IZAZOVI UPRAVLJANJA INFORMATIČKIM RIZICIMA

Pereža, Dino

SVUČILIŠTE U SPLITU

EKONOMSKI FAKULTET

DIPLOMSKI RAD

IZAZOVI UPRAVLJANJA INFORMATIČKIM RIZICIMA

Mentor: **Student:**

izv.prof.dr.sc. Daniela Garbin Praničević **Dino Pereža**

Split, kolovoz, 2020.

SADRŽAJ

1. UVOD

1.1. Problem istraživanja

U današnjem umreženom svijetu informacijska sigurnost (IS) i upravljanje rizikom (eng. Risk Management (RM)) informacijskog sustava potrebni su za svako poduzeće koje želi preživjeti na tržištu. Bilo da se radi o poštivanju propisa, mogućnostima poslovnog razvoja ili čak poboljšanju upravljanja, poduzeća teže provoditi sigurnosnu strategiju zasnovanu na ISSRM (eng. Information System Security Risk Management) pristupu (Mayer et al., 2018). Cilj ISSRM-a je zaštititi imovinu poduzeća od svih šteta koje mogu nastati slučajno ili namjerno prema sigurnosti IS-a, primjenom pristupa upravljanju rizikom. Njegov glavni cilj je predstaviti različite koncepte i njihove međusobne odnose (Mayer et al., 2008). Isto tako Internet broji svaki dan sve više korisnika. Prema svjetskoj internet statistici broj korisnika na dan 30.06.2019 bio je 4,536,248,808 tj. 4,5 bilijuna korisnika (Internetworldstats.com, 2019). U usporedbi sa 2000. godinom to je porast od 1157%.

Tehnologija se u današnje vrijeme razvija i širi vrlo brzo. Svako masovno širenje pa tako i masovno širenje interneta kao jednog novog globalnog gospodarskog prostora povlači za sobom pozitivne ali i negativne strane. Poduzeća se svakog dana nalaze otvorena prema novim napadima i rizicima koji prijete iz vanjskog svijeta radi informacija koje posjeduju u svom internom sustavu. Pošto poduzeća moraju biti umrežena kako bi mogli poslovati, nemaju opciju da se zaštite na način da se isključe sa internetske mreže. Iz tog razloga moraju svakodnevno raditi na poboljšanju sigurnosti.

Prema Mayer et al., (2018) poduzeća se moraju suočiti sa pritiscima koji povećavaju poteškoće u upravljanju sigurnosnim rizicima, a ISSRM pristup više nije dovoljan. Glavni nedostaci utvrđeni u tradicionalnim metodama ISSRM-a su:

1. Postojeći IS su sve složeniji i podložniji su sve većem broju prijetnji kojima treba upravljati.
2. Poduzeća se neprestano razvijaju, uključujući planiranu evoluciju i / ili neplanirane i nove promjene.
3. Postoji regulatorni pritisak na poduzeće koji uključuje zahtjeve ISSRM-a.
4. Teško je imati jasnu i upravljivu dokumentaciju za aktivnosti ISSRM-a.

5. Metode ISSRM-a su generičke, što dovodi do nedostatka smjernica u procesu ISSRM-a koje bi trebalo slijediti s obzirom na raznolikost konteksta uporabe (postojeći IS ili IS u dizajnu, zahtjevi koji proizlaze iz različitih propisa, od strane tijela upravljanja itd.)

Problem u poduzećima je pronaći pravo rješenje te sistematizirati upravljanje rizikom. Isto tako potrebno je imati procjenu složenosti određenih rizika te otkriti slabe točke unutar poduzeća te ih pokušati zakrpati. Gordon et al. (2005) naglašavaju da sigurnosni rizici često ne nastaju na izričito predviđenim vanjskim granicama informatičkog sustava tvrtke, već na mjestima na kojima zaposlenici i druge osobe imaju pristup unutar samog poduzeća.

Najveći izazov i problem je pronaći izvore rizika, koji mogu biti vanjski, unutarnji ili najčešće kombinacija jednih i drugih, te odgovarajuće rješenje kako tim rizicima upravljati.

1.2. Predmet istraživanja

S obzirom na prethodno navedenu problematiku, predmet istraživanja ovog rada je istražiti što bi to bilo "stanje IT sigurnosti" te koji se sve izazovi javljaju kod upravljanja informatičkim rizicima.

Prema Rudel et al., (2018) sigurnost IT-a je stanje u kojem se povjerljivost, integritet i dostupnost informacija i informacijske tehnologije štite odgovarajućim mjerama. Autori također smatraju da su povjerljivost, integritet te dostupnost informacija "srce IT sigurnosti". Istražit će se trenutno stanje sigurnosti, način upravljanja rizicima te će se ispitati razina i kvaliteta upravljanja informatičkim rizicima u poduzećima putem anketnog upitnika. Potom će se pokušati analizirati rezultati i kao što je već navedeno dati će se uvid u to koji su trenutni izazovi pri upravljanju informatičkim rizicima.

1.3. Cilj istraživanja

Uzimajući u obzir važnost informatičke sigurnosti ovaj rad će imati nekoliko ciljeva:

1. Identificirati informatičke rizike
2. Klasificirati informatičke rizike
3. Procijenit složenost određenih rizika
4. Utvrdit načine za upravljanje informatičkim rizicima
5. Utvrditi izazove sa kojima se poduzeće može susresti pri upravljanju informatičkim rizicima

Budući da teorija ukazuje na važnost informatičke sigurnosti ali isto tako i na rizike koji se susreću u današnje vrijeme prvo će se definirati i objasniti značenje informatičke sigurnosti i informatičkih rizika te će u empirijskom dijelu biti utvrđeno trenutno stanje informatičke sigurnosti i bit će ustanovljeni izazovi sa kojima se poduzeća susreću kod upravljanja informatičkim rizicima.

1.4. Istraživačka pitanja

Glavna istraživačka pitanja ovog rada glase:

P1: Na koje načine poduzeća upravljaju informatičkim rizicima?

P2: Da li su poduzeća spremna na izazove upravljanja informatičkim rizicima?

Koristeći adekvatne statističke i kvantitativne metode te rezultate anketnih upitnika dati će se odgovori na istraživačka pitanja.

1.5. Metode istraživanja

1. Metode koje će se koristit u obradi teorijskog dijela rada su:
    - Metoda indukcije - zaključivanje temeljem analize o pojedinim činjenicama u cilju formiranja zaključka o općem sudu, zapažanje konkretnih pojedinačnih slučajeva i izvođenje općih zaključaka iz njih.
    - Metoda dedukcije - Zaključivanje u kojem se iz općih stavova izvode posebni, pojedinačni stavovi.
    - Metoda analize - raščlanjivanje složenih pojmova, sudova i zaključaka na jednostavnije sastavne dijelove i elemente
    - Metoda sinteze - Objašnjavanje stvarnosti spajanja, sastavljanja jednostavnih misaonih tvorevina u složene, povezujući izdvojene elemente i odnose u jedinstvenu cjelinu.
    - Metoda deskripcije - opisivanje činjenica, procesa i predmeta u prirodi i društvu, bez znanstvenog tumačenja i objašnjavanja
    - Metoda kompilacije - postupak preuzimanja tuđih rezultata znanstveno-istraživačkog rada, odnosno tuđih opažanja, stavova, zaključaka i spoznaja
    - Metoda komparacije - postupak kojim se proučavaju odnosi, sličnosti i razlike između dva predmeta ili pojave, sa ciljem da se izvedu određeni zaključci.

2. Metode koje će se koristit obradi empirijskog dijela rada su:
    - Metoda ankete - postupak u tijeku kojega se odabranim ispitanicima postavlja usmeno ili pismeno određeni broj pitanja, na koja oni daju odgovore, koji se zatim podvrgavaju raznim vrstama analize.

1.6. Doprinos istraživanja

Doprinos istraživanja ovog rada može se sagledati iz više aspekata. Prvo će se sa teorijske strane razjasniti što su to rizici i koji informatički rizici postoje. Identifikacijom i klasifikacijom pojedinih rizika olakšat će se poduzećima da na jednom mjestu imaju detaljan i transparentan pregled što im pomaže u razvijanju akcijskih mjera prema prijetećim rizicima. Isto tako, rad će pružiti procjene određenih rizika na samo poslovanje.

