AKTUALNOSTI INFORMACIJSKE SIGURNOSTI U HRVATSKOM OKRUžENJU

mag. oec. Saša Aksentijević, univ.spec. za intel. el. posl.

KONFERENCIJA UHMS "POSLOVANJE I SIGURNOST"

BIOGRAD NA MORU, 21-23. LISTOPAD 2008.

Rijeka, rujan 2008.

Sadržaj

1. Uvod

Podsustav za zaštitu sigurnosti informacijskih sustava trebao bi biti implementiran u okviru informacijskog sustava kompleksnih organizacija, a osobito korporacija koje posluju na turbulentnom tržištu pod stalnim utjecajem promjena te jedinica i tijela državne uprave. U praksi, organizacijski i proceduralni čimbenici informacijske sigurnosti puno češće su pod prijetnjom nego tehnički čimbenici koji su u praksi predmet istraživanja specijalističkih tehničkih disciplina i obično su puno bolje obrađeni, nego organizacijski i legislativni aspekti informacijske sigurnosti. Razlog ovakvom pristupu je činjenica da se najčešće podcjenjuju organizacijski i ljudski čimbenici sigurnosti nauštrb tehničkom aspektu, što u praksi često rezultira manjkavostima i neadekvatnim sustavima zaštite informacijskih sustava. Cilj ovog rada je dati kratak pregled zakonske legislative koja je na snazi od jeseni 2008. godine, donijeti pregled aktualnosti po pitanju informacijske sigurnosti i ukazati na temeljne probleme u njenom provođenju u korporativnom, privatnom i državnom sektoru.

2. Kratki pregled zakonske legislative [1]

U rujnu 2008. godine u Republici Hrvatskoj postoji veći broj zakona i podzakonskih propisa koji reguliraju područje sigurnosti informacijskih sustava. Međutim, ne postoji jedinstveni zakon ili zakonski propis koji bi u cjelokupnosti regulirao to područje. Iz tog razloga, odgovorne osobe u poduzećima moraju se snalaziti u moru propisa tražeći one koji se odnose direktno na njihovo poslovanje. Formalno gledano, najbolje regulirano je područje financijskog sektora, osobito bankarskog i osiguravateljnog. Donošenjem podzakonskih akata temeljem Zakon o informacijskoj sigurnosti pred tijela državne uprave, ali i sve ostale organizacije koje imaju pristup povjerljivim državnim podacima, postavlja se niz vrlo detaljno opisanih obaveza.

2.1 Zakon o zaštiti osobnih podataka

Temeljna regulativa u Republici Hrvatskoj na temu informacijske sigurnosti je Zakon o zaštiti osobnih podataka koji je objavljen u Narodnim novinama broj 103 iz 2003. godine[2]. Po definiciji on se primjenjuje vrlo rastezljivo, na sve "zbirke osobnih podataka u Republici Hrvatskoj", te zahtijeva da ih se štiti od neovlaštenog pristupa ili promjena, gubitka, uništenja ili slučajne, odnosno namjerne zlouporabe. Sve organizacije su dužne Agenciji za zaštitu osobnih podataka dostaviti obavijest o namjeri uspostavljanja zbirke osobnih podataka, te namjeri o daljnjoj obradi tih podataka. Prema tome, obrada osobnih podataka nije dozvoljena bez obavještavanja Agencije, a propisane su i kaznene odredbe za one koji tu vrstu obrade vrše. Sve odredbe ovog zakona primjenjuju se na sve organizacije i poduzeća koja vrše obradu osobnih podataka, osim na fizičke osobe koje tu obradu vrše zbog vlastitih potreba ili potreba svog kućanstva. Osobe koje smatraju da im je obradom podataka povrijeđena privatnost mogu tražiti zaštitu Agencije. U praksi, provođenje ovog zakona je zasad gotovo na nivou preporuke, a zakonodavac ne nastupa odveć represivno.

2.2 Zakon o informacijskoj sigurnosti

Zakon o informacijskoj sigurnosti[3] obvezuje sva tijela državne uprave na provođenje mjera informacijske sigurnosti što uključuje ne samo ulaganje u informacijsku tehnologiju, nego i obrazovanje, odnosno zapošljavanje stručnjaka odgovarajućeg profila. Prema tome predviđaju se ne samo tehnološke nego i organizacijske promjene. Obveznici provođenja ovog zakona su ne samo pravne nego i fizičke osobe koje ostvaruju pristup povjerljivim podacima državne uprave. Sam zakon je jedan od zahtjeva

---

[1] Značajan dio poglavlja preuzet po Saša Aksentijević, „Integralna zaštitna funkcija unutar poduzeća i sustav upravljanja informacijskom sigurnošću – Saipem Mediteran Usluge d.o.o., Rijeka",magistarski rad, Ekonomski fakultet u Rijeci, 2008.

[2] Preuzeto prema Dejan Košutić, "Elementi procjene i upravljanja informacijskim rizicima", Kvadra Savjetovanje d.o.o, Zagreb, 2007.

[3] Narodne novine broj 79 iz 2007. godine

Europske unije, a naslanja se na Zakon o tajnosti podataka te na Zakon o sigurnosno-obavještajnom sustavu.[4] Njime se predviđa i osnivanje Zavoda za sigurnost informacijskih sustava koji će provjeravati provođenje zakona u tijelima državne uprave.

