Sodobna managerska orodja varovanja poslovnega informacijskega sistema gospodarske družbe s poudarkom na načrtovanju neprekinjenega poslovanja

Milan Vršec, Fakulteta za varnostne vede, Univerza v Mariboru; Inštitut za korporativne varnostne študije

Namen prispevka
Namen prispevka je opozoriti na koristnost uporabe sodobnih managerskih orodij v sistemu varovanja poslovnega informacijskega sistema in hkrati predstaviti metodološki pristop k raziskovanju neprekinjeneg,a poslovanja gospodarskih družb. Temeljni razlog za tovrstno predstavitev prispevka je ranljivost in večplastna ogroženost poslovnih informacijskih sistemov. Kajti s hitrim razvojem informacijske tehnologije ki napaja poslovne procese, narašča tudi število nevarnosti in groženj, ki so jim izpostavljena računalniška omrežja in poslovni informacijski sistemi. Raziskovalna spoznanja kažejo na to, da so računalniški kriminal, številni računalniški virusi, hekerski in krekerski vdori, gospodarsko vohunstvo, prisluškovanje in prestrezanje elektronskih komunikacij (Echelon, Carnivore), napake skrbnikov sistemov, informacijske in druge nesreče ter zlorabe informacij s strani zaposlenih, stalnica poslovnih in varnostnih tveganj. Učinkovita managerska orodja za obvladovanje teh tveganj so informacijski standardi, benchmarking, business intelligence, enkripcija in varnostna kultura zaposlenih. Prava učinkovitost ter uspešnost poslovanja gospodarske družbe pa se skriva v planu (elaboratu) neprekinjenega poslovanja in kriznega vodenja.

Metodologija
Metodologija raziskovanja temelji zlasti na anketiranju, intervjuvanju, proučevanju poslovne dokumentacije, SWOT analizi, operativnem pregledu predmetov raziskovanja, sklepanju od splošnega h konkretnemu in obratno in sintezi raziskovalnih dognanj. V načrtovani raziskavi, ki se bo nanašala na proučevanje varovanja kritične infrastrukture pa bodo uporabljene tudi multivariantne statistične metode.

Ugotovitve
Ugotovitve v prispevku so namenjene vodilnemu, srednjemu, varnostnemu in informacijskemu managementu, ki se mora zavedati: prvič, da je učinkovito upravljanje informacij in komunikacij vodilna misel v obvladovanju poslovnih procesov; in drugič, da je sistem upravljanja informacij po prenovljenih standardih serije ISO/IEC 27000 neizbežna nujnost v zagotavljanju neprekinjenega poslovanja po standardih PAS 56, BS 25999, ITIL, idr.

Izvirnost
Izvirnost prispevka je v tem, da avtorja na temelju lastnih raziskovalnih projektov argumentirano predstavita arhitekturo modernega poslovnega informacijskega sistema, ki zagotavlja upravljanje ključnih (prioritetnih) poslovnih funkcijah tudi v kriznih razmerah.

Ključne besede: varovanje informacij, poslovni informacijski sistem, informacijski standardi, benchmarking, business intelligence, enkripcija, neprekinjeno poslovanje, varnostna tveganja, korporacijska kultura, kritična infrastrtuktura

1 Uvod

Struktura in vsebina tega prispevka temelji (zlasti) na projektnih, raziskovalnih, analitičnih in strokovnih spoznanjih, dognanjih in ugotovitvah obeh avtorjev, ki sta v tem desetletju izvedla preko 20 varnostnih projektov v gospodarskih družbah, javnih podjetij, zavodih in nekaterih državnih institucijah. Eno od glavnih spoznanj je, da so poslovni informacijski sistemi močno podvrženi napadom od znotraj (zaposleni, okvare. izpadi) in od zunaj (naravne nesreče, informacijski vdori, kriminalni napadi, vohunjenje, idr.). Temu spoznanju sledu drugo, ki pove, da je v gospodarskih družbah in v drugih organizacijah premalo znanja, premalo volje, premalo zavedanja, premalo vnašanja dobrih praks, tu pa tam pa tudi premalo financ za učinkovitejše varnostne mehanizme. Tretje glavno spoznanje pa je, da je veliko vrzeli in varnostnih lukenj pri varovanju poslovnih skrivnosti. Naša spoznanja potrjuje tudi globalna raziskava o varovanju poslovnih skrivnosti, v kateri je sodelovalo 305 vodij informacijske varnosti s celega sveta. Raziskavo je po naročilu korporacij RSA in Microsofta izvedla družba Forrester Consulting (www.microsoft.com/DLP). To pomeni, da se lastniki, top management in nadzorniki občutno premalo ukvarjajo z obvladovanjem tveganj, ki jih povzročajo pomanjkljivi varnostni mehanizmi v poslovnem informacijskem sistemu. Tu je v bistvu izhodišče problema, ki bi se ga morali zavedati vsaj (varnostni) management kritične infrastrukture.

2 Arhitektura poslovnega informacijskega sistema

Nastanek, urejanje, uporabljanje, pošiljanje, spreminjanje, dodajanje in arhiviranje vseh nastalih dejanj, produktov, storitev, postopkov in procedur poslovanja omogoča in zagotavlja poslovni informacijski sistem. Gre za funkcioniranje vseh poslovnih funkcij in poslovnih procesov, ki jih upravlja management, izvajajo pa zaposleni v ustreznih organizacijskih enotah. Ker pa je poslovanje določene gospodarske družbe odvisno tudi od dobaviteljev, poslovnih partnerjev in pogodbenih izvajalcev so sestavni del poslovnega informacijskega sistema tudi ti zunanji dejavniki.
Arhitekturo poslovnega informacijskega sistema, ki na zgoraj opisa način dobi oznako integralni poslovni informacijski sistem, prikažemo na modulni način. Moduli so naslednji:

- Upravljavsko-managerski modul – vodstvo in nadzorniki ter vodje posameznih organizacijskih enot, ki imajo informacije za potrebe vodenja in nadziranja;
- Kadrovski modul – podatki vseh zaposlenih, plače, izobraževanje, oprema, drugo;
- Modul proizvodnja produktov in storitev z logistiko – priprava, neposredna proizvodnja nabava, prodaja, skladiščenje, transport;
- Računovodsko-finančni modul, ki zajema bilance uspeha, finance, investicije in bančne transakcije;
- Modul poslovnih partnerjev – dobavitelji, družbeniki, solastniki, drugi;
- Modul pogodbenih izvajalcev – ponudbe, naročila, pogodbe, finančne garancije, nadzor, škode;
- Projektni modul – razvojni projekti, socialni projekti, interdisciplinarni in

multidisciplinarni (mednarodni) projekti, okoljski projekti in drugi projekti;
- Komunikacijski modul, ki zajema: intranet, extranet, internet, infranet (prenos alarmnih sporočil), in enkripcijo zaupnih besedil, poslanih po elektronskih medijih.
- Modul družbene odgovornosti po SA 8000 – donatorstvo, humanitarne akcije, odnos do okolja, sponzorstvo, idr.
- Zavarovalni modul (zavarovalni portfelj)- zavarovanje premoženja, osebja, odgovornosti.

Moduli so (lahko) organizacijsko, kadrovsko in strokovno relativno samostojni, vendar so informacijsko, komunikacijsko in varnostno integrirani v celoto poslovnega informacijskega sistema.