Empirijski dio rada će pružiti dodatan uvid u razinu i kvalitetu upravljanje rizicima u poduzećima trenutno te će također ukazati na izazove sa kojima se poduzeća trenutno susreću pri upravljanju rizicima. Tu će se pružit mogućnost da poduzeća naprave usporedbu sa dobivenim rezultati te da vide na kojoj razini upravljanja rizicima se nalaze.

Planirani anketni uzorak uključivao je 10 srednjih do velikih poduzeća. Međutim navedeni je proširen sa mikro i malim poduzećima koja čine, prema službenim podacima Statista-e, preko 99% ukupnog broja svih poduzeća u EU te su samim time relevantni za ovaj rad. Većina tih poduzeća se pokušava prilagoditi digitalizacija koja se trenutno događa te je bitno vidjeti kako su spremni reagirati na razne rizike.

Poduzeća uključena u empirijski dio rada su poduzeća sa sjedištem ili poslovnim jedinicama na području Republike Hrvatske. Anketnim upitnikom htjela su se obuhvatit poduzeća sa različitim karakteristikama. Tako je upitnik poslan većim, multinacionalnim, poduzećima ali i manjim lokalnim poduzećima.

1.7. Struktura diplomskog rada

Rad se sastojati od nekoliko većih dijelova.

Prvi dio rada je uvodni dio koji sadrži opis problema, predmet te ciljeve istraživanja, postavljene hipoteze, definirane metode istraživanja te strukturu rada.

Drugi dio rada bazira se na identifikaciji i analizi rizika. Poduprto teorijom razrađena je problematika rizika u informatičkom svijetu.

U trećem dijelu rada opisano je kako odraditi procjenu složenosti određenih rizika spomenutih u drugom dijelu rada.

Četvrti dio rada sadrži empirijski dio. Obrađeni su rezultati provedene ankete i dobiven je uvid u razinu i kvalitetu te izazove kod upravljanja informatičkim rizicima u poduzećima.

U petom dijelu, nadovezujući se na empirijski dio, utvrđeni su načini za upravljanje informatičkim rizicima.

Šesti dio sadrži zaključak rada, diskusiju rezultata, sažetak, popis literature, tablice i grafova korištenih u samom radu te provedenu anketu kao prilog radu.

2. OPASNOSTI TE IDENTIFIKACIJA I KLASIFIKACIJA IT RIZIKA

Sigurnost informacija kritično je pitanje za mnoga poduzeća. Brz razvoj mrežnih računalnih sustava u modernom društvu dovodi do sve većeg broja raznolikih i složenih napada na podatke i usluge tvrtke. Međutim, podaci su imovina koja mora biti vjerodostojna da bi bila vrijedna i mora biti nedostupna neovlaštenim stranama. Stoga je potrebno pronaći načine zaštite mreža poduzeća od kriminalnih aktivnosti, zvanih upad. Da bi taj cilj bio postignut, tvrtke koriste različite sigurnosne sustave poput vatrozida, sigurnosnih informacija i sustava upravljanja događajima (eng. SIEM), sustave za otkrivanje upada koji se temelje na domaćinu ili mrežne sustave za otkrivanje upada (Palomares Carrascosa, Kalutarage and Huang, 2017).

Werners i Klempt (2005) tvrde da, kako bi se zajamčila informatička sigurnost u poduzeću, najprije se moraju odrediti zahtjevi za informatičku sigurnost, zatim procijeniti postignuta razina sigurnosti, te utvrditi sve mjere sigurnosti čija implementacija dovodi do optimizacije određene razine sigurnosti. Ako su zahtjevi za sigurnost vrlo visoki, treba odraditi dodatnu analizu i procjenu rizika.

2.1. Definiranje osnovnih pojmova

Za početak, bit će objašnjeno nekoliko osnovnih pojmova koji su često korišteni u radu.

Prvi pojam je rizik. Ovaj pojam je vrlo teško objasnit u jednoj definiciji jer ovisi sa kojeg stajališta ga promatramo. Rizik može biti financijski, osiguravajući, poslovni, kreditni itd. Riječ rizik često se koristi u svakodnevnom jeziku i u medijima, ali podrijetlo riječi nije sasvim jasno. Kluge i Seebold (2011) vjeruju da je moguća povezanost sa španjolskom riječi "risco", što znači litica, i ranom romanskom riječju "rixicare", što znači raspravljati. U ovom radu ćemo definirati što je to rizik informacijske sigurnosti.

„Rizik informacijske sigurnosti je potencijal za neovlašteno korištenje, ometanje, izmjenu ili uništavanje podataka. Takvi incidenti mogu ugroziti zdravlje, narušiti privatnost, narušiti posao, oštetiti imovinu i olakšati druga kaznena djela poput prijevare“ (Spacey, 2020).

Također, rizik informacijske sigurnosti obuhvaća utjecaje na poduzeće i na njegove dionike koji bi se mogli dogoditi zbog prijetnji i ranjivosti povezanih s radom i uporabom informacijskih sustava i okruženja u kojem ti sustavi djeluju (Gantz and Philpott, 2013).

„Upravljanje rizicima je sistematičan analitički proces kojim organizacija otkriva (pronalazi), prepoznaje (identificira), umanjuje (reducira) i nadzire (kontrolira) potencijalne rizike i gubitke kojima je izložena“ (Panian et al., 2007).

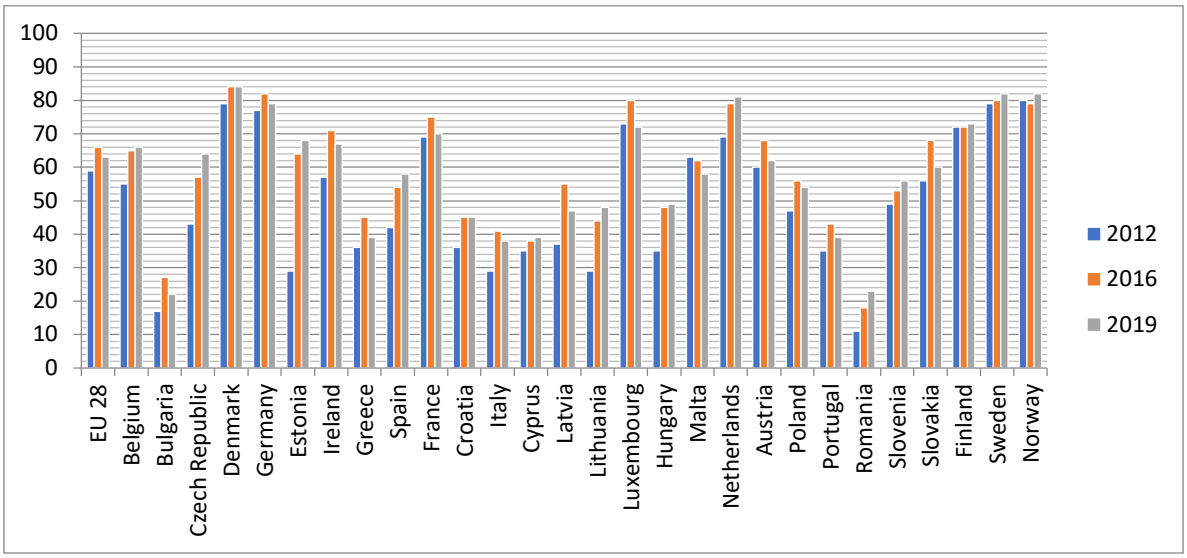
Prema Panian et al., (2007) taj proces omogućuje poduzećima utvrđivanje veličine (ozbiljnosti, težine, razmjera) i učinka potencijalnih gubitaka, vjerojatnosti da će se takav gubitak eventualno i dogoditi te protumjera koje mogu djelovati na smanjenje vjerojatnosti ili veličine gubitka.

„Informacijski sustav (eng. Information System ili IS) je organizirani skup postupaka kojima se prikupljaju, obrađuju, spremaju, pretražuju i prikazuju podatci i informacije značajni za neku organizaciju, ustanovu, društvo ili državu. Sastavni je dio informacijskoga sustava i osoblje obrazovano za rad u sustavu te odgovarajuća oprema. Današnji se informacijski sustavi pretežito ostvaruju uz pomoć suvremene informacijske i komunikacijske tehnologije“ (informacijski sustav | Hrvatska enciklopedija, 2020).