Tijekom 2008. godine trebalo bi biti doneseno pet pravilnika koji reguliraju mjere informacijske sigurnosti:

1. Pravilnik o sigurnosti poslovne suradnje, kojim se definiraju kriteriji sigurnosti klasificirane dokumentacije kojoj pristupaju pravne ili fizičke osobe
2. Pravilnik o sigurnosti podataka, kojim se definiraju opće mjere prevencije, otkrivanja i otklanjanja štete od gubitka i otkrivanja klasificiranih i neklasificiranih podataka
3. Pravilnik o fizičkoj sigurnosti kojim se definira zaštita objekata, prostora i uređaja u kojima se nalaze klasificirani podaci
4. Pravilnik o sigurnosnoj provjeri koji zahtijeva ishođenje certifikata za osobe koje imaju pristup klasificiranim podacima.
5. Pravilnik o sigurnosti informacijskih sustava koji definira zahtjeve sigurnosti klasificiranih i neklasificiranih podataka koji se obrađuju, pohranjuju ili prenose u informacijskom sustavu te zaštitu njegove cjelovitosti i raspoloživosti

2.3 Pravilnik o kriterijima za ustrojavanje radnih mjesta savjetnika za informacijsku sigurnost

Pravilnik o kriterijima za ustrojavanje radnih mjesta savjetnika za informacijsku sigurnost donesen je u ljeto 2008. godine i izazvao je mnogobrojne polemike. Pravilnik definira da osoba koja radi na tom radnom mjestu između ostalog vrši sigurnosnu provjeru i bavi se fizičkom zaštitom, iako ta dva operativna zadatka nemaju direktne veze s reguliranom materijom, odnosno informacijskom sigurnošću. U trenutku donošenja sam Pravilnik je gotovo neprovediv jer nije definiran način odnosno modus provođenja mjera koje predviđa, npr. izobrazbe koju bi trebao provoditi Ured VNS-a koji za sada još uvijek nije ustrojen kako bi to činio. Pravilnik čini i neke proceduralne struke, npr. savjetnik vrši reviziju (audit) vlastitog rada. Problematična je i odredba po kojoj savjetnik za informacijsku sigurnost mora biti osoba koja već radi u odgovarajućoj organizacijskoj jedinici, dakle ne radi se o novim pozicijama i otklanja se mogućnost vanjskih konzultanata (“outsourcing”), osobito za manje organizacije državne uprave. Pravilnik definira kako su njegov predmet državna tijela, tijela jedinica lokalne i područne (regionalne) samouprave te pravne osobe s javnim ovlastima, kada u svom djelokrugu koriste klasificirane podatke, bez da je detaljno definirana ta klasifikacija. U svjetlu te činjenice bilo bi dovoljno da ravnatelj odgovarajuće službe/tijela potpiše izjavu kako ne koristi "klasificirane" podatke te da njegova služba nije predmet ovog Pravilnika. Nisu jasno razgraničene niti odgovornosti, pa tako savjetnik za svoj rad odgovara čelniku tijela ili pravne osobe, a ne Uredu VNS-a koji zapravo provodi edukaciju, motor je cijelog sustava u ovom smislu i prema tome radi zajedno sa savjetnikom na uklanjanju nedostataka.

2.4 Ostala vezana zakonska legislativa

Prema preporuci Hrvatske agencije za zaštitu podataka Vlada Republike Hrvatske je donijela Uredbu o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka. [5] Tom se uredbom propisuje niz mjera koje su sukladne zahtjevima norme ISO 17799, odnosno ISO 27002, te aneksu A standarda ISO 27001. Važan iskorak prema prihvaćanju standardizacije napravljen je pozivanjem na sam standard unutar uredbe. Ovom uredbom propisuje se:

- obveza uporabe uređaja za neprekidno napajanje (UPS)
- korištenje modemskih priključaka za pristup sustavu
- smještanje, postavljanje i ugradnja računala i računalne mreže
- način priključenja računala i ostale informatičke opreme
- način osiguranja posebnih kategorija osobnih podataka

[4] Narodne novine broj 79 iz 2006. godine
[5] Narodne novine broj 139 iz 2004. godine

- pristup prostorijama s računalnom i telekomunikacijskom opremom
- pristup podacima pohranjenim u sustavu
- fizički pristup aplikacijama, računalima i telekomunikacijskom sustavu
- obveza uporabe jedinstvenih korisničkih imena i lozinki
- evidencija i praćenje neovlaštenih pokušaja pristupa
- obveza pohranjivanja zapisa
- sustav kriptološkog osiguranja podataka
- tjedne, mjesečne i godišnje provjere funkcioniranja sustava

Upravljanje kontinuitetom poslovanja nije na adekvatan način obrađeno od strane zakonodavca. Zakon o zaštiti na radu[6] propisuje samoizvođenje evakuacijskih vježbi najmanje svake dvije godine, te propisuje da sve pravne osobe moraju pravovremeno planirati i poduzimati mjere po pitanju planiranja otklanjanja posljedica katastrofa.

Basel II je druga revizija Bazelskih standarda, a to su zapravo preporuke zakonodavcima koje su izdane od strane Bazelskog komiteta za nadzor banaka. Njihova je svrha stvaranje internacionalnog standarda koji nacionalni zakonodavci mogu koristiti pri kreiranju zakonske regulative koja definira koliko kapitala treba biti izdvojeno u obavezne rezerve kako bi se pokrili financijski i operativni rizici banaka. Takav internacionalni standard bi trebao zaštititi financijske institucije od problema koji bi mogli nastati ukoliko jedna banka ili niz banaka ode u stečaj. Logično, čim je veći rizik kojemu je banka izložena, veća je količina pričuvnog kapitala koji banka mora zadržati kako bi osigurala solventnost i općenitu ekonomsku stabilnost.