3 Managerska orodja varovanja poslovnega informacijskega sistema

3.1 Izhodišče: Obvladovanje tveganj v kritični infrastrukturi

V industriji, gospodarstvu, državnih institucijah in v civilni družbi je kar nekaj sektorjev, ki imajo status kritične infrastrukture. To so tisti sektorji, katerih delovanje je neizogibno potrebno za normalno funkcioniranje celotne družbe – vse od državnih organov, industrije, gospodarstva, civilne družbe, do prebivalstva. Po ameriških merilih vitalno (ključno) kritično infrastrukturo sestavljajo naslednji gospodarski sektorji: elektroenergetski sistem, telekomunikacije, zdravstvo, transport, bančništvo in finance, vodovodni sistem, intervencijske službe, radioaktivne snovi, jezovi, vladne službe, zaščita in reševanje ter pomembne poslovne zgradbe (Gheorge 2006, Lewis 2006, Murray 2007). Podobno strukturo kritične infrastrukture opredeljuje evropski program zaščite kritične infrastrukture, ki je bil v Evropski komisiji zasnovan že leta 2005. Proces analiziranja tveganj v okviru risk managementa sestavlja zaporedje 10 korakov /Fennelly, 2003:5), in sicer:
- Definiranje problema.
- Definiranje predmeta obdelave.
- Vrednotenje obstoječih ukrepov in sredstev.
- Identificiranje tveganj.
- Vrednotenje/ocenjevanje tveganj.
- Sortiranje tveganj.
- Priprava ukrepov skrčenja (zmanjšanja) tveganj.
- Izvedba ukrepov skrčenja tveganj.
- Vrednotenje ukrepov skrčenja tveganj.
- Redefinicija tveganj in ukrepov.

Gre za enega od pristopov k celovitemu analiziranju tveganj, ki je naslonjeno na načelo objektivnega presojanja in ocenjevanja negotovosti, nevarnosti in groženj, ki jih lansirajo zgodnji opozorilni sistemi ter analize izpeljanih scenarijev razvoja izrednih dogodkov. Nekateri avtorji dajejo poudarek identifikaciji in vrednotenju tveganj (npr. Hearnden/Moore, 1999:12-20), pri čemer izhajajo iz vzrokov za nastanek varnostnih tveganj (naravne nesreče, požari, kriminalna dejanja, industrijske nesreče, človekova malomarnost/brezbrižnost/napake/sabotaže, itd.) in posledic uresničitve tveganj, ki se izrazijo v materialnih, človeških, socialnih in moralnih škodah in izgubah. Zaradi tega, omenjena avtorja pravita, da je treba tveganja obvladovati sistematično. To nakazuje naslednjo proceduro: izogibanje (avoidance) visokim tveganjem, prenos (transfer)

neobvladljivih tveganj na zavarovalnice, zadržanje (retention) nekaterih tveganj zaradi izkoristka poslovnih priložnosti in skrčenje oziroma zmanjšanje (reduction) tveganj na raven, ki je obvladljiva.

V bistvu postaja skrb za upravljanje s tveganji ena od sodobnih poslovnih in korporacijskih funkcij, s katero se morajo ukvarjati lastniki, upravljavci, management in nadzorniki. *Tveganje postaja nov ključ skupnih interesov v poslovnem svetu in zahteva po visoki stopnji korporacijske odgovornosti*« (Borodzicz). To še posebej velja za gospodarske družbe, poslovne sisteme, koncerne in korporacije, ki upravljajo s kritično infrastrukturo. Politični in gospodarski dejavniki v Evropi in drugod po svetu se namreč več ali manj zavedajo, da je energetika (nafta, plin, električna energija) ključni del kritične infrastrukture, ki kroji usodo vsega ostalega gospodarstva, državnih institucij, civilne družbe in prebivalstva. Prav v kritični infrastrukturi obstajajo številna varnostna tveganja, zaradi katerih marsikoga od naftno-plinskih gigantov/mogodcev (denimo Gazprom) boli glava. Na tem mestu predstavljamo eno od *enačb varnostnega tveganja* (Security Risk Equation), ki jo sestavljajo naslednji parametri (Biringer, B.E., Matalucci, R. V., O Connor,. S. L. , 2007):

$$\mathbf{R = P_A * (1 - P_E) * C}$$

Posamezni parametri pomenijo:
R = tveganje napada na kritično infrastrukturo,
$\mathbf{P_A}$ = zelo verjetni napadi na kritično infrastrukturo,
$\mathbf{P_E}$ = verjetnost učinkovitosti zaščite kritične infrastrukture,
$\mathbf{(1 - P_E)}$ = neučinkovitost zaščite kritične infrastrukture,
C = posledice napadov na kritično infrastrukturo.

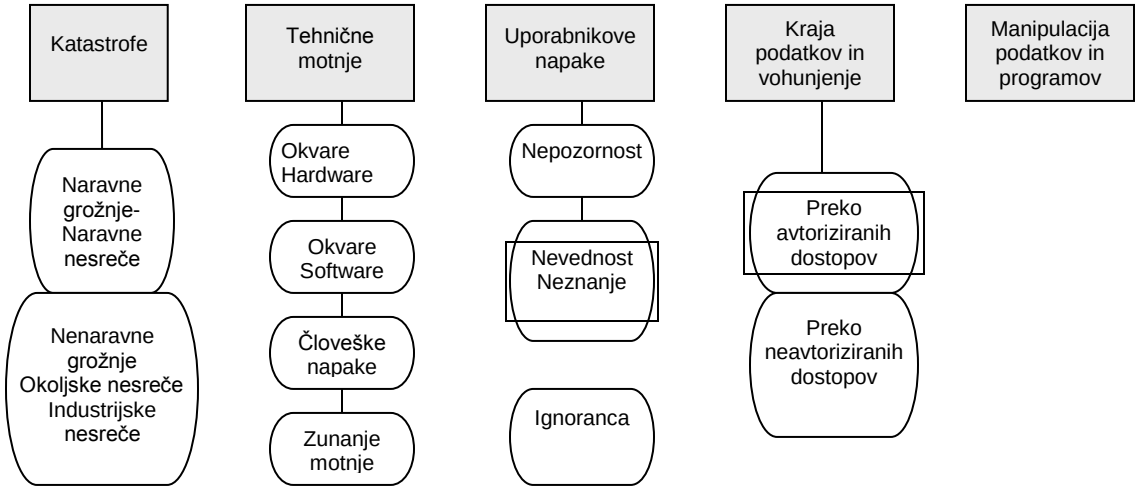
Pri ocenjevanju tveganj v industriji, gospodarstvu in pri izvajanju poslovnih funkcij bi se morali lastniki, upravljavci, management in poslovneži zavedati neizpodbitnega dejstva, da je v sklopu poslovnih, finančnih, logističnih in drugih tveganj treba nenehno obvladovati tudi varnostna tveganja, ki izhajajo iz naslednjih *verjetnih izrednih dogodkov*: (Broder, 2006):

- Naravne katastrofe (potresi, poplave, tornadi, plazovi, itd.),
- Industrijske nesreče (eksplozije, kemična izlitja, požari, tehnološke okvare, delovne nesreče, okoljske nesreče/katastrofe),
- Civilni dogodki (bombne grožnje, sabotaže, izgredi, stavke),
- Terorizem (tuji in domači),
- Kriminalna dejanja (vlomi, ropi, goljufije, zlorabe, poneverbe, gospodarsko vohunstvo, kraje, ugrabitve, utaje),
- Interesni konflikti (zlorabe informacij, poslovne goljufije, motnje v sistemih plač, idr.),
- Nuklearne nesreče.

Preveritev zgornje enačbe bi morala pokazati v katerih sektorjih kritične infrastrukture obstajajo varnostne in druge vrzeli, zaradi katerih se lastniki, management in nadzorniki soočajo s tveganji. Vsa varnostna tveganja so z varovanjem in zavarovanjem obvladljiva. Najmanj obvladljiva so seveda tveganja naravnih nesreč. V teku je raziskava varnostnih mehanizmov v kritični infrastrukturi (Vršec, Mir. 2010), ki bo razjasnila vse parametre, ki se nanašajo na obvladovanje tveganj. Spoznanja iz te raziskave bodo dobrodošla tudi za redefiniranje varnosti poslovnih informacijskih sistemov.