„Informatička (IT) sigurnost odnosi se na osiguravanje sigurnosti svih upotrijebljenih informacijskih tehnologija, tj. svih hardverskih i softverskih sustava (računalni i mrežni sustavi). Cilj je sigurnost obrade i komunikacije informacija koja zahtijeva ispravne procese hardverskih operacija i softvera ili programskih sustava. Dakle, sigurnost podataka i informacija trebala bi se osigurati kroz informatičku sigurnost. Konačno, IT sigurnost trebala bi jamčiti sigurnost tj. ispravnost svih aplikacija koje informatičke tehnologije podržavaju ili izvršavaju“ (Gabriel, 2020).

2.2. Ponašanje i razumijevanje rizika krajnjih korisnika kod e-trgovine

E-trgovina u posljednjih 10 godina dobiva sve više na važnosti kod krajnjih korisnika te samim time i kod poduzeća koja se prilagođavaju zahtjevima korisnika (kupaca). Sve više korisnika naručuje i kupuje preko interneta što je ujedno brže i komotnije ali isto tako izlaže korisnika većem riziku za krađom podataka nego klasičan odlazak u trgovinu.



Grafikon 1 Porast e-trgovine u Europi
Izvor: Izrada autora prema http://appsso.eurostat.ec.europa.eu/nui/submitViewTableAction.do

Grafikon 1 prikazuje usporedno porast e-trgovine prema državama za godine 2012., 2016. te 2019. Svaki stupac označava koliko posto korisnika Interneta je te godine obavilo on-line kupnju. Evidentno je da e-trgovina osjetno raste svake godine, a njen daljnji rast se i dalje predviđa. Gledajući na razini članica EU 28 u 2012. godini je 59% ukupnog broja Internet korisnika obavilo neki oblik on-line kupnje, 2016. godine ih je bilo 66% dok je 2019. godine zabilježen blagi pad ali tj. 63% ukupnih Internet korisnika.

Za dobivanje uvida u poznavanje zaštite krajnjih korisnika pri e-trgovini, u nastavku su opisani rezultati ankete koju je proveo Pereža (2017).

Cilj ankete bio je dobiti sliku o tome koliko današnje društvo zna o Internet sigurnosti te sigurnosti pri e-kupovini.

Vrlo je bitno da web adresu prodajnog mjesta korisnici upisuju sami. Ako prate linkove iz poruka, e-maila, chatova, društvenih mreža, moguće je da će ih odvesti na neke phishing stranice koje će htjeti ukrasti lozinku. Ovdje su rezultati skoro podjednako podijeljeni, no ipak samo 36,3% ispitanika web adresu upisuje samostalno dok njih 13.7% povremeno ulazi na stranice preko linka.

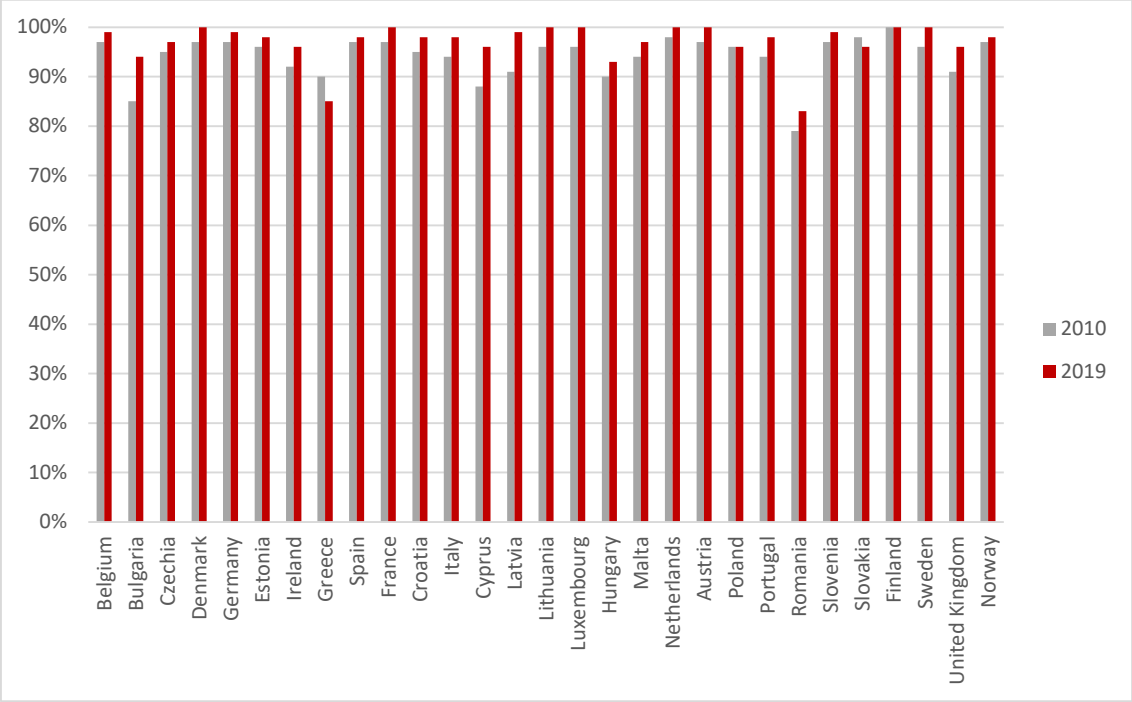
Prije same kupovine mali broj kupaca pročita sve uvjete. Većina ih samo preskoči tj. ako treba označi ih kao pročitane bez da ih detaljnije pogleda. Vrlo je bitno da kupci znaju po kojim uvjetima kupuju i čemu to točno daju njihovu suglasnost. Prema ovoj anketi samo 25% ljudi pročita uvjete kupnje, dok isti taj postotak ljudi nikada ne čita uvjete.

Korištenje iste lozinke kod svih registracija nije dobro iz razloga ako dođe do krađe lozinke, neovlaštena osoba imat će pristup svim računima i stranicama gdje je korištena ta lozinka. Većina ispitanika je svjestan koliku važnost pridonosi ispravan odabir lozinke (korištenje snažne lozinke).

Bazirano na rezultatima ankete, Pereža (2017.) zaključuje da metode sigurnosti koje postoje da nas štite ne znače mnogo ako korisnici nisu educirani o tome kako ih koristit. Zaštita na Internetu je bitna kako za tvrtke , tako i za same krajnje korisnike. Ako zaposlenici u poduzeću nisu pravilno educirani o zaštita i ponašanju na Internetu može doći da raznih vanjskih napada, a ako krajnji korisnik nije upoznat sa mjerama sigurnosti može se dogodit da mu osobni podaci budu ukradeni i zlouporabljeni. Pošto je Internet naša sadašnjost ali i budućnost treba ljude više educirati kako bi se znali samostalno zaštiti kada su online.

2.3. Korištenje informacijskih i telekomunikacijskih tehnologija u poduzećima

Kao što je već u uvodnom dijelu spomenuto, broj korisnika interneta se povećava iz godine u godinu. U današnje vrijeme je internet nešto bez čega poduzeća ali ni krajnji korisnici ne bi mogli poslovati tj. obavljati neke od svojih svakodnevnih obaveza, a njegovo širenje ne staje. Od 2000. godine do 2019. ukupan broj korisnika je porastao za 1157%. Kako raste broj korisnika tako raste i broj poduzeća koje koriste Internet, što je vidljivo iz Grafikona 2.



Grafikon 2 Korištenje internetskih i komunikacijskih usluga prema državama
Izvor: Izrada autora prema https://ec.europa.eu/eurostat/web/digital-economy-and-society/data/database

Grafikon 2 uspoređuje korištenje internetskih i komunikacijskih (ICT) usluga od strane poduzeća u pojedinim državama. Prikazani podaci izraženi su u postotku svih poduzeća registriranih određene godine (2010. ili 2019.) u državi. Kao što je vidljivo svaka država ima porast poduzeća koja koriste ICT usluge, te nam ukazuje na to da su ICT usluge sve više potrebne u svakodnevnom poslovanju. Ali istodobno, kako raste i korištenje ICT usluga, raste i rizik korištenja samih. Što je više poduzeća koji koriste te usluge, to je više opasnosti za njihove podatke na internetu.