Hrvatski zakonodavac u Zakonu o bankama[7] definira i operativni rizik koji proizlazi iz neadekvatnog upravljanja informatičkim i pridruženim tehnologijama. Hrvatska Narodna Banka izdala je Smjernice za upravljanje informacijskim sustavom u cilju smanjenja operativnog rizika u ožujku 2006. u kojima vrlo detaljno propisuje načine na koje je moguće implementirati upravljanje informacijskom sigurnošću banke, čime je dala do znanja da se većina operativnog rizika nalazi u radu informacijskih sustava, te da su mjere zaštite informacija najbolji način da se umanji taj rizik.

Temeljna poglavlja koja razmatra taj dokument su sljedeća:

- Temeljna načela sigurnosti informacijskog sustava te elementi upravljanja rizikom
- Upravljanje informacijskim sustavom
- Upravljanje rizikom informacijskog sustava
- Unutarnja revizija
- Sigurnost informacijskog sustava
- Planiranje kontinuiteta poslovanja
- Razvoj sustava i eksternalizacija
- E-bankarstvo, rizici i upravljanje rizicima
- Zaključci i preporuke

Temeljem Smjernica, Hrvatska Narodna Banka izdala je i Odluku o primjerenom upravljanju informacijskim sustavom[8], u kojemu se uz provedbene rokove definira i obveza provođenja onoga što je u smjernicama naznačeno.

U Zakonu o osiguranju[9] neizravno se propisuje potreba za sustavom upravljanja informacijskom sigurnošću, ali se i direktno nominiraju obveze i odgovornosti po pitanju zaštite podataka te njihove privatnosti koje se odnose na zaposlenike osiguravajućih društava, njihove dioničare te povezane osobe.

[6] Narodne novine broj 59 iz 1996. godine
[7] Narodne novine broj 84 iz 2002. godine
[8] Narodne novine broj 80 iz 2007. godine
[9] Narodne novine broj 151 iz 2005. godine

Postavlja se i zahtjev obavljanja unutarnje revizije sigurnosti informacijskog sustava te se taj proces stavlja u direktan odnos s umanjivanjem rizika poslovanja osiguravajućih društava. U Pravilniku o detaljnom obliku i najmanjem opsegu te sadržaju revizorskog prijedloga i revizorskog izvješća društava za osiguranje, koji je objavljen u Narodnim novinama broj 76 od 2006. godine, naglasak je stavljen na upravljanje svim vrstama rizika, detaljno je naznačeno da izvješće mora obuhvatiti i kvalitetu informacijskog sustava osiguravajućeg društva te politiku i organizaciju sigurnosti i zaštite informacijskog sustava, odnosno primjerenost vanjskih, sistemskih i ostalih kontrola.

3. Razmatranje problematike pozicije rukovoditelja sigurnošću i informacijskom sigurnošću[10]

Pozicija CSO-a je pozicija unutar vrhovnog rukovodstva, dok pozicija CISO mora posjedovati najviše moguće stupnjeve samostalnosti, profesionalnog integriteta i nezavisne procjene sigurnosti informacijskog sustava. Kao i prema ostalim ljudima na istoj razini, postoje znatna očekivanja po pitanju obrazovanja i iskustva. Visoki stupnjevi obrazovanja CSO te CISO su vrednovani u svim industrijama i predstavljaju element koji može poboljšati kredibilitet u većini kompanija. Diploma prava, poslovne administracije, računovodstva i financija, menadžmenta sigurnosti, menadžmenta informacijskih sustava ili kriminalistike su poželjne, kao i certificiranje u sigurnosti i povezanim disciplinama. No, povezanost obrazovanja s poslom i certifikati moraju biti u skladu s organizacijskom kulturom. Stoga u obzir treba uzeti i kvalitetu, tip iskustva i ostala direktno povezana postignuća, jer ona predstavljaju važnu referencu za poduzeće koje zapošljava ljude na sigurnosnim funkcijama. Najčešće se traži barem 3-5 godina direktnog iskustva u izrazito rukovodećoj funkciji te demonstrirana sposobnost razvoja i rukovođenja funkcionalnim proračunom kapitalnih i tekućih izdataka.

Hrvatska je mala zemlja, koja ima iza sebe breme rata i niz tipičnih problema za tranzicijske zemlje. Nezaposlenost je visoka, nezaposlenost među visokoobrazovanim stanovništvom najviša u usporedbi sa svim zemljama OECD-a, postotak visokoobrazovanog stanovništva je izrazito nizak (oko 7 %), oko 60 % visokoobrazovanog stanovništva je zaposleno, a radno sposobnog stanovništva ima 38 %. Odljev visokoobrazovane radne snage iz države, osobito iz tehnološkog sektora je značajan i iznosi 30 %, što znači da iz ionako malog fundusa visokoobrazovanih, svaki treći takav Hrvat ne živi i ne radi u Hrvatskoj.