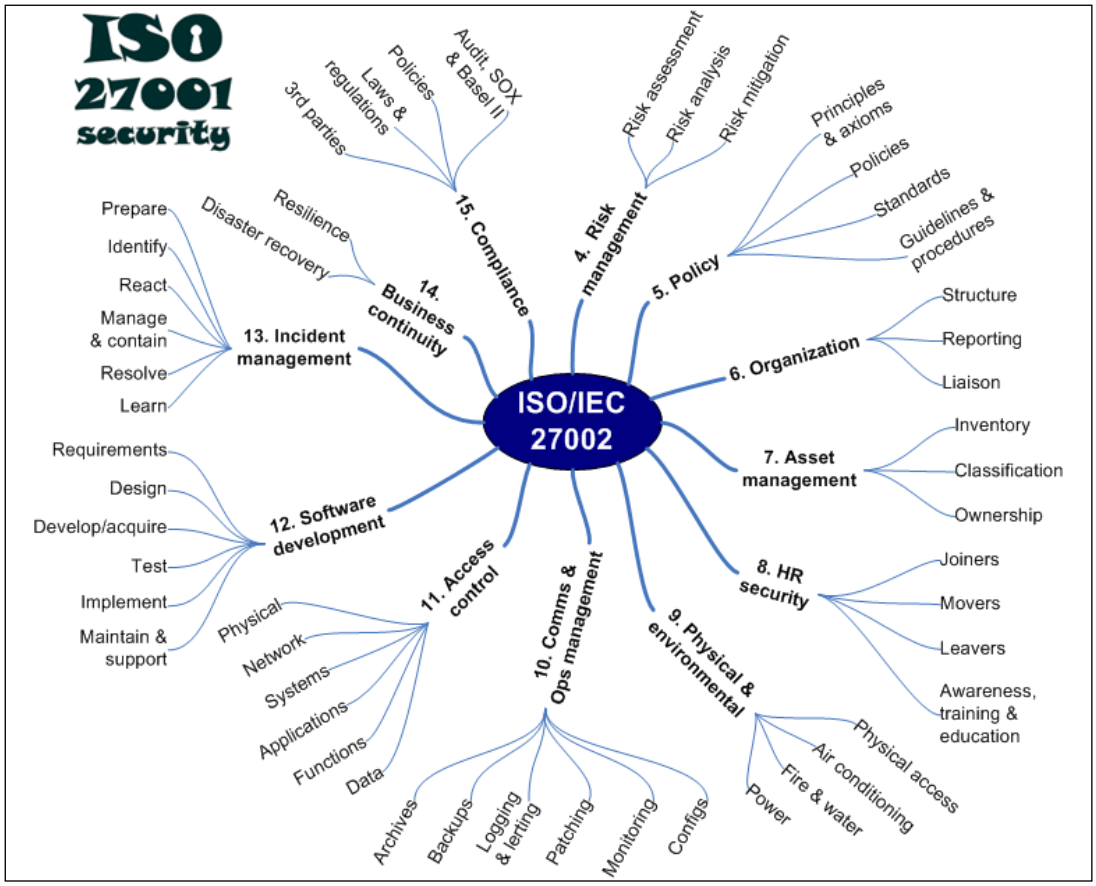
3.2 Informacijska varnost in informacijski standardi

Varovanje informacij, varstvo osebnih in tajnih podatkov, varovanje poslovnih skrivnosti in intelektualne lastnine ter zaščita inovacij, blagovnih znamk in konkurenčnih prednosti je v gospodarstvu vse bolj aktualna tema razprav in raziskav. *Potreba po informacijski varnosti obstaja ne glede na velikost podjetja in ne glede na to ali je podjetje javno ali zasebno* (Bacik, 2008). Kajti gospodarske in druge družbe doživljajo vse več raznih napadov, težav in problemov. Po raziskavah svetovno znanega ponudnika rešitev informacijske varnosti Symantec, s sedežem v Cupertrinu v Kaliforniji, je na svetu vsako sekundo 100 kibernetskih napadov, vsake štiri sekunde in pol pa je napad tudi uspešen. Napadi se vsako leto rapidno povečujejo – denimo v letu 2009 jih je bilo za 71 % več kot leto poprej (več o tem glej: www.symantec.com). Gre za hekerske, krekerske, kriminalne, vohunske in druge vdore v računalnike, računalniška omrežja in v poslovne informacijske sisteme korporacij, koncernov, poslovnih sistemov, gospodarskih družb, podjetij, državnih institucij in posameznikov. Na eni strani gre torej za grožnje, na drugi pa za slabosti v informacijski tehnologiji, informacijskih sistemih in upravljavcih in uporabnikih informacij (slika 1). Četudi *informacijska tehnologija omogoča organizacijam informacijsko partnerstvo, ne da bi združevale lastnino* (Gričar, 2002), Vendar pa je le treba pomisliti na morebitno multipliciranje slabosti in vrzeli v strojni in programski opremi in v uvajanju varnostnih mehanizmov. S tega zornega kota je veliko boljše,



Slika 1: Grožnje in slabosti sistemov informacijske tehnologije (Povzeto po: Alpar, 2007).

da si uspešen gospodarski subjekt vzpostavi lasten poslovni informacijski sistem, s sodobno strojno in programsko opremo, ki bo varovan po konceptu standardov varovanja informacij.
Serija standardov varovanja informacij ISO 27000 ponuja široke možnosti celovitega varovanja računalniškega omrežja in celotnega spleta informacij (več o tem: Bradeško, 1998; Bratuša/Egan, 2007; Stamp, 2006; Bacik, 2008; Brotby, 2009, Erjavec, 2010), ki se pretakajo po intranetu, extranetu, internetu in infranetu. Najpomembnejši je sistemski pristop na nivoju celotne organizacije. Sistemski pristop omogočata standarda varovanja informacij ISO/IEC 27001 in ISO/IEC 27002 (slika 2). ISO/IEC 27001, ki vključuje tudi Demingov koncept (načrtuj-naredi-preveri-ukrepaj), je standard za certificiranje sistema upravljanja varovanja informacij (SUVI).



Slika 2. Struktura standarda ISO/IEC 27002 *(www.iso27001security.com).*

Standard ISO/IEC 27002 pa omogoča (usmerja) naslednje: oceno tveganj, izdelavo varnostne politike, organizacijo varovanja informacij, upravljanje (varovanja) premoženja, upravljanje človeških virov (zaposleni pred, med in po zaposlitvi), fizično varovanje območij in zgradb, varovanje računalniškega omrežja pred napadi in vdori, varovanje elektronskih komunikacij (tudi kriptografska zaščita), nadzor dostopa/vstopa/nepooblaščenega gibanja po območjih in po zgradbah, nadzor dostopa v omrežje in v informacijski sistem, alarmiranje informacijskih incidentov in odzivanje nanje, upravljanje neprekinjenega poslovanja, skladnost z zakonodajo, krovno varnostno politiko in standardi kakovosti, postopki presoje in postopki revizije informacijskega sistema.

3.3 Poslovno poizvedovanje - business intelligence

Tudi business intelligence je v podjetjih bolj redko prisoten. Nekaj ga je zaslediti v naših multinacionalkah, ki nastopajo na tujih trgih, kjer se soočajo s konkurenco. O business intelligence je kar nekaj definicij. Hrvaška avtorja (Javorović in Bilandžić, 2007, 2008), pojmujeta business intelligence kot *poslovno obveščevalno delovanje*, ki je tesno povezano z občutljivimi poslovnimi informacijami, ki povedo kaj več kot je javno dostopno. Omenjenima avtorjema se pridružuje še tretji (Kralj, 2010), ki navedeno pojmovanje še razširja v *poslovno raziskovanje* varnostnega obvladovanja iskanja, pridobivanja, analiziranja in uporabe podatkov in informacij. Nekateri pa business intelligence razumejo zgolj kot poslovno inteligenco, ki se nanaša na spretnosti, aplikacije in prakse, ki se uporabljajo za pomoč pri poslovanju in dodano