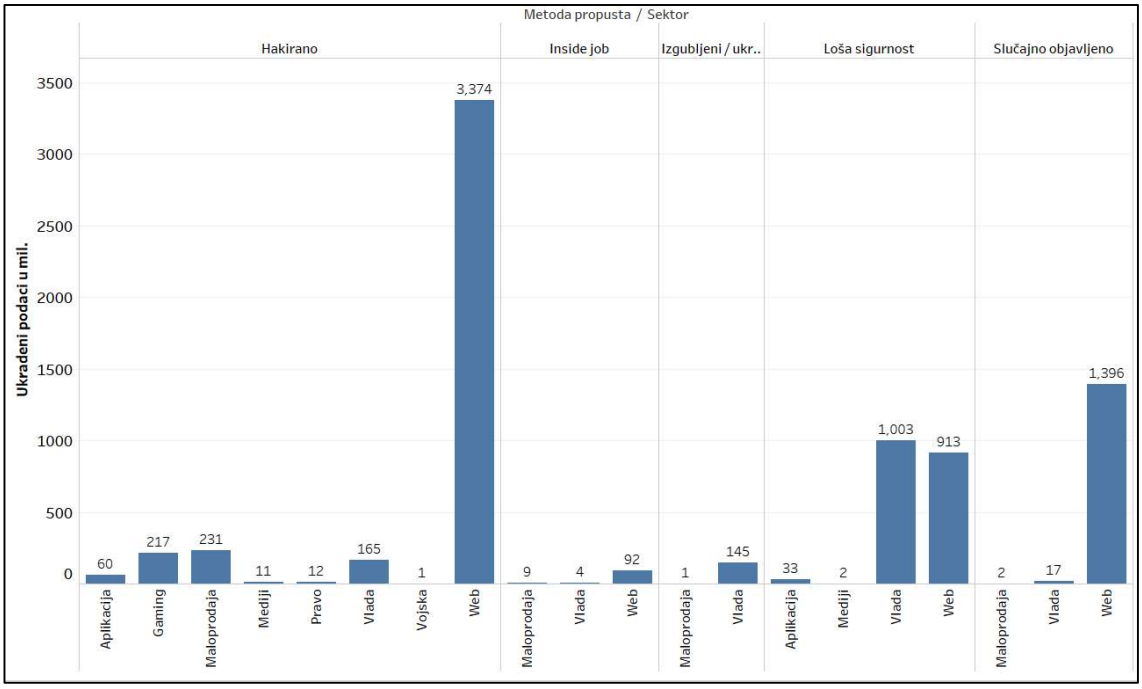
2.4. Incidenti sa krađom podataka

Trenutno najveći problem tj. rizik za poduzeća je krađa podataka. To se odnosi na tajne podatke samog poduzeća ali i na podatke koje poduzeće ima o svojim kupcima tj. korisnicima usluge. Kako bi se barem malo zaštitili privatni korisnici donesena je Opća uredba o zaštiti podataka. Opća uredba o zaštiti podataka (eng. General Data Protection Regulation) novi je zakon o zaštiti privatnosti i osobnih podataka koji će se primjenjivati u svim država članica EU-a (Vodič kroz GDPR za početnike - GDPR Informer, 2020).

Prema anketi koja je odrađena od strane Eurobarometra, 2 od 5 ispitanika strahuje od mogućnost korištenja njihovih osobnih podataka bez prethodne obavijesti (Attitudes on Data Protection and Electronic Identity in the European Union, 2011).

Anketa je pokazala da bi:

- 62 % korisnika za gubitak podataka prije okrivilo poduzeće kojem su dali podatke nego hakere koji su podatke ukrali
- 72 % američkih ispitanika izjavilo je da bi bojkotiralo poduzeće koje nedovoljno pažnje pridaje zaštiti njihovih podataka
- 50 % ispitanika radije bi kupovalo preko poduzeća koje može dokazati da mu je stalo do zaštite podataka



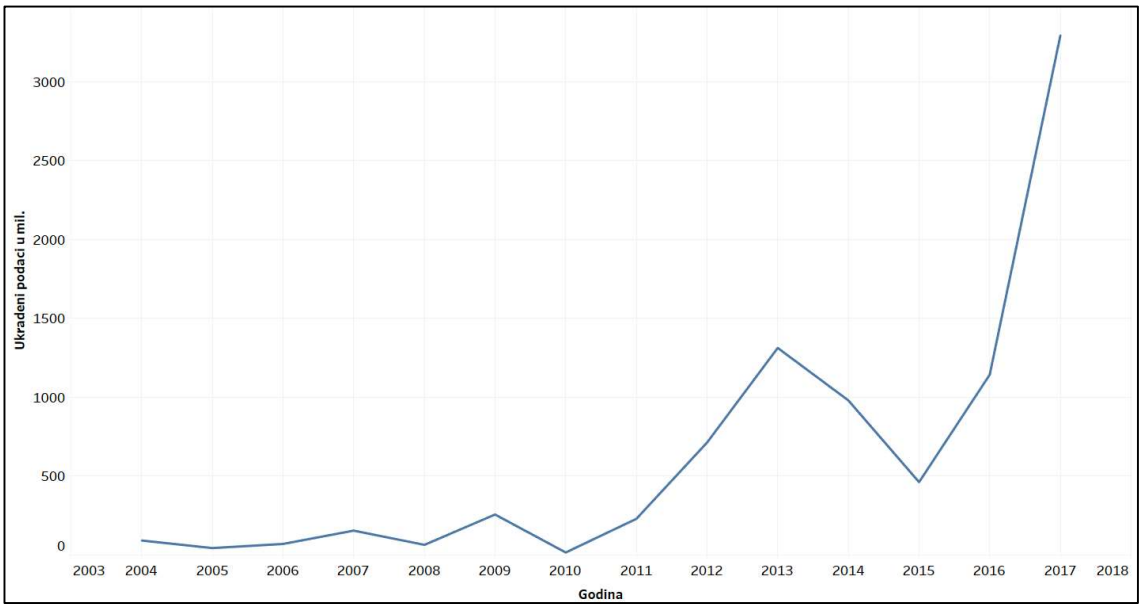
Grafikon 3 Broj ukradenih podataka prema metodi propusta te sektoru
Izvor: Izrada autora prema https://www.kaggle.com/estratic/data-breaches-2004-2017-en-20180218

Na grafikonu 3 je prikazan broj ukradenih podataka u milijunima prema metodi propusta u određenim sektorima. Podaci se temelje na 265 zabilježenih slučajeva krađe podataka diljem svijeta u periodu od 2004. godine do 2017. godine. Daleko najveći rizik pojavljuje se kod poduzeća kojima je primarna djelatnost rad preko web-a (interneta). Najviše podataka, njih 3 347 000 000, je hakirano, njih 1 396 000 je objavljeno slučajno pogreškom poduzeća te nešto

manji broj (913 000) je izložen krađi radi loše sigurnosti. Zabrinjavajući podatak iz grafikona je i sektor vlade koji ima lošu sigurnost, a pohranjuje podatke građana.

Hakeri i hakiranje najveći su problem kada se govori o krađi podataka pa ćemo pobliže objasniti što su to hakeri.

„*Hakeri* su tehnički pametni (sposobni) ljudi u hardverskom i softverskom okruženju. Pronaći će slabosti u sustavima kako bi ukazali na njih ili ih koristili u određene svrhe, kao što su neovlašteni unos ili promjena funkcija. Hakeri u softverskom i internetskom okruženju ne manipuliraju hardverom, već pokušavaju dobiti pristup sustavima. Pristup može biti, primjerice, putem mreže kao što su Internet ili fizička sučelja“ (Was ist ein Hacker?, 2017).



Grafikon 4 Broj ukradenih podataka u mil. od 2004. do 2017. godine
Izvor: Izrada autora prema https://www.kaggle.com/estratic/data-breaches-2004-2017-en-20180218

Grafikon 4 nam prikazuje krivulju kretanja krađe podataka kroz godine. Kao što je i očekivano, broj ukradenih podataka raste kroz godine isto kao što se i Internet razvija tj. proširuje. Sve više korisnika te sve više poduzeća koja koriste Internet znači i sve više osobnih i povjerljivih podataka koji su izloženi rizicima kao krađi.

2.4.1. Stvarni primjeri krađe podataka

U nastavku će biti opisani neki stvarni primjeri sigurnosnih incidenata koji daju pregled širokog spektra mogućih prijetnji. U svakom je primjeru narušeno barem jedno od tri sigurnosna svojstva (dostupnost, povjerljivost, integritet).