Sve navedeno predstavlja znatne probleme u regrutiranju visokoobrazovane radne snage, što najteže pogađa sektore informatike, te strojarsko, elektro i brodograđevno inženjerstvo. Navedeni problemi nisu jedinstveni samo za Hrvatsku, nego predstavljaju globalnu pojavnost zbog eksplozivnog razvoja kvartarnog i kvinarnog sektora, a osobito su izraženi u nerazvijenim i tranzicijskim zemljama. Iz tog razloga pojavio se niz certifikacija, osobito u informatičkoj industriji, koje pokušavaju premostiti ove probleme, uvodeći obrazovne specijalističke ekvivalente. U području informacijske sigurnosti, organizacije koje se smatraju rezidentnim standardima su ISO, osobito u području standarda ISO 27001, (ISC)2, sa svojim industrijskim standardom - CISSP/CISM, te EC-Council, sa certifikatima vezanim uz područje etičkog hakiranja. Rubne certifikacije koje djelomično svojom metodologijom dodiruju područje informacijske sigurnosti su ITIL v3 te certifikacija PM instituta i PRINCE. Osim visokoškolskog obrazovanja, bilo koja od navedenih certifikacija trebala bi predstavljati prednost i potvrdu teoretskog i praktičnog znanja kandidata za poziciju CISO.

Osim profesionalnih certifikacija, poslijediplomski studij iz informacijske sigurnosti izvodi se na Fakultetu organizacije i informatike u Varaždinu pod naslovom “Sigurnost i revizija informacijskih sustava” s ekvivalentom od 90 ECTS bodova. Na Ekonomskom fakultetu u Rijeci se izvodi poslijediplomski specijalistički studij “Inteligentno elektroničko poslovanje” a na Ekonomskom fakultetu u Zagrebu “Informatički menadžment”, unutar kojih se magistrant može orijentirati na samostalno izučavanje problematike informacijske sigurnosti.

Problem kod formiranja nove funkcije kao što je CISO je nedostatak većeg broja raspoloživih

[10] Značajan dio poglavlja preuzet po Saša Aksentijević, „Integralna zaštitna funkcija unutar poduzeća i sustav upravljanja informacijskom sigurnošću – Saipem Mediteran Usluge d.o.o, Rijeka”,magistarski rad, Ekonomski fakultet u Rijeci, 2008.

kandidata koji imaju praktično znanje. Ljudi koji su došli u dodir s informacijskom sigurnošću vrlo često će na nju gledati isključivo. Oni koji su se u praksi bavili primarno fizičkom zaštitom, stavit će jak naglasak na zaštitarsku službu i identifikacijske procedure, ljudi koji imaju podlogu u izradi aplikacija, orijentirat će se na zaštitu aplikacija, baze podataka i algoritme provjere identiteta, ljudi koji su bili odgovorni za mreže, bavit će se sigurnošću mrežne opreme i mrežnog pristupa, dok će oni zaduženi za sigurnost sistema, informacijsku sigurnost vidjeti primarno kao osiguranje od neautoriziranog pristupa podacima i servisima unutar kompjutorskog sistema. Rijetki su ljudi koji su bili zaduženi za cjelokupnu sigurnost i koji imaju sliku poželjnih obrazaca osiguranja sigurnosti informacijskog, telekomunikacijskog ali i proceduralnog sustava organizacije, a još manje takvih ljudi je raspoloživo na tržištu rada.

Od lokalnih odjela za upravljanje ljudskim resursima ne može se očekivati veće znanje oko specifičnosti regrutiranja funkcija CISO ili CSO, što se opet može nadovezati uz problematiku djelatnosti: odjeli poduzeća koja su inženjerska poznavati će zahtijevane kompetencije za većinski kadar kojim se bave, slično se može reći i npr. za financijski sektor, no niti jedni niti drugi neće poznavati u detalje kompetencije zahtijevane od funkcije CISO. Nažalost, iz praktičnog iskustva s najvećim hrvatskim agencijama za pronalaženje kadrova i savjetovanje u području ljudskih resursa, može se zaključiti da i one pate od kvantitativnog sindroma te da ne posjeduju niti kompetencije, niti značajniju bazu obrazovanih kadrova višeg i visokog menadžmenta koji traže novi poslovni izazov. U kontaktu s jednom od najvećih takvih agencija, na upit vezano uz "headhunting" i eventualnu suradnju po pitanju viših pozicija, zaprimljen je odgovor "da se oni time ne bave", iako medijski istupi i njihova web stranica na sav glas govore protivno tome. Ne bi bilo posve netočno tvrditi da "headhunting" u Hrvatskoj *per se* ne postoji, odnosno da se "headhunting" kod nas često naziva traženje i popunjavanje pozicija nižeg rukovodstva u uobičajenim poslovnim funkcijama (financije, ljudski resursi, tehnički odjeli).