vrednost v sistemu odločanja. Kakorkoli, business intelligence *so oči in ušesa uspešnih podjetij* (Trivunovič. 2009); je torej orodje managementa s katerim pridobiva ključne informacije na legalen in etično zdržen način. Torej ne gre za katerekoli informacije temveč za informacije, ki so dodana vrednost lastnemu znanju in izkušnjam ki dvigujejo konkurenčno sposobnost in prispevajo k bogatitvi razvojne strategije. Potemtakem gre za strateški vidik s poslovnim poizvedovanjem pridobljenih informacij. *Pomembno je namreč vprašanje, kaj se bo zgodilo jutri, ali kaj se bo zgodilo v prihodnje* (Schwarz, 2007). Zato je poizvedovalna dejavnost ena od najpomembnejših skrbi odločevalcev v strateškem in korporativnem okolju, kajti skrbno obdelan portfelj zbranih informacij predstavlja sistem za podporo pri odločanju. Razvojna strategija brez poizvedovalnih informacij je le preprosto ugibanje, ki sproža številna in neobvladljiva poslovna, finančna in varnostna tveganja. Vse bolj pa je evidentno, da se poizvedovalna dejavnost vrašča v benchmarking. V preteklosti je bila namreč vloga poslovnega poizvedovanja in poslovnega raziskovanja v benchmarkingu prezrta. Proces poizvedovalne dejavnosti poteka v korakih, kot so: načrtovanje poizvedovanja (tudi v sklopu kake raziskave), izbira tarč na trgu, priprava komunikacijskih poti, iskanje virov informacij, izbira metod in taktik delovanja, analiziranje pridobljenih podatkov ter posredovanje teh podatkov odločevalcem, marketingu in krovnemu varnostnemu managerju. V bistvu gre za poslovno poizvedovanje, ki ga v gospodarskem subjektu lahko izvaja le univerzitetno izobražen, dodatno usposobljen, visoko izkušen in komunikativen manager, strokovnjak, poslovnež, lobist ali oseba odgovorna za stike z javnostjo. V korporacijah in koncernih pa se s to dejavnostjo ukvarja posebna služba, ali pa pogodbeno najeta agencija.

3.4 Primerjanje s konkurenti - benchmarking

Splošno je že znano, da se vsaka uspešna korporacija, koncern, poslovni sistem in podjetje ukvarja z marketingom, analizo trga, konkurenco (tržnimi tekmeci) in pridobivanjem podatkov o poslovno uspešnih podjetjih v isti gospodarski panogi. Lastnike, upravljavce, management, poslovneže, razvojnike, inovatorje in vrhunske strokovnjake torej zanima kaj se dogaja v procesih razvoja in v proizvodnih procesih tržnih tekmecev in hkrati kaj se dogaja na globalnem, regionalnem in nacionalnem (lokalnem) trgu. Poslovno uspešna podjetja se potemtakem zavedajo lastnih konkurenčnih sposobnostih ter konkurenčnih prednosti tržnih tekmecev. Če vse to počnejo načrtno, sistematično in kontinuirano lahko rečemo, da v poslovne procese uvajajo poslovno in managersko orodje, ki mu pravimo benchmarking (več o tem npr.: Camp, 2006, Watson 2007). Tako podjetje vztrajno in postopoma spoznava domača in tuja konkurenčna podjetja in ugotavlja kako visoko je na konkurenčni lestvici v primerjavi z drugimi. Tako je benchmarking razumljen kot splošen poslovni koncept iskanja, pridobivanja, analiziranja, vrednotenja, selekcije in uporabe podatkov in informacij o konkurenci.

Nekateri avtorji (npr. Kovačič, 2005) omenjajo več vrst benchmarkinga, ki so: interni, konkurenčni, nekonkurenčni in funkcijski benchmarking. V splošnem je »benchmarking proces ustvarjanja poslovnega znanja s primerjavo in analizo poslovnih informacij o drugih podjetjih, s ciljem izboljšati kakovost poslovnega odločanja« (Prašnikar, 2002:16). Vendar pa se benchmarking vedno bolj spogleduje z business intelligence, s čimer se poveča učinkovitost metod in tehnik iskanja in zbiranja podatkov.

Benchmarking je zelo zahtevna naloga za management, ki zahteva visoko stopnjo načrtnosti, pa tudi angažiranje zunanjega strokovnjaka-eksperta-svetovalca. To pomeni, da se bencmarking poslovnega orodja uspešno loti le tisti management podjetja, ki ima pravo razvojno strategijo, ki zna nekoliko tvegati in ki je pogumen za profesionalni spopad s konkurenti.

3.5 Tajnopisje – kriptografija, enkripcija

Z razvojem računalniške tehnologije, informatike, komunkacij in satelitskih navigacij se je močno razvila tudi kriptografija, ki se uporablja domala na vseh področjih komuniciranja (elektronska pošta, faxi, mobilna telefonija, internetni protokoli, idr.). Enkripcija kot praktični postopek ali procedura je torej ključnega pomena za varovanje vsebine zasebno ali poslovno občutljivih elektronskih in drugih sporočil pred nepooblaščenimi fizičnimi in pravnimi osebami. Za uvedbo enkripcije v poslovni informacijski sistem gospodarske družbe, državnega organa in druge organizacije pa je potrebno kar veliko specifičnega znanja. Zato mora služba informatike ali kakšna druga služba zaposliti tudi poznavalca tega področja, ali pogodbeno najeti zunanjega referenčnega strokovnjaka. Kajti gospodarska družba, ki v mednarodnem komuniciranju (multinacionalka) operira s tajnimi podatki in s poslovnimi skrivnostmi si mora zagotoviti zanesljiv sistem šifriranja in dešifriranja sporočil. Vedeti mora namreč, da na zemeljski obli obstajajo številni prisluškovalni sistemi podprti s satelitsko navigacijo (**GPS**-ZDA**, Galileo.-** Evropa **Glonass**-Rusija **Beidou 1/Compas**-Kitajska **IRNSS**-Indija in drugi), ki prestrezajo elektronske in druge komunikacije. Eden od teh sistemov je ECHELON s številnimi prisluškovalnimi postajami (ena od teh je prikazana na sliki 3) in drugo infrastrukturo kot so denimo centri - s super računalniki za obdelovanje podatkov. Echelon je spoznan kot gigantski in najbolj skrivnosten vohunski sistem, ki so ga razvile ZDA, Kanada, Anglija in Avstralija. Prestreza in prisluškuje mednarodnim telefonskim pogovorom in elektronskim komunikacijam predvsem za interese in koristi ameriških (pa še kakšnih drugih) korporacij, ki si s pridobitvijo zaupnih podatkov in informacij pridobijo prednosti na svetovnih trgih. Drugi znani in prav tako vohunsko naravnan sistem prisluškovanja je Carnivore, ki ga upravlja FBI. Zato je šifriranje na bazi kriptografskih algoritmov (glej: Katz, 2007 in Knuth, 2010) dobrodošel varnostni mehanizem v mednarodnem elektronskem komuniciranju.

Slika 3: ECHELON: Prisluškovalna postaja na Menwith Hill v Veliki Britaniji (www.greaterthings.com/.../organizations/Echelon).

V tem kontekstu v nadaljevanju navajamo nekaj varnostnih mehanizmov, ki prispevajo k višji stopnji varnosti poslovnih informacijskih sistemov. Ti so:
Simetrična in asimetrična enkripcija (zasebni in javni ključi) zagotavlja varen prenos elektronskih komunikacij. Zanesljivi so 128 in 256 bitni kriptografski algoritmi. Primeri algoritmov: Evklidov algoritem, Dijkstrov algoritem, Algoritem MD5, Evolucijski algoritem, Primov algoritem.
Kvantna enkripcija, ki izhaja iz kvantne teorije in iz Heisenbergovega teorema negotovosti, po katerem kvantne informacije ni mogoče izmeriti. Zaradi tega ni mogoče neopazno prestrezati in prisluškovati elektronskim komunikacijam, kajti vsak poskus prestrezanja se takoj zazna in prenos sporočila se takoj samodejno zaustavi (prekine). Je to morda protiorožje Echelonu?
Enkripcija mobilnih komunikacij, denimo z 256 bitnim kriptografskim algoritmom AES Advanced Encryption Standard.
Penetracijski testi (Penetration Testing) so metoda varnostnega testiranja poslovnih informacijskih sistemov, s katerimi se ugotavljajo morebitne varnostne vrzeli in nato predlagajo izboljšave.
Proti prisluškovalni pregledi poslovnih in drugih prostorov, z namenom, da se najdejo morebitne prisluškovalne naprave in da se hkrati v prihodnje zagotovi profesionalna pristopna kontrola, po potrebi pa tudi video nadzor.
Računalniška forenzika preiskuje digitalne nosilce podatkov kot so: CD, DVD, trdi diski, spominske kartice, SIM kartice, USB ključi idr.

