Moćan alat za unapređenje IT-a ili beskorisna papirologija

Branko Pavlović,
član Izvršnog komiteta Delta Generali osiguranja i predsednik Udruženja aktuara Srbije

Tokom pripreme za sertifikaciju potrebno je napisati mnogo dokumenata i to opterećuje zaposlene u kompaniji, koji i bez toga obično imaju previše posla. Ključni kriterijum za razrešenje dileme je situacija posle sertifikacije. U kompanijama u kojima se kasnije zaista poštuju usvojene procedure primećuje se značajno poboljšanje u IT-u, dok u kompanijama gde ne postoji svest o značaju bezbednosti informacija kod zaposlenih, sve ostaje samo mrtvo slovo na mnogo papira

Poverenje klijenata i reputacija kompanije, koji se zasnivaju na različitim vrstama informacija, najvažniji su za uspešno funkcionisanje i tržišnu borbu jedne osiguravajuće kompanije. Ugrožavanje poverljivosti, integriteta ili raspoloživosti informacija dovodi u pitanje njene buduće poslovne aktivnosti i poziciju na tržištu. Zbog toga se u poslednje vreme posebna pažnja poklanja ISO 27000 standardu, posvećenom bezbednosti informacija, koja se odnosi na potrebu kontrole prijema, prenosa, čuvanja, obrade i distribucije informacija.

Jedna od definicija informacije kaže da je to podatak koji ima vrednost za primaoca. Informaciona imovina se deli u 6 kategorija: podaci, softver, hardver, usluge, osoblje i nematerijalna imovina (ugled i reputacija). Standard ISO 27000 se bavi poslovnim rizikom kojem je kompanija izložena ako bilo koje njene informacije dođu u posed nevlašćenim licima koja ih mogu zlouporebiti, promeniti ili učiniti nedostupnim.

Informaciona imovina izložena je raznim pretnjama, koje mogu dovesti do štete. Veličina štete zavisi od ranjivosti imovine. Rizik definišu kombinacija verovatnoće neželjenih događaja i njihovih posledica. Kao i svaki drugi rizik u delatnosti osiguranja i ovaj informacioni rizik se može izbegavati, preneti, smanjiti ili prihvatiti.

Zahtevan standard

Standard ISO 27000 je vrlo zahtevan po pitanju dokumentacije koju je potrebno pripremiti pri uspostavljanju sistema. Naravno, to je samo prvi korak, jer kasnije treba implementirati sva usvojena pravila i obezbediti njihovo poštovanje u svakodnevnom radu. Potrebno je napisati stotine stranica, organizovanih u sledeća dokumenta:

- Deklaracija o politici integrisanog sistema menadžmenta (IMS),
- Poslovnik IMS,
- Procedure koje regulišu upravljanje rizicima po bezbednost informacija,
- Procedure za postupanje u slučaju bezbednosnih incidenata,
- Plan kontinuiteta poslovanja,
- Plan oporavka sistema u slučaju katastrofalnih događaja,
- Upustvo za klasifikaciju informacija,
- Registar informacione imovine,
- Procena rizika, koja se vrši određivanjem ranjivosti i veratnoće nastanka neželjenog događaja svake pojedinačne informacione imovine,
- Mere za upravljanje procenjenim rizicima,
- Izjava o primenjivosti koja opisuje način primene 133 kontrole koje se koriste za smanjenje pojedinačnih rizika i
- Izveštaji o internim proverama i preispitivanju donetih pravila od strane rukovodstva kompanije.

Takođe, svi pojedinačni ugovori o radu se dopunjuju klauzulama o obavezi čuvanja informacija i propisuju disciplinske mere u slučaju nepoštovanja navedenih klauzula.