Dodatni problem predstavlja problem kompenzacije. U Hrvatskoj je raspon plaća izrazito nizak, što je posve jasno ukoliko se pogledaju statistički obrađene male razlike između prosječno isplaćenih plaća zaposlenicima sa srednjom i visokom stručnom spremom, a osobito još manja relativna razlika u odnosu na plaće onih koji imaju specifično obrazovanje, poput magisterija, doktorata ili strukovnih ekvivalenata (certifikacije, poslovni Master studiji). Funkcija CISO trebala bi biti izrazito samostalna u svoj funkcioniranju, bilo da se radi o internom CISO-u ili o eksternom stručnjaku koji je implementacijski savjetnik ili eksterni revizor. CSO je funkcija višeg rukovodstva i ukoliko nije tretirana po pitanju kompenzacije adekvatno, dobit će se ili hibrid, ili će se samo zadovoljiti zakonski ili organizacijski okvir. Recimo to napokon jasno - funkcija CSO trebala bi imati menadžerski ugovor, a njena kompenzacija trebala bi biti makar na tragu one CFO-a, CTO-a ili CIO-a, odnosno ekvivalentnih funkcija starijeg rukovodstva unutar organizacije. To je jedini način da prava osoba bude na pravom mjestu, te da organizacija materijalno kompenzira godine iskustva koje su potrebne da bi netko stekao praktična iskustva potrebna za ispunjavanje funkcije CSO, pošto ona ne plaća samo C(I)SO-ov mjesečni rad, nego i njegovo znanje, certifikaciju i iskustvo koje pridodaje organizaciji kao dodanu vrijednost. Kod CISO-a, njegova kompenzacija mora biti ekvivalent istim razinama organizacijske strukture, što obično odgovara razinama voditelja usporedivih odjela. Čak niti velike tvrtke u Hrvatskoj nemaju dovoljno dobro razrađenu klasifikaciju radnih mjesta, dok taj instrumentarij uglavnom nemaju niti agencije specijalizirane za zapošljavanje.

Iz svega izloženog, može se zaključiti da su ograničavajući faktori regrutiranja kadrova za funkcije CISO i CSO sljedeći:

- karakteristike i ograničenja tržišta radne snage
- nesposobnost specijaliziranih agenata na tržištu radne snage da regrutiraju ljude za specifične rukovodeće funkcije
- sposobnost organizacije da jasno komunicira svoje potrebe i interno na vrijeme kanalizira potrebe za formiranjem funkcija CISO/CSO
- nepostojanje standarda kompenzacijske sheme starijeg rukovodstva

Za sada, jedini načini regrutiranja ljudi na ove funkcije ostaje marginalni angažman specijaliziranih agencija koje se reklamiraju kao "headhunting", u nadi da će slučajno naići pogodan

kandidat, te osobni kontakti višeg rukovodstva i rukovoditelja upravljanja ljudskim resursima, odnosno korištenje metoda socijalnog umrežavanja. Iz jasnih razloga, uvoz kandidata iz drugih zemalja vjerojatno nije moguć, jer bi u protivnom bila prilagođena kompenzacijska shema i kandidati bi se mogli naći i unutar države.

4. Uloga informacijske sigurnosti pri promjeni poslovnog okvira u Hrvatskoj – monistički i dualistički poslovni sustavi

Prva tvrtka u Hrvatskoj koja je uvela anglosaksonski, monistički model upravljanja je Arenaturist. Prema novom Zakonu o trgovačkim društvima, koji je 1. travnja 2008. stupio na snagu izmjenom statuta na Skupštini, dioničari su zamijenili Nadzorni i Upravni odbor jedinstvenim tijelom, Upravnim odborom na čijem čelu je neizvršni direktor kojemu obično odgovaraju izvršni direktori koji nisu članovi Upravnog odbora. U takvom sustavu većinski vlasnik osigurava svoj utjecaj na upravljanje društvom putem Upravnog odbora, dok je u dualističkom taj proces osiguran putem Nadzornog odbora. Članove Upravnog odbora izabiru dioničari na Skupštini, osim jednog kojeg imenuje Radničko vijeće. Dok je Nadzorni odbor u dualističkom sustavu bio ovlašten za nadzor upravljanja društvom, monistički sustav ne prepoznaje strogu podjelu između poslovnog upravljanja i nadzora, budući da potonji obavljaju osobe koje nisu u potpunosti odvojene od upravljanja. U dualističkom sustavu dioničar utječe indirektno, putem Nadzornog odbora koji izabire na skupštini dioničara. Nadzorni odbor pak izabire menadžment, odnosno Upravu ili direktora te im na koncu daje ili uskraćuje suglasnost o radu. U načelu, Nadzorni odbor je pasivno tijelo, za razliku od Upravnog odbora koje je aktivno i njegovi članovi svakodnevno doprinose boljem radu poduzeća u svojem području djelovanja Članovi odbora donose smjernice razvoja i upute izvršnim direktorima te ih mogu opozvati, a da ne iznesu važan razlog, jer su za to dovoljne sjednica ili pismena odluka. Upravni odbor postavlja okvir pri obavljanju poslovnih aktivnosti, donosi poslovnu politiku i upravlja operacijama. Takve planove i okvire djelovanja najčešće pripremaju izvršni direktor, ili pojedini odjeli, ili povjerenstva Upravnog odbora, ali uvijek ih usvaja Upravni odbor. Smjernice i upute obvezujuće su za izvršne direktore.

Upravni odbor donosi odluke na sastancima, i to može činiti ako je prisutna najmanje polovica od ukupnog broja članova. Broj članova Upravnog odbora mora biti neparan.

Proces prelaska s dualističkog na monistički sustav nužno bi zahtijevao razvijenu kulturu informacijske sigurnosti unutar korporacije koja mijenja sustav upravljanja. Ispravno postavljen sustav upravljanja informacijskom sigurnošću može poslužiti kao olakšavajući čimbenik jer između ostalog jasno razgraničuje vlasništvo nad informacijama, definira nivoe pristupa i klasificira podatke, prema tome, omogućuje jednostavnije postavljanje novog sustava.