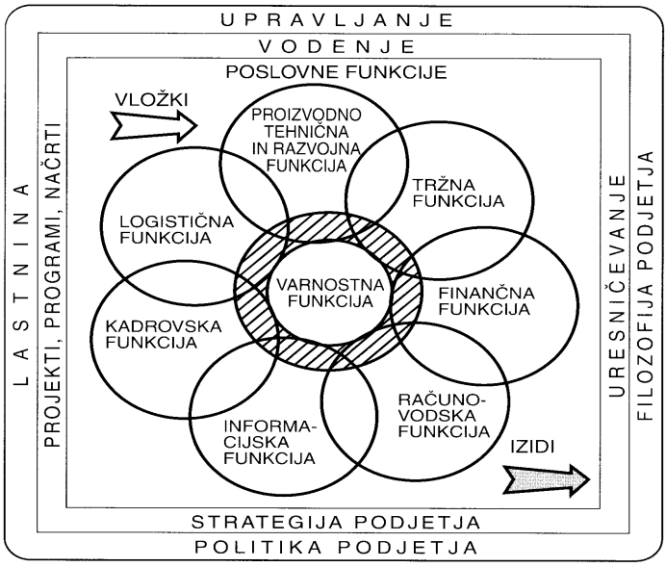
4 Zagotavljanje neprekinjenega poslovanja

Gospodarski subjekt, ki ima vizijo in razvojno strategijo si vzpostavi tudi proces zagotavljanja neprekinjenega poslovanja – tudi v pogojih gospodarske, ekonomske, finančne in socialne krize. Zagotavljanje neprekinjenega poslovanja (Business Continuity), obvladovanje nevarnosti, ogroženosti in tveganj (Risk Management) ter obvladovanje kriznega vodenja (Crisis Management) so v vsaki gospodarski družbi in drugi organizaciji nujne sestavine upravljanja poslovnih procesov, človeških virov (zaposlenih), kapitala, uporabnikov, poslovnih partnerjev in zunanjih izvajalcev (outsourcing). Neprekinjeno poslovanje definirajo procesi, postopki, odločitve in aktivnosti, ki zagotavljajo neprekinjeno poslovanje podjetja/organizacije/ustanove v primerih, ko grozi prekinitev delovanja. To zahteva izdelavo načrtov, ki pomagajo pri izogibanju kriznih situacij in katastrof ter omogočajo hitro obnovo. Da bi si podjetje, državni organ, zavod ali druga organizacija zagotovila potrebne informacije tudi v primeru izpada kakšne ali vseh poslovnih funkcij na osnovni lokaciji, si mora vzpostaviti rezervno lokacijo, na katero redno elektronsko prenaša in hrani informacijski sistem. Le na ta način si vsaka organizacija zagotovi neprekinjeno poslovanje.
Načrtovanje neprekinjenega poslovanja (business continuity planning – BCP) je metodologija, ki se uporablja za izdelavo načrta neprekinjenega poslovanja, ki zajema tudi obnovo delovanja ključnih poslovnih in (po potrebi) drugih funkcij podjetja/organizacije/ustanove v primeru kriznih in izrednih razmer (več o tem glej denimo: Syed, 2003; Fulmer, 2004; Bowman, 2008).
Z uvajanjem in upravljanjem neprekinjenega poslovanja se ukvarjajo tudi različni standardi, ki definirajo načine in postopke uvajanja ter upravljanja neprekinjenega poslovanja.
BSI priporočilo **PAS 56** predstavlja priporočila za postopke, principe in terminologijo upravljanja neprekinjenega poslovanja, ki sta ga pripravila angleški inštitut za standarde (BSI) in Insight Consulting.
BS 25999 je angleški standard za neprekinjeno poslovanje in je v dveh delih. Standard **BS 25999-**

1: 2006 obravnava minimalne zahteve in dobro prakso pri upravljanju neprekinjenega poslovanja. Standard **BS 25999-2: 2007** pa določa zahteve za vzpostavitev, izvajanje, kontrolo, pregled, vzdrževanje in izboljšave sistema neprekinjenega poslovanja.
ISO/IEC 27001 predstavlja standardno specifikacijo za upravljanje učinkovitega sistem nadzora informacijske varnosti (Information Cecurity Management System – ISMS) z uporabo pristopa stalnih izboljšav (glej denimo: Arnason, 2007; Whitman, 2007, Calder, 2006).
Upravljanje neprekinjenega poslovanja (BCM – Business Continuity Management) poteka po načrtu neprekinjenega poslovanja (BCP-Business Continuity Plan), ki je izdelan po konceptu standarda BS 25999 in po konceptu standardov varovanja informacij ISO/IEC 27001 in ISO/IEC 27002. Upoštevajoč zgoraj navedene standarde ima model izdelave načrta neprekinjenega poslovanja naslednje sestavine:

Definicija, namen in prednosti načrta neprekinjenega poslovanja
Določanje obsega poslovanja v primeru hudih motenj in neželenih odklonov
Pregled verjetnih hudih motenj - izrednih dogodki poslovne in varnostne narave
Ključne (prioritetne) poslovne funkcije
Zunanji in notranji vplivi na poslovanje
Vrzeli v poslovanju
Upravljanje (obvladovanje) sprememb
Upravljanje tveganj - Risk Management
Finančna tveganja – tveganja poslovnih rezultatov
Razvojna tveganja
Tveganja kršenja predpisov
Informacijska in komunikacijska tveganja
Tveganja pri upravljanju z osebnimi podatki
Tveganja človeških virov
Tveganja poslovnih partnerjev in zunanjih izvajalcev (outsourcing)
Tveganja izgube ugleda in dobrega imena
Varnostna tveganja kot specifična tveganja
Modeli upravljanja tveganj – splošni in Andersenov model
Strategija in cilji načrta neprekinjenega poslovanja
Testiranje in vzdrževanje načrta neprekinjenega poslovanja – scenariji, vaje
Informiranje in usposabljanje zaposlenih, poslovnih partnerjev in pogodbenih izvajalcev
Razvoj in dograjevanje načrta neprekinjenega poslovanja

V spletu poslovnih funkcij (slika 4) je treba – z vidika strukture lastnih produktov, strukture uporabnikov produktov in iz strukture poslovnih partnerjev, dobaviteljev in zunanjih pogodbenih izvajalcev – opredeliti katere poslovne funkcije oziroma kateri poslovni procesi so ključni ali manj pomembni za neprekinjeno poslovanje in za krizne razmere. S tega vidika delimo poslovne funkcije na: kritične, vitalne, občutljive in nekritične.



Slika 4: Varnostna funkcija kot prepletajoča poslovna funkcija (Vršec, 2003).

Kritične in vitalne funkcije so tiste, ki morajo delovati v vseh razmerah – torej tudi v kriznih razmerah. To so: proizvodni procesi z logistiko (dobavitelji), kadrovska funkcija (zaposleni) in informacijsko-komunikacijska funkcija.
Zagotavljanje neprekinjenega poslovanja daje gospodarski družbi naslednje prednosti:

- Omogoča načrtno upravljanje s hudimi motnjami, ali bolje rečeno, omogoča obvladovanje hudih motenj, ki jih povzročajo izredni dogodki; hkrati pa zagotavlja proces preprečevanja škod in izgub (Loss Prevention).
- Ustvarja sistemski pristop k vzpostaviti zgodnjega opozorilnega sistema, ki upravo dovolj zgodaj opozori, da se pripravlja nekaj kar predstavlja odmik od poslovne politike ter načrta in etike poslovanja, ali odmik od tehnične brezhibnosti opreme in naprav. Opozorila so lahko tehnične (alarm) ali človeške narave (nekdo opazi, ali zazna, ali izve, ali poizve, ali odkrije/razkrije, ali domneva, da se bo zgodilo nekaj škodljivega za določen poslovni proces, posameznega zaposlenega ali za družbo kot celoto, ali za katerega od poslovnih partnerjev).
- Omogoča neprekinjeno delovanje poslovnega informacijskega sistema 24 ur na dan vse leto.
- Zagotavlja razpoložljivost ključnih poslovnih funkcij oziroma poslovnih procesov v poslovnem času tudi v kriznih situacijah.
- Omogoča ponovno vzpostavitev poslovanja po hudih motnjah (izrednih dogodkih). Čas ponovnega vzpostavljanja je odvisen od odzivnih časov tistih, ki sanirajo nastalo škodo.
- Prispeva k zaupanju poslovanja družbe. To pomeni, da zaposlenim, poslovnim partnerjem, vlagateljem, delničarjem, borznim posrednikom, borzni hiši, bankam in drugim vliva zaupanje v procesu poslovnega sodelovanja, komuniciranja in izmenjave poslovnih informacij.