Primjer 1:

Na meti krađe su najčešće prijenosna računala te tvrdi diskovi sa osjetljivim i privatnim informacijama. Kako piše Bilton (2009), u Engleskoj je ukraden nešifrirani tvrdi disk s osjetljivim podacima od oko 500 zaposlenika Royal Air Force-a (RAF). Ovaj tvrdi disk sadržavao je pojedinosti o kaznenim osudama zaposlenika, istragama, detaljne pojedinosti dugova, zdravstvene uvjete, zloupotrebe droga, izvanbračne poslove (prijevare partnera) uključujući imena trećih strana. Te bi se informacije mogle upotrijebiti za ucjenjivanje dotičnih pojedinaca i predstavljaju ozbiljan rizik za zaposlenike i RAF.

Primjer 2:

Prema članku od Charette (2008) 2008. godine otvoren je novi terminal na aerodromu Heathrow, a već prvog dana bilo je velikih problema s prihvaćanjem prtljage. Istraga je pokazala da su filtar podataka koji nije uklonjen, a koji je korišten za testnu fazu, i nedovoljan kapacitet poslužitelja odgovorni za ovaj ozbiljan incident. Glavni izvršni direktor British Airways-a, Willie Walsh, priznao je da zna da program ne radi ispravno, ali da je svjesno prihvatio rizik, jer bi odlaganje otvaranja bilo jako skupo. Osim toga, obuka zaposlenika nije se mogla završiti, što je značilo da 20% zaposlenih nije bilo upoznato sa sustavom. U ovom je slučaju rizik je bio prihvaćen, ali očito loše procijenjen.

Primjer 3:

Kako piše Fildes (2009) Hakeri su na web stranici objavili više od 10.000 lozinki od korisnika koji koriste e-pošte pružatelja Hotmail. Te su lozinke dobili putem takozvanog phishing napada. Phishing napadi navode korisnike na lažnu stranicu i traže od njih da upišu njihovu adresu e-pošte i zaporku. Te informacije prevaranti mogu potom koristiti za pristup računima e-pošte žrtve. Ova vrsta napada može biti posebno pogubna za bankovne web stranice.

2.5. Identifikacija rizika

Identifikacija rizika postupak je popisa potencijalnih projektnih rizika i njihovih karakteristika (Bugajenko and Kwong, n.d.).

Identifikacija rizika spada u prvu fazu upravljanja rizikom. Točna identifikacija rizika osigurava učinkovitost upravljanja rizikom. Ako menadžeri rizika ne uspiju identificirati sve moguće gubitke ili dobitke koji se odnose na poduzeće, tada će ti neidentificirani rizici postati neupravljivi (Tchankova, 2002).

Kao što je već napomenuto u radu, koncept rizika posebno je raširen u ekonomiji i stvara problem ako se isti pojam koristi u različitim područjima s različitim značenjima.

Prema temelju uzroka IT-rizici mogu biti:

- Eksterni
- Interni

Eksterne uzroke primarno karakterizira, kao što i sam naziv govori, činjenica da se ne nalaze u utjecaju poduzeća, ali uzrokuju štetu za samo poduzeće. To je posebno vidljivo u slučaju rizika koji proizlaze iz elementarnih nepogoda kao što su npr. požari, zemljotresi, poplave ili oluje. Osim elementarnih nepogoda, tu ubrajamo i opasnosti koje prijete od trećih strana koje na ilegalan način pokušaju doći do podataka (npr. prijevara, pljačke, provale, hakerski napadi itd.) (Hechenblaikner, 2006).

Interni uzroci se nalaze unutar sfere utjecaja poduzeća tj. poduzeće može utjecati na njih te se mogu razlikovati u zaposlenicima, u procesima i u sustavima. Kod zaposlenika možemo navesti da uzrok rizika može biti svjestan i nesvjestan tj. na svjesno i nesvjesno nepoštivanje propisa.

Pod nesvjesno ponašanje spada:

- pogreška
- nemar
- nesposobnost

Svjesnim pogrešnim ponašanjem smatra se:

- prijevara
- krađa
- oštećenje imovine

Također se bilježi rizik neželjene migracije zaposlenika, osobito s ključnih pozicija, i rizik od nedovoljno kvalificiranog osoblja. Ankete u bankarskom sektoru pokazale su da je 61% operativnih gubitaka pripisano zaposlenima (Becker et al., 2010).

Prema Podziņš and Romānovs (2017.) jedan od glavnih razloga zašto je identifikacija rizika vrlo korisna, jest to što pruža opravdanje u slučajevima većih ulaganja u IT. Bez identifikacije rizika poduzeće ne bi moglo doći do kvalitetnog zaključka. Također u ovoj fazi poduzeće prepoznaje prijetnje, ranjivosti i imovinu povezanu s njegovim IT sustavima. Zajedno s fazom procjene rizika, stručnjak za upravljanje rizikom odgovoran je za:

- utvrđivanje vrijednosti imovine
- razinu vrijednosti imovine koju poduzeće štiti te
- razinu prihvaćanja rizika

U prethodnom poglavlju (2.4.) je prikazana statistika propusta i scenariji koji su se određenim poduzećima ili javnim ustanovama dogodili. Ako se ne radi na identifikaciji i procjeni rizika poduzeća se suočavaju sa mogućnosti velikih financijskih gubitaka, gubitaka reputacije pa čak stečaj i bankrot. Da bi se to izbjeglo, potrebno je znati s kakvim se rizicima suočava poduzeće svakodnevno. Stručnjak za upravljanje rizikom mora identificirati i procijeniti poslovne rizike i pružiti ekonomično rješenje za njihovo ublažavanje. Nakon toga poduzeće može pratiti rizike visokog prioriteta kako bi pravovremeno na njih reagiralo.

2.5.1. Cyber rizici

U ovom poglavlju objasnit će se što su to cyber rizici. Spremić (2017) kaže da Cyber rizici predstavljaju vjerojatnost nastanka nekoga neželjenoga događaja (prijetnje) koji u danim okolnostima može uzrokovati štetu, zastoj ili umanjenje intenziteta rada IS-a ili štetu nad informacijama koje su u njemu pohranjene. Dakle Cyber rizici su one vrste informatičkih rizika koje se odnosne na intenzivnu primjenu digitalnih tehnologija u poslovanju. Što poduzeća više koriste suvremene informacijske i digitalne tehnologije, to će biti više izložena cyber i

informatičkim rizicima. A u današnje doba, koje se također ponekad naziva i digitalno doba, sve više poduzeća se okreću tehnologiji te umreženosti preko Interneta.

Postoje različite vrste informatičkih rizika, a to su:

- Strateški informatički rizici:
    - Rizici neusklađenosti poslovanja i informatike, odnosno svi rizici kojima se ugrožavaju strateški poslovni interesi
- Rizici provedbe informatičkih programa i projekata
    - Rizici da ulaganja u informatiku neće biti ispravno vođena, te rizici da provedba tih ulaganja kroz informatičke programe i projekte neće biti učinkovita ili neće doprinijeti stvaranju nove vrijednosti
- Rizici provedbe poslovnih procesa (operativni ili transakcijski)
    - Rizici izmjene informacijske tehnologije u redovitoj provedbi poslovnih procesa
- Infrastrukturni informatički rizici
    - Rizici rada informatičke infrastrukture i opreme i svi ostali rizici koji se odnose na redovito funkcioniranje informatičke infrastrukture

2.5.2. Metodologije identifikacije IT rizika

Podziņš i Romānovs (2017) razlikuju sljedeće metode:

- Povijesna metoda
- Metoda sustavnog pristupa
- Metoda induktivne ili teorijske analize

2.5.1.1. Povijesna metoda

Ovu metodu najčešće koriste osiguravajuće kuće. One promatraju koliki je rizik određene prijetnje na temelju empirijskih podataka o događajima koji su se dogodili ranije. Tijekom prepoznavanja i procjene rizika stručnjaci za upravljanje rizikom trebaju, uvijek kada je to moguće, koristit povijesne podatke. Ono što se dogodilo u prošlosti može uvelike pomoći stručnjaku kako bi se osiguralo da se isti problem ne ponovi u budućnosti. Ali za poduzeća u IT sektoru to ne pomaže uvijek te se moraju osloniti na neke od drugih metoda.

2.5.1.2. Metoda sustavnog pristupa

Ova metoda podrazumijeva uključivanje ljudi koji su stručnjaci za određene teme tj. za određeno područje, ljudi koji stvarno razumiju tehnologiju, imaju razumijevanje o prijetnjama koje nas okružuju i mogu pružiti stručno mišljenje temeljeno na IT temi koja trenutno okružuje poduzeće. Čak u nekim slučajevima prognoziraju događaje koji se još nisu dogodili, ali postoje naznake da će do njih doći. Ovdje je potrebno sagledati ne samo pojedinačne točke neuspjeha, već ponekad čak i agregirane rizike, gdje rizik dolazi iz nekoliko različitih stvari koje djeluju zajedno u formiranju rizičnog događaja.