5. Upotreba kvantitativnih metoda za procjenu isplativosti ulaganja u informacijsku sigurnost u Republici Hrvatskoj

Analiza rizika može biti dobar alat organizaciji za stvaranje inventorija cjelokupnosti procesa organizacije. Posljedica procesa stvaranja plana kontinuiteta poslovanja može ustvari u konačnici rezultirati smanjenjem troškova, koje može biti veće od investicije u sam proces. U slučaju naglog i velikog rasta organizacije, određene poslovne funkcije mogu biti zapostavljene, ili može doći do stvaranja birokracije i neefikasnih struktura. Plan kontinuiteta poslovanja može naznačiti postojanje takvih struktura. Efikasno rukovođenje incidentom, osobitom ozbiljnim, može imati pozitivno djelovanje na tržišnu vrijednost tvrtke i odnos uključenih strana. U slučaju važnog sigurnosnog incidenta, tvrtka može biti procjenjivana u odnosu na najvažnije rivale po pitanju načina na koji je incident razriješen. Postojanje efikasnog plana kontinuiteta poslovanja i oporavka rezultira manjim gomilanjem nedovršenog posla tijekom prekida, što naposljetku rezultira bržim oporavkom i povratkom u nominalno stanje. Vrijednost investicije podcrtana je postojanjem plana kontinuiteta poslovanja jer dobar plan minimizira ili posve negira utjecaj negativnih događaja na poslovni rezultat. Prijedlog plana kontinuiteta poslovanja mora biti točan, detaljan, dokumentiran, no ne smije se zaboraviti kako konačna odgovornost za prihvaćanje ili neprihvaćanje investicije u plan kontinuiteta poslovanja i plan oporavka leži na odgovornim instancama u Upravama društva.

U praksi se često kod opravdavanja određene investicije koriste argumenti koji ne bi prošli stroge

kriterije logike u smislu znanosti, pri čemu se ukazuje na značaj informacijske sigurnosti pozivom na činjenicu da je to opće poznato, govori se o tome kako katastrofalno po poslovanje poduzeća ili organizacije može djelovati katastrofa koja je posljedica neprimjenjivanja mjera opće ili informacijske sigurnosti ili se navode primjeri iz prakse. Jasno je da su sve ove metode punovaljano oruđe u rukama profesionalca i u poslovnom odnosu doista predstavljaju dokaz. Na kraju krajeva, doista je jasno kako je ulaganje u informacijsku sigurnost u uvjetima poslovnih okruženja današnjice nužnost. Međutim, ne postoji konkretan razlog zbog kojega se ne bi isplativost ulaganja u informacijsku sigurnost iskazivala kvantitativno, koristeći određene pokazatelje. Teorija vođenja projekata te teorija rukovođenja rizicima daju nam vrijedne alate u tom smislu.

Četiri su temeljna razloga zbog kojih se relativno rijetko u našoj praksi nailazi na studije isplativosti ulaganja u informacijsku sigurnost:

- u slučaju internog rada na razvoju informacijske sigurnosti, odgovorni često moraju ići linijom manjeg otpora zbog nemogućnosti direktnog utjecaja na politiku investiranja (CISO uglavnom nije član uprave, CSO u našim poduzećima i institucijama uglavnom niti ne postoji u upravi). Iz tog razloga u najboljem slučaju poduzimaju se one mjere koje nalaže "najbolja praksa" struke, ono što zaduženi za informacijsku sigurnost najlakše provode samostalno jer s tim imaju prakse te ono što subjektivno "ne košta previše"

- za izradu kvalitetne i točne studije isplativosti, te za otklanjanje čimbenika subjektivnosti pri donošenju odluke o prihvaćanju ili neprihvaćanju rizika, odnosno njegovom uklanjanju tehnološkim i organizacijskim mjerama, potrebna je uska suradnja između uprave i unutrašnjih ili vanjskih kadrova koji vrše procjenu i predlažu rješenja. U tom smislu, onaj tko izrađuje model mora biti opskrbljen ne samo načelno točnim, nego i svježim informacijama koji se tiču financijskog stanja tvrtke, organizacijske sheme, sheme informacijskog sustava, te možda čak i strateške pozicije organizacije, stanja opće sigurnosti i mnogih drugih činjenica koje se tiču poslovanja i funkcioniranja organizacije. To predstavlja dvojak problem: s jedne strane, uprave su s pravom paranoične i daju na uporabu samo one podatke za koje opravdano ili neopravdano smatraju da ih se može dijeliti, iako bi u ovakvim situacijama morale upravo zbog štićenja strateških interesa u potpunosti surađivati. S druge strane, ponekad niti same uprave ne raspolažu točnim informacijama jer su današnje korporacije i neprofitne organizacije toliko velike i kompleksne, da do uprave stižu filtrirane informacije, zbog smanjenja poreznog tereta koristi se politika transfernih cijena te povezanih društava, što je dodatna otegotna okolnost u procjeni rizika i distribuciji informacija

- upitno je koliko oni koji se bave informacijskom sigurnošću vladaju instrumentarijem kvantitativne procjene rizika i studija isplativosti ulaganja u opću i informacijsku sigurnost. Radi se o dosta složenim metodama koje u izradi koriste stohastičnu komponentu, a pri procjeni koristi se i programska podrška koja je izrazito specijalizirana te stoga i skupa. Sve to teret neizrađivanja egzaktnih i kvantificiranih studija isplativosti ravnopravno dijeli između nevoljkih uprava i nedovoljno znanjem i metodama naoružanih konzultanata za informacijsku sigurnost

