve_za_leto_2012.pdf.

[20] Republika Slovenija, Ministrstvo za notranje zadeve. (2012). Katalog informacij javnega značaja, Policija. Pridobljeno na http://www.policija.si/index.php/informacije-javnega-znaaja/katalog-ijz/974-urad-za-informatiko-in-telekomunikacije.

[21] Slovenska tiskovna agencija. (2011). Izginili ključni dokazi v primeru Magajna, Pridobljeno na http://www.iusinfo.si/DnevneVsebine/Novice.aspx?id=71649.

[22] Textalyser. (2012). Pridobljeno na http://textalyser.net/index.php?lang=en#analysis.

▪

Borut Jereb je predavatelj na Fakulteti za logistiko. Leta 1991 je uspešno zagovarjal doktorat s področja računalniških znanosti na Univerzi v Ljubljani. Od leta 1991 do leta 1992 je kot vabljeni profesor raziskoval in poučeval na Oregon State University. Po vrnitvi v Slovenijo si je skoraj dve desetletji kot svetovalec in kot vodja v podjetjih in v javnem sektorju pridobil veliko praktičnih izkušenj na področju optimizacije poslovanja. V zadnjem času se ukvarja predvsem z upravljanjem tveganj, IT-varnostjo, standardizacijo in zakonodajo.