2.5.1.3. Metoda induktivne ili teorijske analize

Princip je sličan kao kod metode sustavnog pristupa, samo što induktivna metoda pokušava pronaći ono što treba učiniti, pogotovo ako se promatra nešto gdje još nitko nije stručnjak. Kao npr. kada dođe nova tehnologija ili novi poslovni proces. Zbog toga nije moguće uvijek znati koje će se vrste prijetnji pojaviti. No, koristeći sustavni pristup stručnjaka, maštu i sposobnost ljudi da vide kako će stvari izgledati, moguće je izvesti uspješnu induktivnu analizu.

2.6. Životni ciklus informacijske sigurnosti

Simon i Moucha (2019) kažu da je integracija sigurnosnih aspekata u cjelokupni životni ciklus informacijskog sustava ključ za sigurnost informacija. Oni kao tipične probleme iz prakse navode:

1. Nedovoljni zahtjevi
    - Kod natječaja na području IT infrastrukture, sigurnost informacije se ne spominje ili se spomene samo usputno
2. Loš pristup u projektu
    - Kod pristupa takvim informatičkim projektima uvijek se nađe razlog zašto se zanemari sigurnost. Npr. raste pritisak zbog sve kraćih zahtjeva na tržištu, a uspostavljene smjernice upravljanja projektima i procesi smatraju da je sigurnost informacija samo rudimentarna ili je uopće nema.
3. Agilni modeli

- Agilne metode, na primjer prema SCRUM-u, također se vrlo snažno usredotočuju na krajnji proizvod. O novim značajkama i njihovoj primjeni raspravlja se u redovnoj koordinaciji s vlasnikom proizvoda. Sigurnosne značajke također se razmatraju ovisno o vrsti proizvoda, ali mnogi ciljevi sigurnosti i zaštite podataka ne mogu se opisati ili implementirati u atomskim strukturama značajki ili korisničkim pričama ili samo slabo, ali oni ipak zahtijevaju dugoročnu i sveobuhvatnu perspektivu.

4. Privatnost
    - Na području zaštite podataka trenutno još uvijek postoji neizvjesnost u vezi sa time kako postupati sa privatnim podaci prema Općoj uredbi o zaštiti podataka (eng. GDPR - general data protection regulation)

Peltier (2005) o životnom ciklusu informacijske sigurnosti:

Pri provedbi upravljanja rizikom bit će potrebno promatrati taj postupak kao dio tekućeg životnog ciklusa informacijske sigurnosti. Životni ciklus informacijske sigurnosti započinje analizom rizika, kao i kod većine poslovnih procesa. Uprava poduzeća zadužena je da pokaže da se tijekom postupka donošenja odluke poduzimaju pažljive mjere za postupanje s bilo kojim novim zadatkom ili projektom.

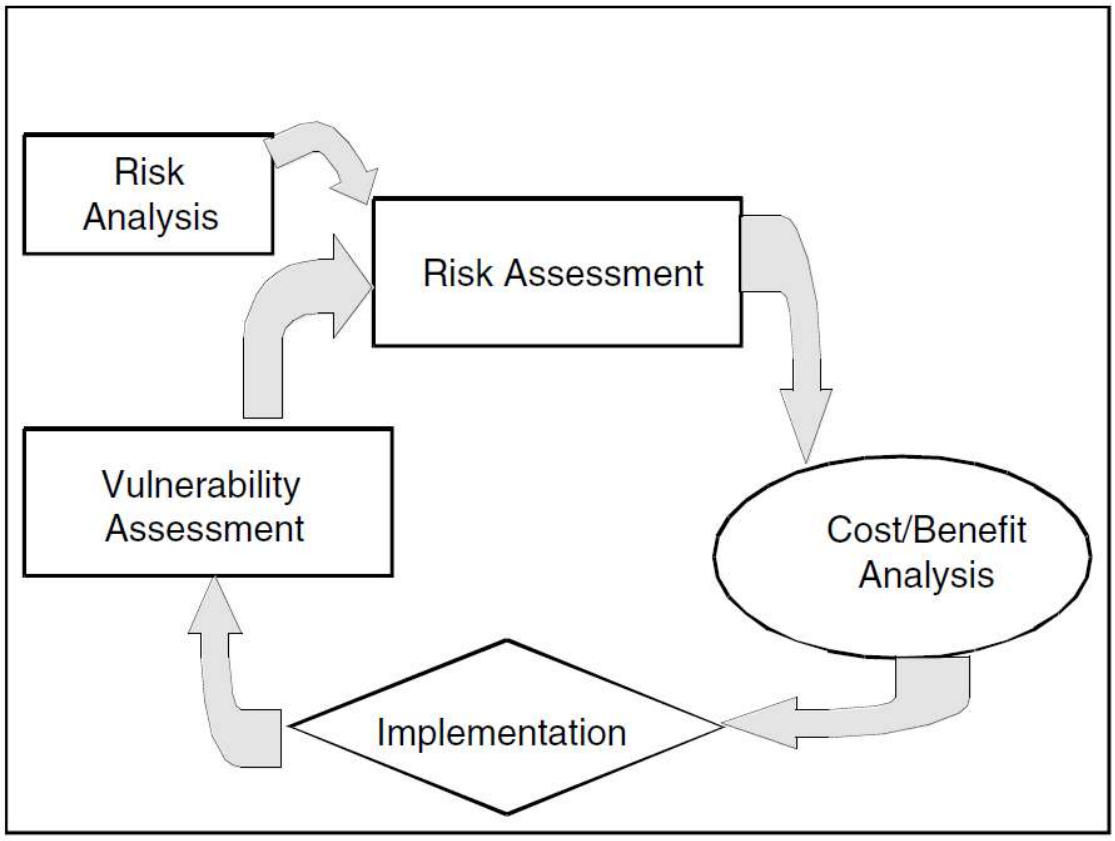
Nakon dovršetka analize rizika, sljedeći korak u životnom ciklusu informacijske sigurnosti je provođenje procjene rizika. Rezultati analize ili procjene rizika koristit će se u dva navrata: kada se treba donijeti odluka i kada se pojavi potreba za ispitivanjem postupka odlučivanja.

Procjena rizika trebala bi omogućiti poduzeću da preuzme kontrolu nad svojom sudbinom tj. da bude spremna nositi se sa rizikom. S učinkovitim postupkom procjene rizika, implementirat će se samo one kontrole i zaštitne mjere koje su zapravo potrebne.

Procjena rizika se provodi kako bi se odredilo koje prijetnje postoje za sami projekt ali i za poduzeće. Te prijetnje se moraju prioritizirati te se moraju odrediti zaštitne mjere i kontrole. Da bi procjena bila efektivna, mora se provesti analiza troškova i koristi (eng. Cost-benefit analysis). Njome se određuje koje kontrole te po kojoj cijeni će pomoći umanjiti rizik za poduzeće te će pokazati da li je taj trošak za poduzeće prihvatljiv. Implementirati zaštitne mjere i kontrole samo zato jer se čine dobre ili zato što ih primjenjuju druga poduzeća, može nanijeti

veliku štetu poslovanju. Svako poduzeće je drugačije te provođenjem odgovarajuće analize rizika, zaštitne mjere i kontrole će udovoljiti specifičnim potrebama poduzeća.

Sljedeći korak, nakon što su zaštitne mjere i kontrole provedene, prikladno je provesti procjenu kako bi se utvrdilo rade li kontrole koje su donesene. U struci informacijske sigurnosti pojam ranjivost (eng. vulnerability) definiran je kao stanje nedostajuće ili neučinkovito upravljane kontrole koja dopušta da se pojavi prijetnja s većim utjecajem i/ili većom učestalošću.



Slika 1 Životni ciklus informacijske sigurnosti
Izvor: Peltier, 2005

2.6.1. Procjena i analiza rizika

Kako mnogi ljudi izjednačavaju procjenu i analizu rizika, za početa će ova dva pojma biti definirana te opisana razlika između njih.