Za obvladovanje neprekinjenega poslovanja in kriznega vodenja so poleg močnega kriznega štaba potrebni tudi močna služba informatike, močna varnostna služba in ustrezno organizirana zaščita in reševanje (civilna zaščita s štabom CZ vred). To so atributi brez katerih se ne moremo pogovarjati o uspešnem organiziranju in poslovanju v kriznih razmerah.

5 Obvladovanje kriznega vodenja

Sestavni del neprekinjenega poslovanja je tudi vodenje organizacije v kriznih gospodarskih, socialnih, poslovnih, finančnih in varnostnih razmerah. Na kratko tovrstno upravljanje organizacije poimenujemo *krizno vodenje (krizni management*), ki ga izvaja od krovnega vodstva imenovan *krizni štab*.V krizi odločevalci (vodstva in krizni štabi) zaznajo ogrožanje poslovnega in tržnega položaja. V krizi je običajno omejen čas za sprejemanje odločitev. Tako stanje postavlja odločevalce pod velik stres in jih prisili, da sprejemajo odločitve v negotovih razmerah in ob pomanjkljivih informacijah, v katerih nekateri dogodki uidejo nadzoru. Kriza je večji, nepredvidljiv dogodek, ki ima možnost negativnih izidov. *Dogodek in njegove posledice lahko bistveno škodujejo neki organizaciji in njenim zaposlenim, izdelkom, storitvam, finančnim pogojem in ugledu* (Barton, 2007). *Krizna situacija vključuje: grožnjo virom in ljudem, izgubo nadzora ter opazne in/ali neopazne učinke na ljudi, vire in organizacije (*Heath, 1998). Kriza je potemtakem situacija, izhajajoča iz nenadnih, tudi nepričakovanih sprememb v gospodarski in drugi družbi ali njenem okolju, ki jo označujejo:

- dejanska in/ali zaznana grožnja osnovnim ekonomskim, finančnim, poslovnim in etičnim vrednotam (nepoznavanje ranljivosti in ogroženosti delovanja in poslovnih funkcij),
- izgubljen nadzor nad poslovno, tržno in finančno situacijo (neobvladovanje tveganj), premalo skrbi lastnikov in poslovodstev za načrtovanje neprekinjenega poslovanja (ni prave vizije, niti prave razvojne strategije, niti prave poslovne in varnostne politike),
- negotovost in potreba po hitrem odločanju in ukrepanju (nevarnost sprejemanja slabih odločitev).

Iz definicij krize izhaja izvirni problem, ki se vidi v tem, da zahteve odziva na hudo motnjo oziroma na izredni dogodek praviloma presegajo razpoložljive vire prizadetih gospodarskih in drugih družb. Za krizno vodenje je potreben krizni štab, ki ga imenuje vodstvo s pisnim sklepom. Vodenje kriznega štaba je z organizacijskega, strokovnega in psihofizičnega vidika zahtevno managersko opravilo, ki običajno poteka v razmerah psihološkega pritiska, časovne stiske, pomanjkljivih in nepreverjenih informacij, zasičenosti komunikacij in pritiskov nadrejenih. Zato mora vodstvo vodji kriznega štaba zagotoviti materialne in kadrovske pogoje za delo, delegirati mu mora jasne kompetence in zahtevati odgovornost. Krizni štab ima vodjo in potrebno število članov. Vodstvo predstavljata vodja štaba - nekdo iz vrha vodstva podjetja, ki ima status krovnega varnostnega managerja (ali druga oseba z vrha vodstva), trije njegovi pomočniki (vodja službe informatike, vodja varnostne aslužbe in vodja kadrovske službe). Obvezna člana štaba sta še vodja proizvodnje in vodja logistike. Krizni štab ima naslednje splošne naloge:

- zagotavljanje neprekinjenega poslovanja po načrtu neprekinjenega poslovanja,
- delovanje po kriznem načrtu, ki je sestavni načrta neprekinjenega poslovanja,
- zagotavljanje informacij za upravljanje in vodenje,
- postavljanje mehanizmov za zgodnje odkrivanje simptomov krize (zgodnji opozorilni sistem),
- prognozo potencialnih dogodkov in njihovih možnih posledic,
- priprava kriznih scenarijev,
- usposabljanje članov kriznega štaba in
- priprava specialistov (informatikov, računalničarjev in drugih) in tehnoloških sredstev za sodelovanje v kriznem managementu ter strateško načrtovanje aktivnosti za vzpostavljanje v prvotno stanje,

- vzpostavljanje komunikacij z okoljem,
- izvedba prehoda na rezervno lokacijo.