- kod nas (no, ne zavaravajmo se – i drugdje!) je upravljanje informacijskom sigurnošću tek u svojim začecima, dok se određivanje stohastične komponente u izradi matematičkog modela temelji na dugom i bogatom iskustvu ili na velikom broju uzoraka. Iz tog razloga se konzultanti ne vole upuštati u kvantitativne studije isplativosti, pošto nisu niti sami sigurni u njihovu točnost

U samom početku procesa kvantifikacije rizika i procjene isplativosti ulaganja u informacijsku sigurnost, četiri su osnovna pristupa koji se uspješno mogu koristiti pri izradi taksonomije rizika: Brainstorming, Delphi metoda, diskusijske grupe i nominalne grupe. Pri konkretnoj kvantifikaciji, mogu se koristiti GAP i SWOT analiza te Monte Carlo metoda.

6. Sigurnost informacijskih sustava i financijske institucije

Sigurnost financijskih institucija u Hrvatskoj u ovom trenutku uglavnom se bazira na nužnim zahtjevima regulatora i upitno je koliko prati zahtjeve struke. Naime, 2005., 2006. i 2007. godine došlo je do naglog rasta pokazatelja burzovnog prometa, tržišne kapitalizacije tvrtki izlistanih na Zagrebačkoj burzi, te i likvidnosti. Krajem 2007. godine dolazi do nagle korekcije, pri čemu značajnu ulogu igra

regulator koji preuzima primarno manekensku ulogu i vođen autokratski, niti blizu adekvatno ne ispunjava svoju primarnu ulogu, a to je osiguravanje jednakih uvjeta svima na tržištu kapitala te zaštita ulagača i stvaranje zakonskog okvira. U okviru ove neispunjene zadaće, doneseni su nesmotreno pravilnici koji su dodatno izazvali korekciju na tržištu koja u jesen 2008. godine još uvijek traje. Mirovinski fondovi su počeli naglo povlačiti uloge iz otvorenih investicijskih fondova, potičući rasprodaju dionica. Povrh toga, donesen je pravilnik po kojemu se ograničava mogućnost ulaganja investicijskih fondova u manje likvidne dionice, te je za njih donesen poseban pravilnik o uvjetima trgovanja čime su još više gurnute na marginu jer se njima trguje samo jednom tijekom trgovinskog dana a njihova cijena time još više pada. Naposljetku, neadekvatno štićenje informacija o financijskim izvješćima rezultiralo je očitim "insiderskim" trgovanjem. Dan ili dva prije izlaska financijskih izvješća koja se javno objavljuju na burzi, ljudi koji imaju privilegirane informacije dizali bi ili spuštali cijene dionicama, zauzimajući nove pozicije ili krateći postojeće. Štoviše, zabilježeni su i slučajevi direktnih manipulacija od strane trezora tvrtki, no još uvijek sve teško dokazivo i na granici dobrog gospodarenja kapitalom vlastite tvrtke. Poznat je slučaj kada je predsjednik Uprave jedne velike hrvatske banke prodao svoje bonus dionice neposredno nakon što je dignuta cijena dionicama kupovinom od strane mirovinskog fonda koji nosi naziv te iste banke, i to bez nekog očitog razloga. Naravno, odmah nakon prodaje, cijena dionicama pala je značajno natrag prema realnoj razini.

Regulator je procesirao zanemariv broj slučajeva povlaštenog trgovanja. Bilo bi zanimljivo čuti razlog, točnije, opravdanje za takvu permisivnost. Na rubu humorističnog bili su nastupi regulatora koji je poništavao manipulacijske transakcije vrijedne par tisuća ili par desetaka tisuća kuna, dok se na nominalno slobodnom tržištu događaju očite manipulacije koje su 2008 godine dosegle takve razmjere da se nazivaju "drugom privatizacijom u Hrvata".

Moglo bi se reći kako su ovo porođajne muke tržišta kapitala i dio više stoljeća stare priče u kojoj pri burzovnom susretu onih koji imaju novac i onih koji imaju iskustvo, oni s novcem s burze odlaze s iskustvom dok oni s iskustvom s burze odlaze s novcem. No, zakonite, nezakonite ili granične manipulacije tržištem kapitala čiji je facilitator curenje povlaštenih i povjerljivih informacija u smjeru stranke kojoj se pogoduje, dosta toga govore o stanju i odnosu prema informacijskoj sigurnosti. Na kraju krajeva, samo jedna hrvatska banka ima certificiran svoj sustav upravljanja informacijskom sigurnošću po ISO 27001:2005 standardu i to u izrazito ograničenom opsegu.

Situacijska pozicija korporativne informacijske sigurnosti još je značajnija kada su u igri velike korporativne akcije, poput isplate velikih dividendi ili izvanrednih događaja poput spajanja, podjela ili preuzimanja. Tipični primjer su špekulacije oko izvanredne dividende T-HT-a, preuzimanje INE od strane MOL-a ili curenje informacija iz Braniteljskog fonda oko toga koliko je branitelja povuklo svoje udjele. Sve informacije koje nađu svoj put do medija uzrokuju znatne pomake cijene predmetnih dionica na burzi.

Posljedica je ta da prosječni ulagač, ili onaj institucionalni ulagač koji nema privilegirane informacije, nema istu poziciju u tržišnoj utakmici.