Procjena rizika se koristi kako bi se utvrdilo kakve prijetnje postoje određenoj imovini i povezanoj razini rizika te prijetnje. Prioritiziranje prijetnji tj. uspostavljanje razine rizika pruža poduzeću potrebne informacije za odabir odgovarajućih kontrolnih mjera čija je važnost već spomenuta te zaštitnih mjera ili protumjera kako bi se rizik smanjio na prihvatljivu razinu (Peltier, 2005).

Analiza rizika je tehnika prepoznavanja i procjene čimbenika koji mogu ugroziti uspjeh projekta ili postizanje cilja. Ova tehnika također pomaže u definiranju preventivnih mjera za smanjenje vjerojatnosti pojavljivanja ovih faktora i utvrđivanju protumjera za uspješno suočavanje s tim ograničenjima kad se pojave (Peltier, 2005) .

Iz perspektive modela faktorske analize informacijskog rizika - FAIR (eng. Factor Analysis of Information Risk), analiza rizika često je sastavni dio procesa veće procjene rizika.

Šira procedura procjene rizika obično uključuje (Copeland, 2020):

- prepoznavanje problema koji doprinose riziku,
- analizu njihovog značaja (ovo je mjesto na kojemu se FAIR uklapa),
- identificiranje mogućnosti za rješavanje problema rizika,
- utvrđivanje koja opcija će se najbolje uklopiti (još jedna prilika za primjenu FAIR-a),
- komuniciranje rezultata i preporuka donositeljima odluka.

Proizlazi da se „analiza" odnosi na procjenu važnosti i / ili omogućavanje usporedbe opcija.

Nažalost, velik dio onoga što se danas može vidjeti u upravljanju rizikom je procjena bez smislene (ili točne) analize. Kao rezultat dobiva se slaba informiranost prioriteta i neefikasne odluke.

Svrha svake analize rizika je pružiti donositelju odluke najbolje moguće informacije o izloženosti gubicima i njihovim mogućnostima suočavanja s njim.

Spominjali smo i model FAIR pa ćemo i njega ukratko opisati.

Faktorska analiza informacijskog rizika jedini je međunarodni standardni kvantitativni model informacijske sigurnosti i operativnog rizika (Institute, 2020).

- FAIR pruža model razumijevanja, analize i kvantifikacije cyber rizika i operativnog rizika u financijskom smislu.

- Za razliku od okvira za procjenu rizika koji svoj rezultat usredotočuju na kvalitativne tablice boja ili na numeričke ponderirane ljestvice.
- To gradi temelj za razvoj snažnog pristupa upravljanju informacijskim rizicima.

Dietrich, Reckert i Salomon (2003) smatraju kako upravljanje rizikom nije sam cilj. Također nije namijenjen isključivo odgovoru na pitanje "o čemu trebamo ranije brinuti". Umjesto toga, glavna svrha upravljanja rizikom je objedinjavanje dostupnih znanja o tim problemima i promicanje rane i stalne komunikacije o njima.

Na pitanje zašto bi trebalo odraditi procjenu rizika te kada bi trebalo odraditi analizu rizika, odgovoran daje Peltier (2005):

Ako se odradi formalna procjena rizika ona pruža dokumentaciju koja dokazuje da mu se daje potrebna pažnja. Rezultat procesa analize i procjene rizika općenito se koristi dva puta:

- Prvi će se puta koristiti kada se donesu odluke
    - Za analizu rizika to znači da će se odlučiti hoće li se nastaviti s novim projektom ili ne te
    - Za procjenu rizika to znači da će se odlučiti koje vrste kontrola ili zaštitnih mjera treba primijeniti.
- Drugi put će se rezultati koristiti kad se pojavi problem i poduzeće mora pokazati postupak koji je korišten za donošenje odluka. Dokumentacija stvorena u postupcima upravljanja rizikom omogućit će poduzeću da pokaže tko je sve bio uključen, o čemu se razgovaralo, što se razmatralo i koje su odluke donijete.

Kad god se troše (investiraju) novac ili resursi, potrebno je provesti analizu rizika. Prije započinjanja zadatka, projekta ili razvojnog ciklusa, poduzeće treba provesti analizu potreba za projektom. Razumijevanje pojmova analize rizika i njihova primjena u poslovnim potrebama poduzeća osiguravat će samo izvršavanje potrebnih troškova.

2.6.2. Proces analize rizika

Analiza rizika temelj je na kojem se donose odluke o upravljanju rizikom tvrde Rainer, Snyder i Carr (2015). Također kažu kako je analiza rizika točka u procesu upravljanja rizikom u kojoj nastaje najviše poteškoća. Činjenica da se rizik često mora izraziti interpretacijama čini svaku mjeru rizika izrazito subjektivnom. Visok stupanj subjektivnosti povezan s interpretacijama

rizika znači da je menadžment često skeptičan prema rezultatima analize rizika i da nije voljan donositi važne odluke na temelju njih.

Peltier (2005). o procesu analize rizika kaže:

Za ovaj će postupak biti potrebna analiza troškova i koristi (eng. Cost-benefit analisys). Proces analize troškova i koristi trebao bi sadržavati benefite i mogućnosti imovine ili procesa koji se pregledava.

Dio analize pregledat će troškove projekta. Ti troškovi uključuju:

- nabavu
- razvoj
- rad
- održavanje (npr. razvoj dokumentacije, obuka za korisničku i infrastrukturnu podršku i moguće nadogradnje)
- troškovi pretvorbe ili migracije

Svi ti troškovi se ispituju u novčanoj valuti (npr. Euro, Dolar, Hrvatska kuna) te u uključenosti osoblja.

Iako je važno uzeti u obzir sve elemente troškova prilikom odlučivanja o nastavku sa projektom, prethodno nabrojani troškovi samo su jedna od varijabli. Troškovi o ne provođenju novog projekta također se moraju uzeti u obzir u postupku analize.

Još jedan važan čimbenik koji treba uzeti u obzir u ovom postupku je utjecaj pitanja usklađenosti s propisima. Novi bi projekt trebao, kad god je to moguće, poboljšati regulatorne zahtjeve. Ponekad novu ideju ili koncept napravi odjel, poput marketinga, i dobije podršku i prihvaćanje rukovodstva prije nego što osoblje za infrastrukturu, proračun i sigurnost dobiju priliku za analizu utjecaja projekta.

2.6.2.1. Kvantitativni i kvalitativni pristupi analizi rizika

Pri analizi rizika, autori razlikuju kvantitativni i kvalitativni pristup. U nastavku je prikazan pogled na ovu podjeli iz dvije perspektive. Iz perspektive autora Peltier (2005.) te autora Dietrich, Reckert i Salomon (2003).

Dietrich, Reckert i Salomon (2003) tvrde da za procjenu rizika postoje različite motivacije. S jedne strane, rizici se mogu procijeniti kvantitativno, tj. u novčanim jedinicama. To je posebno potrebno ako se poduzeće želi osigurati od rizika ili ako ga želi bilancirati. S druge strane, a to je dovoljno u većini slučajeva, rizici se mogu procijeniti u odnosu jedan na drugog. Tada govorimo o kvalitativnom pristupu analizi rizika ili općenito o kvalitativnom upravljanju rizikom.

Opis kvantitativnih metoda vrednovanja uključuje veliku primjenu matematike (npr. Aktuarska matematika), no Dietrich, Reckert i Salomon (2003) kažu kako treba napomenuti da se gotovo sve aktivnosti upravljanja rizikom mogu provesti bez kvantitativne analize i to bez ikakvih daljnjih problema.

Kao motivaciju za kvantitativni pristup Dietrich, Reckert i Salomon (2003) spominju:

- određivanje prioriteta samih rizika s obzirom na potrebu za planiranjem
- određivanje prioriteta mjera koje treba provesti s obzirom na redoslijed njihove provedbe

Peltier (2005). opisuje razliku između ova dva pristupa pri analizi rizika na sljedeći način.

U analizama rizika izrađuje se temeljna razlika između kvantitativnog i kvalitativnog pristupa. Kvantitativne metode temelje se na matematičkim modelima statistike i proračunu vjerojatnosti. Njih koriste osiguravajuće kuće za izračun premije osiguranja. Preduvjet za kvantitativnu procjenu rizika je dovoljno poznavanje ulaznih parametara i pristup značajnim povijesnim podacima. Šumski požari i zemljotresi su primjeri rizika koji se mogu relativno kvantificirati u određenim regijama zbog velike količine dostupnih povijesnih podataka. Teže je ili nemoguće kvantificirati rizike o kojima ne postoje povijesni podaci ili rizici koji proizlaze iz novih tehnologija (nanotehnologija, genetski inženjering) ili razvoja (klimatske promjene).