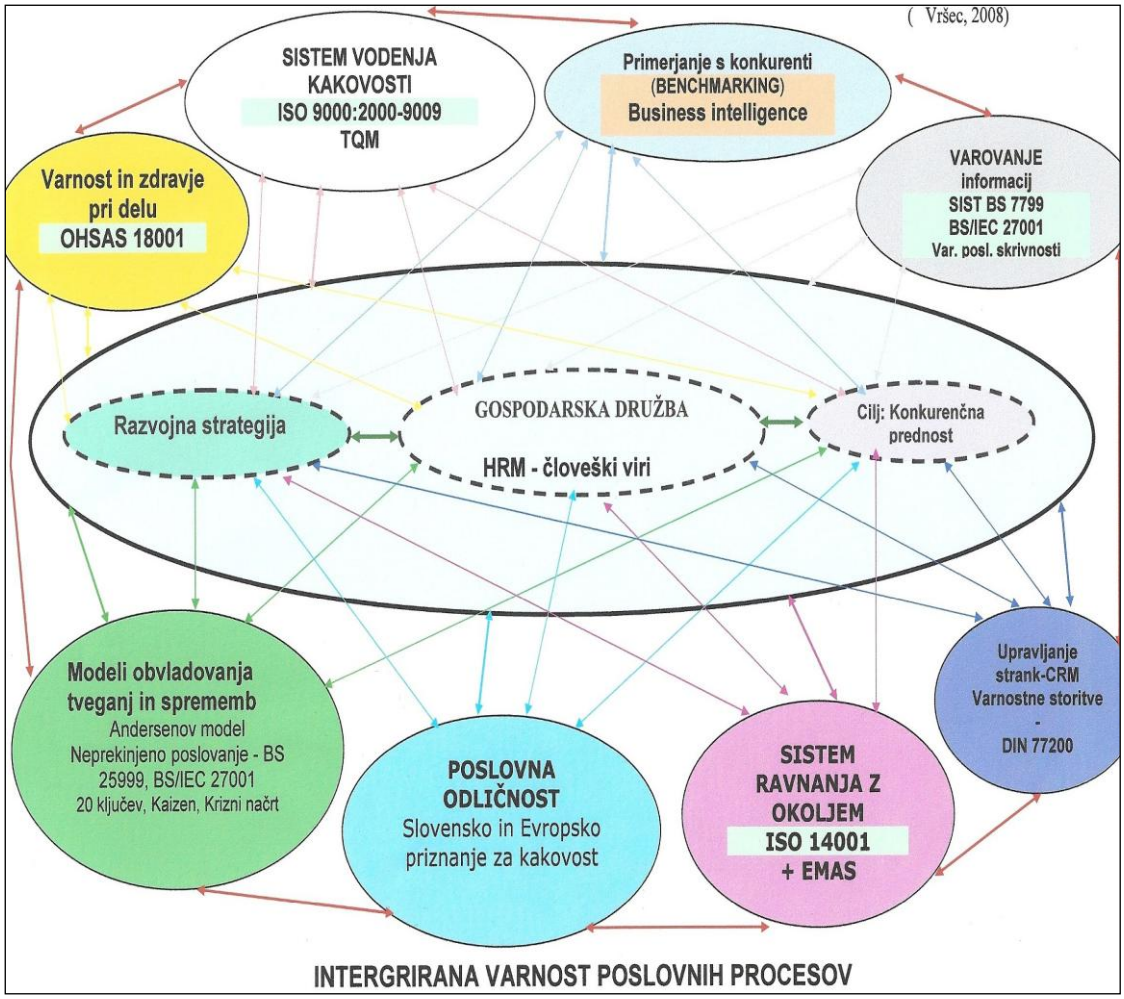
Na podlagi posnetka in ocene stanja ter ocene ranljivosti, ogroženosti in tveganj ter ustreznih scenarijev je treba pristopiti k varnostno orientiranemu projektu (izdelavi elaborata) za zagotavljanje neprekinjenosti poslovanja in obratovanja podjetja tudi v kriznih poslovnih, finančnih, varnostnih in drugih razmerah. Krizno načrtovanje lahko členimo na načrtovanje neprekinjenega poslovanja (business continuity planning), oziroma načrtovanje poslovanja ob (katastrofi) nesreči (disaster recovery planning), načrtovanje takojšnjega odziva na nesrečo (emergency response planning) in načrtovanja ponovne vzpostavitve poslovnih procesov (business resumption planning) ipd., kajti govorimo o celovitosti kriznega načrtovanja.
Proučevanje raznovrstnih kriz se v zadnjem času osredotoča na obvladovanje groženj, sprememb, tveganj in konkretnih izrednih dogodkov kot so denimo naravne nesreče, ekološke nesreče, požari, bombne grožnje, kriminalna dejanja, teroristični akti, izpadi elektroenergetskega sistema, izpadi telekomunikacij, informacijski incidenti, idr. Poudarek je predvsem na krizni preventivi, opozorilnih sistemih, pripravljenosti na krizne razmere, ukrepanju v krizi in sanaciji nastalih posledic, kakor tudi na problemih vodenja, odločanja, nadzora, zbiranja podatkov in informacij ter zagotavljanja komunikacij s poslovnimi partnerji, dobavitelji, pogodbenim,i izvajalci in drugimi.
Izredni dogodki večjega in velikega obsega vnesejo v vsakodnevno relativno mirno delo, obratovanje, poslovanje in življenje nemir, preplah, strah, negotovost, tveganje, ali celo šok, paniko, grozo in obup. Situacija je toliko hujša, če gospodarske in druge družbe niso na kaj takega pripravljene. Med izredne dogodke velikih razsežnosti in posledic uvrščamo: potrese, povodnji, orkane, viharje, obilne padavine, letalske, rudniške, železniške in cestnoprometne nesreče, večje vlome in roparske napade, teroristična dejanja, »električne mrke«, razlitja ogromnih količin nevarnih snovi v morje, vodovje ali v zemljo (ogrožanje podtalnice), velike gozdne požare in požare ter eksplozije na industrijskih objektih in objektih z velikim številom ljudi (poslovne zgradbe, kinodvorane, gostinski lokali, hoteli, gledališča, športna igrišča, vlaki, avtobusi), itd. Posledice vsakega izrednega dogodka so praviloma neugodne, ker se izražajo v materialni, finančni, poslovni, človeški in moralni škodi in hkrati izgubi. Če so materialne, finančne, poslovne, obratovalne (proizvodne) in človeške posledice šokantne, opredelimo tak dogodek kot havarijo oziroma katastrofo za podjetje. Vsak izredni dogodek velikega obsega je treba razreševati po načrtu odzivanja na katastrofe, torej po kriznem načrtu.
Model kriznega načrta ima naslednje sestavine:

Definicija kriznega upravljanja
Namen in cilj kriznega upravljanja
Ranljivost in ogroženost poslovnih funkcij
Obvladovanje poslovnih in varnostnih tveganj
Imenovanje in sestav kriznega štaba
Kompetence vodje kriznega štaba
Pogoji za delovanje kriznega štaba
Prehod na poslovanje na rezervni lokaciji
Rezervna lokacija – potrebni prostori – potrebna strojna in programska oprema po izbrani varianti (ali polna strojna in programska oprema, ali nepopolna strojna in programska oprema, ali samo varnostne kopije z minimalno strojno in programsko opremo)

Avtonomna in brezhibna energijska podpora
Nujna kadrovska zasedba
Izvajanje ključnih (prioritetnih) poslovnih funkcij
Visoka stopnja tajnosti rezervne lokacije in varnostni ukrepi
Testiranje kriznega načrta
SCENARIJI kriznih situacij za izredne dogodke: potres, požar grožnja z bombo, eksplozija, izpad informacijskega sistema (izpad osnovne lokacije)
Scenarij Potres
Scenarij Požar
Scenarij Grožnja z bombo in eksplozija
Scenarij Izpad informacijskega sistema
Metodološki in vsebinski okvir evakuacije zaradi nastalega izrednega dogodka
Praktični preizkus evakuacije v realnem (poslovnem) času - procedura
Informacijska podpora
Zgodnji opozorilni sistem
Načrt alarmnega in odzivnega sistema
Odzivi in odzivanja na alarmna sporočila - shema
Klici v sili
Sistem obveščanja – alarmiranja – prioritete- krizni komunikacijski načrt
Dosegljivost odgovornih oseb in drugih zaposlenih ter dosegljivost odgovornih oseb zunanjih izvajalcev
Vodenje akcije razreševanja nastalega izrednega dogodka
Način odpravljanja vzroka in posledic nastalega izrednega dogodka
Vzpostavljanje osnovne lokacije v prvotno stanje (Business Recovery Plan)
Zavarovalni portfelj

6 Varnostna kultura

Na sliki 5 je ponazorjen procesni pristop h graditvi in vzdrževanju varnostne kulture na bazi koncepta korporativne varnosti. Gre za uvajanje varnostnih standardov (OHSAS 18001, ISO 14001, SIST BS 27000 idr.), uvajanje poslovnih in managerskih orodij (benchmarking, business intelligence, HRM, CRM) in zagotavljanje neprekinjenega poslovanja (BS 25999, SIST BS 27001) poslovnih procesov. To pomeni da varnostna kultura zaposlenih, strank, obiskovalcev, poslovnih partnerjev, zunanjih pogodbenih izvajalcev in drugih vpletenih v poslovne procese določene gospodarske družbe, ne nastaja samoumevno in samodejno. V prvi vrsti je treba v miselnost, ravnanje in vedenje zaposlenih vgraditi organizacijsko kulturo v management pa etične standarde. To nastaja tako, da se s projekti vzpostavi koncept korporativne varnosti, ki nam pove: prvič, da je *varnostna kultura del splošne kulture* (Cooper, 2000) in , drugič, da sta *organizacijska kultura in varnost tesno povezani* (Antonsen, 2009), Ki tako tvorita celoto pozitivnih vrednot.



Slika 5: Koncept korporativne varnosti.

V proces izboljševanja varnostne kulture sodi tudi preverjanje lojalnosti (zvestobe, pripadnosti) delodajalcu, ki se vidi tudi v tem v koliki meri zaposleni upoštevajo zaščito podatkov, informacij in poslovnih skrivnosti. Z vidika zaščite konkurenčnih prednosti pa je treba upoštevati tudi zakonska določila o konkurenčni prepovedi in konkurenčni klavzuli. »Piko na i« varnostni kulturi pa daje kvaliteta notranjega socialnega dialoga, ki se izraža z delovnimi odnosi, plačami, dejanskimi delovnimi pogoji, vrednotami, ugledom in odgovornostjo managementa, itd. Varnostna kultura je potemtakem obraz gospodarske družbe, je konkurenčna prednost in je tudi kreator ugleda in dobrega imena družbe.