Srećom, zahtjevi koje u svojim nadzorima Narodna banka Hrvatska stavlja pred financijski sektor, osobito banke, po pitanju informacijske sigurnosti u okviru operativnih u praksi su sve veći, što rezultira u povećanom, ali često nevoljkom ulaganju banaka i ostalih financijskih institucija u informacijsku sigurnost.

7. Zaključak

Krajem 2008. godine u Republici Hrvatskoj, zbog približavanja legislativi Europske unije, na snazi se nalazi čitav niz zakona, uredbi i pravilnika koji detaljno reguliraju područje informacijske sigurnosti i pratećih disciplina, odnosno djelatnosti koje podupiru njeno provođenje u korporacijama i organizacijama u skladu s pravilima struke. Zakoni, propisi i uredbe razlikuju se ovisno o tome reguliraju li bazični okvir (npr. Zakon o zaštiti osobnih podataka) informacijske sigurnosti ili specifična, specijalizirana područja (npr. Pravilnik o kriterijima za ustrojavanje radnih mjesta savjetnika za informacijsku sigurnost). Zbog ishitrenog i brzog donošenja zakonske podloge dio tih zakona se u trenutku njihovog donošenja ne provodi, dio je nažalost napisan dosta nestručno i nejasno, a dio se zbog neorganiziranosti aparata koji bi trebao provoditi nadzor u praksi ne provodi.

U državnim tijelima u trenutku nastanka ovog rada ne postoji sistematski postavljen sustav upravljanja informacijskom sigurnošću, odnosno, on se nalazi na svom operativnom začetku. S druge strane, ipak je donesena zakonska podloga, kao temeljni provedbeni okvir.

U Republici Hrvatskoj općenito svijest o potrebi i kulturi informacijske sigurnosti je razmjerno niska. Korporativni dio Hrvatske ima povećani senzibilitet prema informacijskoj sigurnosti, što potječe od stalne borbe profitnih marži koje su pod pritiskom konkurencije, tržišnih prilika i potrebe za pojačanjem postojećih mjera informacijske sigurnosti kako bi se poboljšao tržišni položaj usprkos povećanim ulaganjima. Sprega državnih tijela i privatnog-korporativnog sektora najbolje je regulirana u odnosu regulatora, Narodne banke Hrvatske i financijskih institucija čiji se rad regulira i nadzire, te se u okviru upravljanja operativnih rizika zahtijevaju kriteriji izvrsnosti kod informacijske sigurnosti, oporavka od katastrofe i kontinuiteta poslovanja. Nažalost, u praksi, zbog izbjegavanja zakona i korištenja povlaštenih informacija, vrlo često dolazi do korištenja nedovoljno štićenih osjetljivih informacija i stjecanja osobne koristi. U sektoru srednjih i malih poduzeća, informacijska i opća integralna sigurnosna funkcija uglavnom su marginalizirane, mjere se provode u nužnom opsegu i nestručno i ne postoji sustavni model njihovog inkorporiranja u poslovnu paradigmu.

Pozicija rukovoditelja sigurnošću, odnosno rukovoditelja informacijskom sigurnošću, privilegija je velikih organizacija i podložna je raznim tumačenjima u pogledu potreba za obrazovanjem kandidata, položajem unutar organizacijskog ustroja i kompenzacijskom shemom. Tržište rada nema efikasne mehanizme kojima bi obrađivalo kandidate i kanaliziralo ih u smjeru organizacija koje ih trebaju. No, niti same organizacije još nemaju u potpunosti razvijenu svijest o položaju funkcije CISO/CSO u vlastitom organigramu, ne shvaćaju njihovu funkciju i odgovornosti te potrebu za samostalnošću i neovisnošću kao prerogativima efikasnog ispunjavanja svoje zadaće, a to je osiguravanje poslovnih procesa i protoka informacija. Upravljanje sigurnošću može se pokazati krucijalnim pri korporativnim akcijama i promjeni poslovnog modela iz dualističkog u monistički.

U Republici Hrvatskoj postoje visokoškolske ustanove koje izvode programe vezane uz informacijsku sigurnost, uglavnom poslijediplomske, te su raspoloživi edukacijski kanali ka najvažnijim strukovnim certifikacijama, kao i udruge koje se bave informacijskom i općom sigurnošću. Nažalost, kvantitativne metode za procjenu isplativosti ulaganja u informacijsku sigurnost ne koriste se u značajnijem opsegu zbog nepoznavanja instrumentarija, metoda i relativno niske konkurencije.

8. Popis literature

a. Saša Aksentijević, „Integralna zaštitna funkcija unutar poduzeća i sustav upravljanja informacijskom sigurnošću – Saipem Mediteran Usluge d.o.o., Rijeka”,magistarski rad, Ekonomski fakultet u Rijeci, 2008.

b. Dejan Košutić, “Elementi procjene i upravljanja informacijskim rizicima”, Kvadra Savjetovanje d.o.o., Zagreb, 2007.

c. Narodne novine broj 79 iz 2007. godine

d. Narodne novine broj 79 iz 2006. godine

e. Narodne novine broj 139 iz 2004. godine

f. Narodne novine broj 59 iz 1996. godine

g. Narodne novine broj 84 iz 2002. godine

h. Narodne novine broj 80 iz 2007. godine

i. Narodne novine broj 151 iz 2005. godine