Priprema svih navedenih dokumenata je zaista zahtevan posao, ali njihovom implementacijom u praksi se unapređuje način upravljanja informacionim sistemom, posebno u sledećim aspektima:

- prava pristupa podacima, odnosno bazama podataka značajno se ograničavaju i svode na minimalna neophodna prava da bi svi poslovni procesi mogli da funkcionišu,
- sprovodi se politika "praznog stola i praznog ekrana", odnosno na stolovima i ekranima ne treba držati ništa što nije neophodno za posao koji se obavlja u tom trenutku,
- promene u karijeri svakog zaposlenog, a naročito odlazak iz kompanije prate se odgovarajućim promenama prava pristupa informacionim resursima,
- ugovorima o radu i ugovorima sa poslovnim partnerima i klijentima se preciziraju obaveze čuvanja informacija,
- server sobe se posebno štiti od neovlašćenog pristupa, požara, poplava, strujnog udara, itd.
- propisuje se dnevno kopiranje baza podataka i čuvanje rezervnih kopija informacija,
- definiše se rukovanje i odgovornost za čuvanje prenosnih medijuma (CD, USB memorije, lap top i sl.),
- uvodi se procedura za uklanje podataka sa informatičke opreme koja se rashoduje,

- uvode se pravila za korisničke lozinke za pristup svim delovima sistema, definišu periodi njihovog automatskog ažuriranja i posebno skreće pažnja zaposlenima da se lozinke nikome ne smeju otkrivati,
- kontinuirano se sprovode aktivnosti na razvijanju svesti zaposlenih o važnosti bezbednosti informacija, itd.

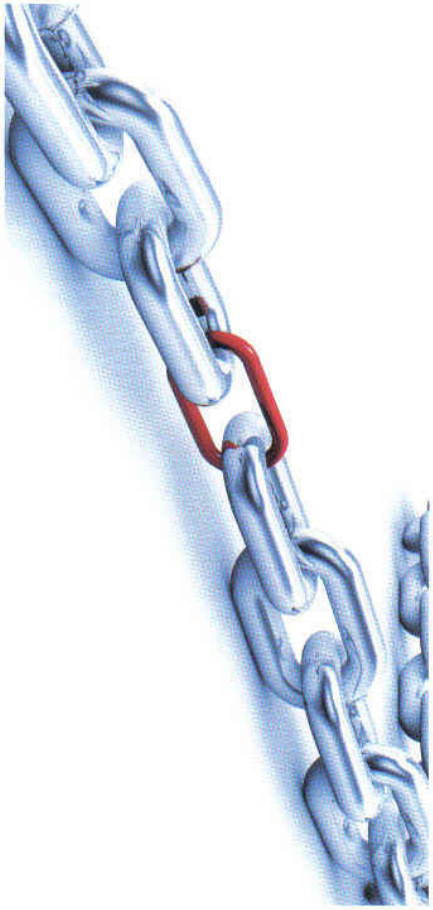
Pozitivni efekti

Kompanija koja odluči da poštuje zahteve standarda ISO 27000 šalje poruku svojim klijentima i poslovnim partnerima da su njihovi podaci sigurni i zaštićeni i da je poslovna politika kompanije usmerena na stalna poboljšanja upravljanja informacijama i uslugama koje pruža. Direktna posledica je veći stepen poverenja i lojalnosti klijenta prema kompaniji.

Pored činjenice da ovaj standard predstavlja najbolju praksu u oblasti zaštite i upravljanja informacijama, postoji mnoštvo drugih pozitivnih efekata koji se dobijaju njegovom primenom:

- povećava se poverenje klijenata i poslovnih partnera u kompaniju,
- razvija se svest zaposlenih o značaju zaštite informacija,
- obezbeđuje se sistem upravljanja rizicima,
- posvećuje se pažnja preventivnom delovanju,
- uređuje se i poboljšava raspoloživost informacija,
- omogućava se učešće na tenderima koji imaju zahtev usklađenosti sa standardima,
- dobija se prestiž na tržištu u odnosu na konkurenciju,
- poboljšava se marketinška promocija kompanije kroz medijske objave o dobijanju sertifikata standarda i isticanju loga sertifikata na kompanijskom promotivnom materijalu,
- smanjuje se pritisak ostalih revizora,
- dobija se još jedno nezavisno mišljenje sertifikacionog tela o kvalitetu rada sa informacijama u kompaniji,
- formira se samoodrživ sistem upravljanja kvalitetom, zahvaljujući čestim preispitivanjima i godišnjim revizijama sertifikacionog tela, itd.