7 Zaključek

Poslovni informacijski sistemi so glavno orodje upravljavcev, managementa, nadzornikov, poslovnežev, tržnikov, inovatorjev, vrhunskih strokovnjakov, končno pa tudi vseh zaposlenih in zunanjih vpletenih, ki pri svojem delu in poslovanju potrebujejo delček podatkov in informacij tega sistema. Vendar pa je poslovni informacijski sistem izredno ranljiv in ogrožen zlasti, ko gre za izvirno znanje, bogat intelektualni kapital, kakovostne, drage in priznane blagovne znamke, inovacije, patente, visoko konkurenčno sposobnost in širok splet poslovnih skrivnosti. Če si gospodarska družba ali pa kakšna druga organizacija želi vzpostaviti ali obdržati sloves

zanesljivega partnerja, si mora zgraditi profesionalne varnostne mehanizme, da ne pride do izginotja, kraje, poškodovanja ali uničenja posameznih delov poslovnega informacijskega sistema. Zato je nujno, da se poleg fizičnega in tehničnega varovanja v varnostni sistem uvedejo tudi sodobna managerska orodja varovanja poslovnih procesov. To je tudi nujni pogoj za zagotavljanje neprekinjenega poslovanja in obvladovanje kriznega vodenja.

8 Literatura

Alpar, P. (2007). *Informationsmanagement: IT-Sicherheit*. Marburg: Philip's Universität Marburg.

Antonsen, S. (2009). *Safety culture: theory, method and improvement*.

Bacik S. (2008). *Building an Effective Information Security Policy Architecture*. Boca Raton: CRC Press.

Barton, L. (2007). *Crisis Leadership Now: A Real-World Guide to Preparing for Threats, Disaster, Sabotage, and Scandal*. New York, London: McGraw-Hill.

Broder, J. F. (2006). *Risk Analysis and the Security Survey*. Boston, Oxford. Butterworth-Heinemann.

Berk, A., Peterlin, J. in Ribarič, P. (2005*). Obvladovanje tveganja – Skrivnosti celovitega pristopa*. Ljubljana: GV Založba.

Biringer, B. E. (2007). *Security Risk Assessment and Management: Professional Practice Guide for Protecting Buildings and Infrastructures*. New York: Wiley&Sons.

Borodzicz, E. (2005). *Risk, Crisis and Security Management*. New York: John Wiley&Sons.

Bilandžić, M. (2008). *Poslovno – obaveštajno djelovanje-Business intelligence u praksi*. Zagreb: Zagrebački holding d.o.o. Podružnica AGM.

Bradeško M. (1998). Varnost računalniških omrežij in storitev. *Podjetnik XIV*., str. 74-77.

Bratuša, T., Egan, M. in Mather, T. (2007). *Varovanje informacij – hekerski vdori in zaščita*. Ljubljana: Pasadena.

Brotby, W. K. (2009). *Information Security Management Metrics: a Definitive Guide to Effective Security Monitoring and Measurement*. New York, London: Auerbach Publications-Taylor&Francis Group.

Camp, R. C. (2006). *Benchmarking: The Search for Industry Best Practices That Lead to Superior Performance*. Productivity Press.

Cooper, M. D. (2000). Towards a model of safety culture. *Safety Science, 36,* 111-136.

Čaleta, D. (2010). Varovanje kritične infrastrukture v razmerju do obvladovanja tveganj. V D. Čaleta (ur), *Mednarodni posvet s področja varnostnega managementa, na temo: Upravljanje varnostnih tveganj povezanih z varovanjem kritične infrastrukture* (str. 52-62). Ljubljana: Inštitut za korporativne varnostne študije.

Egan, M., Mather, T. (2005). *Varovanje informacij-grožnje, izzivi in rešitve*. Ljubljana: Pasadena.

Erjavec, A. (2010). Varovanje informacij s standardi ISO/IEC 27000 in stanje na področju certificiranja po standardu ISO/IEC 27001. V D. Čaleta (ur), *Mednarodni posvet s področja varnostnega managementa na temo: Upravljanje varnostnih tveganj povezanih z varovanjem kritične infrastrukture* (str. 63-72). Ljubljana: Inštitut za korporativne varnostne študije.

Fennelly, L. (2003). *Effective Phisical Security*. Butterworth-Heinemann.

Fulmer, K. A. (2004). *Business Continuity Planning: A Step- by- Step Guide with Planning Forms on CD-ROM*. Rothstein Associates Inc.

Gheorghe, A. V. (2006). *Critical Infrastructures at Risk: Securing the European Elektric Power System (Topics in Safety, Risk, reliability and Quality).* Springer.

Gričar, J. (2002). *Poslovni informacijski sistem*. Kranj: Fakulteta za organizacijske vede.

Hearnden, K. in Moore, A. (1999). *The Handbook Business Security. A Practical Guide to Managing the Security Risk.* London: Kogan Page.

Heath, R. (1998). *Crisis Management for Managers and Executives*. Financial Times/Pitman Pub.

Javorović, B. in Bilandžič, M. (2007). *Poslovne informacije i business intelligence*. Zagreb: Golden marketing-Tehnička knjiga.

Katz, J. in Lindell, Y. (2007). *Introduction to Modern Cryptograpfy*. Chapman and Hall/CRC.

Knuth, D. E. (2010). *The Art Computer Programming: Combinatiorial Algorithms v. 4. (Series in Computer Science&Information Processing*. Addison Wesley.

Kralj, R. (2010). Business intelligence za potrebe gospodarskih družb. V D. Čaleta (ur), *Mednarodni posvet s področja varnostnega managementa na temo: Upravljanje varnostnih tveganj povezanih z varovanjem kritične infrastrukture* (str. 43-51). Ljubljana: Inštitut za korporativne varnostne študije.

Lewis, T. G. (2006). *Critical Ifrastructure Protection in Homeland Security: Defending a Networked Nation*. Wiley-Interscience.

Murray, A. (2007). *Critical Infrastructure: Reliability and Vulnerability (Advances in Spatial Science).* New York: Springer.

Stallings, W. (2010). *Cryptography and Network Security: Principles and Practice*. Prentice Hall.

Stewart J. M., Tittel, E. in Chapple, M. (2008). *Certified Information Systems Security Professional*. Indianapolis: Wiley Publishing.

Stamp M. (2006). *Information security principles and practice*. New Jersey: JohnWiley & Sons.

Syed, A. (2003). *Business Continuity Planning Methodology*. Sentryx.

Vršec, M. (2003). Ocena ogroženosti in varnostnih tveganj kot ena od ključnih podlag za varnostno politiko in varnostni sistem. V M. Pagon (ur.), *Dnevi varstvoslovja*. Ljubljana: Visoka policijsko-varnostna šola.

Vršec, M. (2008). *Redefiniranje ranljivosti in ogroženosti podjetij z izvirnim metodološkim pristopom*. V V. Rajkovič (ur.), *27. mednarodna znanstvena konferenca o razvoju organizacijskih znanosti. Znanje za trajnostni razvoj* (str. 3061-3074). Kranj: Moderna organizacija.

Vršec, M. (2007). *Varovanje poslovnih skrivnosti, konkurenčne klavzule in varovanje informacij v skladu s standardom ISO/IEC 27001 in CRAMM metodologijo*. Študijsko gradivo. Ljubljana: Fakulteta za varnostne vede.

Vršec, M., Brumnik, R. in Vršec, M. (2009). Approach's to estimate vulnerability and threats of information critical infrastructure. *Sist. obrobki ìnf.*, *79*(7), 7-11.

Vršec, M. (2010). Izzivi varnostnih managerjev. V D. Čaleta (ur). *Mednarodni posvet s področja varnostnega managementa, na temo: Upravljanje varnostnih tveganj povezanih z varovanjem kritične infrastrukture* (str. 5-21). Ljubljana: Inštitut za korporativne varnostne študije.

Vršec, M. (2010). Dileme in izzivi na področju naročil varnostnih storitev. V D. Čaleta (ur), *Mednarodni posvet s področja varnostnega managementa, na temo: Upravljanje varnostnih tveganj povezanih z varovanjem kritične infrastrukture* (str. 32-42). Ljubljana: Inštitut za korporativne varnostne študije.

Watson, G. H. (2007). *Strategic Benchmarking Reloaded with Six Sigma: Improving Your Company's Performance Using Global Best Practice*. Wiley&Sons.