Postojanje navedenih prednosti do sada na domaćem tržištu nije stimulisalo previše kompanija van informatičke delatnosti da uvede standard ISO 27000. Ipak, to će se promeniti u bliskoj budućnosti sa donošenjem nove domaće regulative. NBS je pre nekoliko meseci donela Odluku o minimalnim standardima upravljanja informacionim sistemom finansijske institucije, koja stupa na snagu u 2014. godini. Banke, osiguravajuće kompanije i ostale finansijske institucije će najverovatnije sprovesti zahtevane promene informacionih sistema u skladu sa standardom ISO 27000, ali u ovom trenutku nije jasno da li će pokazati interes za sertifikaciju. U slučaju da se odluče za sertifikaciju, finansijske institucije će na taj način povećati interesovanje i velikog broja sopstvenih dobavljača iz različitih privrednih oblasti za ovaj standard. Promene regulative će takođe zahtevati u budućnosti od državnih institucija i javnih preduzeća primenu ovog standarda.



U zavisnosti od kadrova kojima raspolaže, svaka kompanija treba da donese odluku da li će uvoditi standard sopstvenim snagama ili angažovati konsultante. U oba slučaja je najvažnije znati da će primena standarda posle sertifikacije zavisiti isključivo od zaposlenih u kompaniji

Delta Generali osiguranje je dobilo sertifikat za standard ISO 27000 pre godinu dana. Dobra priprema za implementaciju ovog standarda bila je sertifikacija za standard ISO 9000, koja je u kompaniji izvršena nekoliko godina ranije. Implementacija je trajala oko godinu dana i ostvarena je sopstvenim kadrovskim resursima kompanije. Najviše aktivnosti na uvođenju ovog standarda su imali zaposleni koji se bave informacionim tehnologijama i sistemom kvaliteta, ali su značajan doprinos ovom projektu dali i ostali zaposleni. Projektom je rukovodila Komisija za bezbednost koja je formirana u skladu sa zahtevima standarda i koja je nastavila sa radom i posle dobijanja sertifikata u cilju daljeg unapređenja upravljanja bezbednošću informacija kompanije u budućnosti. Troškovi uvođenja i očekivani godišnji troškovi poštovanja ovog standarda manji su od dva odsto IT budžeta kompanije, godišnje.

Na osnovu iskustva u implementaciji standarda ISO 27000 u Delta Generali osiguranju, savetovao bih zainteresovanim kompanijama da pre odluke o uvođenju ovog standarda pažljivo prouče zahteve za njegovo uvođenje. S obzirom na veliki obim zahteva, važno je razumeti da se ne mogu proskočiti neki zahtevi, koji se možda u prvom trenutku čine nepotrebnim. Takođe, bitno je naći pravu meru u nivou detaljnosti sprovođenja zahteva, jer se u slučaju preterane revnosti riziku je višegodišnja implementacija.

U zavisnosti od kadrova kojima raspolaže, svaka kompanija treba da donese odluku da li će uvoditi standard sopstvenim snagama ili angažovati konsultante. U oba slučaja je najvažnije znati da će primena standarda posle sertifikacije zavisiti isključivo od zaposlenih u kompaniji.

U praksi se može videti da većina kompanija koja uvodi ovaj standard već primenjuje ISO 9000, standard za sistem upravljanja kvalitetom. Sistem upravljanja kvalitetom je manje zahtevan i definiše opšte procese u kompaniji. Tokom njegovog uvođenja zaposleni se obučavaju da implemenitraju i sprovode zahteve ISO standarda i da definišu poslovne procese. Tako se prethodnim uvođenjem standarda ISO 9000 stvara dobra osnova za implementaciju mnogo zahtevnijeg standarda upravljanja bezbednošću informacija, ISO 27000.

Opšti odgovor na dilemu da je ISO 27000 moćan alat za unapređenje IT-a ili samo još jedna beskorisna gomila papira se ne može dati. Tokom pripreme za sertifikaciju potrebno je napisati mnogo dokumenata i to opterećuje zaposlene u kompaniji, koji i bez toga obično imaju previše posla. Ključni kriterijum za razrešenje dileme je situacija posle sertifikacije. U kompanijama u kojima se kasnije zaista poštuju usvojene procedure primećuje se značajno poboljšanje u IT-u, dok u kompanijama gde ne postoji svest o značaju bezbednosti informacija kod zaposlenih, sve ostaje samo mrtvo slovo na mnogo papira. ■