Peltier (2005). o prednostima i nedostacima kvantitativnog pristupa:

Prednosti kvantitativnih modela su:

- Rezultati se temelje na objektivnim matematičkim modelima
- Može se provesti analiza troškova i koristi
- Rezultate je lako razumjeti (npr. Financijski gubitak godišnje)

Nedostaci kvantitativnih metoda su:

- Veliki trošak
- Složeni izračuni
- Trening zahtijeva mnogo vremena
- Aktivnosti izvan okvira teško je razmotriti

Ako se kvantitativni pristup ne može primijeniti, često se koristi kvalitativni pristup. Ovo se manje odnosi na predviđanje budućih događaja, a više na to kako upravljati trenutnim rizicima na ekonomičan način. U ovom se procesu često stvaraju popisi poznatih rizika i njihova vjerojatnost nastanka

Peltier (2005). o prednostima i nedostacima kvalitativnog pristupa:

Prednosti su:

- Jednostavni izračun
- Monetarno vrednovanje imovine nije potrebno
- Velika fleksibilnost procesa
- Lako se mogu uključiti ne-tehničari i stručnjaci koji se bave sigurnošću

Nedostaci su:

- Visoka subjektivnost
- Analiza troškova i koristi može se provesti samo u ograničenoj mjeri

3. PROCJENA SLOŽENOSTI RIZIKA

Prepoznavanje i ocjena rizika zajedno čine komponentu procjene rizika u procesu upravljanja rizikom. Procjena rizika uključuje prepoznavanje rizika i njihovu ocjenu radi utvrđivanja značajnih rizika s kojima se susreće poduzeće, projekt ili strategija. Budući da se upravljanje rizikom u strategiji fokusira na poboljšano donošenje odluka, procjena rizika je glavni doprinos upravljanja rizikom u formuliranju strategije. Iako je procjena rizika vitalno važna, korisna je samo ako se zaključci procjene koriste za informiranje odluka i / ili za identificiranje odgovarajućih reakcija na rizik za vrstu rizika koji se razmatra (Hopkin, 2017).

Kao što postoji više definicija rizika, postoji i mnogo različitih okvira za procjenu rizika.

Talabis i Martin (2013) kažu da se sa velikim brojem različitih okvira može ponekad lako zbuniti, pogotovo kada grupa ili pojedinac inzistiraju na njihovom pravom putu. Baš kao i definicija rizika, i same procjene rizika informacijske sigurnosti imaju zajedničke generičke komponente i aktivnosti koje se dijele u svim okvirima. Poznavanje osnovnih komponenti omogućit će da se uklone temeljna načela iz svih okvira procjene, što će zauzvrat omogućiti provedbu predvidljive procjene rizika bez obzira na pristup, metodologiju ili tehniku koja se koristi.

3.1. Pristup procjeni rizika

U ovom poglavlju prikazano je što Hopkin (2017) kaže o vrstama pristupa procjeni rizika.

Nekoliko je načina kojima se može pristupiti prilikom planiranja postupka procjene rizika. Jedna od ključnih odluka bit će koga uključiti u proces procjene rizika. Ponekad procjenu rizika provodi upravni odbor metodom odozgo prema dolje (eng. Top-down). Procjena rizika se također može obaviti uključivanjem pojedinih članova osoblja i lokalne uprave. Taj pristup naziva se pristup odozdo prema gore (eng. Bottom-up) te je također vrlo važan.

Mišljenje glavnog izvršnog direktora (eng. Chief Executive Officer) je od presudne važnosti, posebno jer pomaže u definiranju cjelokupnog odnosa poduzeća prema riziku. Izvršni direktor moći će pružiti dobro strukturiran pogled na značajne rizike s kojima je poduzeće suočeno. Nedostatak oslanjanja na mišljenje izvršnog direktora jest taj što je fokus vjerojatno na vanjskim rizicima. Iako će predsjednici uprave biti zabrinuti zbog upravljanja financijskim i

infrastrukturnim rizicima, interni rizici možda neće biti njihova glavna briga ili područje interesa.

Općenito, na sveukupni pristup poduzeća procjeni rizika snažno će utjecati odabrane tehnike procjene rizika. Razne tehnike zahtijevaju uključivanje određenih pojedinaca i zahtijevaju poseban pristup provođenju procjene rizika. Važno je da se pristup koji je usvojen podudara s tzv. kulturom poduzeća.

Na primjer, ako poduzeće obično ne održava sastanke i radionice, onda radionica možda nije najprikladniji pristup procjeni rizika. Isto tako, ako se kultura poduzeća uvelike oslanja na izvještaje i pisane radove, to može biti najbolji način provođenja procjene rizika.

3.1.1. Top-down procjena rizika

Tablica 1 Prednosti i nedostaci top - down pristupa

Prednosti	Nedostaci
Vjerojatno će doći do pristupa cijelom poduzeću - rizici pri vrhu će imati utjecaja na cijelo poslovanje	Stariji menadžeri i direktori su više usredotočeni na rizike izvan organizacije
Najvažniji strateški rizici za poduzeće mogu se brzo uhvatiti	Ograničena svijest o internim operativnim rizicima ili međuovisnostima rizika unutar poslovanja
Pokazuje interes od vrha menadžmenta, što rezultira prihvaćanjem aktivnosti upravljanja rizikom na svim razinama	Opasnost da takav pristup postane previše površan, jer viši menadžeri vjeruju da mogu upravljati krizama
Budući da potječe od vrha, vjerojatno će postati dosljedna metodologija u cijelom poduzeću	Novi rizici koji proizlaze iz operativnih aktivnosti poduzeća možda nisu u potpunosti identificirani

Izvor: Izrada autora prema Hopkin (2017)

Tablica 1 daje primjere prednosti i nedostataka provođenja postupka procjene rizika od vrha prema dolje (top-down). Procjena rizika od vrha prema dolje uglavnom će se usredotočiti na rizike povezane sa strategijom, taktikom, operacijama i usklađenosti u tom redoslijedu.

3.1.2. Bottom-up procjena rizika

Tablica 2 Prednosti i nedostaci bottom - up pristupa

Prednosti	Nedostaci
Ostvaruje značajan interes na svim razinama poduzeća.	Malo pažnje će se obraćati na vanjske rizike ili strateške rizike.
Može se odraziti na postojeću radnu shemu i može se raspravljati o utjecajima rizika koji prelaze trenutne operativne rizike.	Vremenski dugotrajno te može demotivirati ako treba više vremena za dobivanje ukupnih rezultata.
Operativno osoblje ima veliku svijest o lokalnim rizicima i njihovim uzrocima, što može izbjeći više razine menadžmenta.	Opasnost da pristup postane previše detaljan, što rezultira silosnim pristupom procjeni rizika.
Metodologija se može mijenjati prema lokalnim normama i kulturi, a to je korisno za multinacionalno poduzeće.	Operativno osoblje možda neće izvijestiti o novim rizicima koji proizlaze iz operativnih aktivnosti poslovanja.

Izvor: Izrada autora prema Hopkin (2017)

Tablica 2 daje primjere prednosti i nedostataka provođenja postupka procjene rizika od dna prema gore. Kao i kod toliko mnogo aspekata uspješne inicijative za upravljanje rizikom poduzeća, organizacija bi trebala odlučiti o protokolima i postupcima za procjenu rizika koji su najprikladniji.

Većina, ako ne i svi okviri procjene rizika, vrte se oko šest aktivnosti koje će biti prikazane u nastavku poglavlja.

3.2. Procjena rizika

Poduzeća koriste procjenu rizika kako bi utvrdila kakve prijetnje postoje određenoj imovini i povezanoj razini rizika te prijetnje. Prioritiziranje prijetnji (uspostavljanje razine rizika) pruža organizaciji potrebne informacije za odabir odgovarajućih kontrolnih mjera, zaštitnih mjera ili protumjera kako bi se rizik smanjio na prihvatljivu razinu.

Autori Wegener, Milde i Dolle (2016) opisuju NIST 800-30 (eng. National Institute for Standards and Technology – NIST) standard kod procjene rizika. Taj standard dijeli postupak upravljanja rizikom na ukupno devet dijelova:

1. Karakterizacija sustava
    - U ovom se koraku prvo prikupljaju sve dostupne informacije o sustavu. To uključuje informacije o podacima pohranjenim u sustavu, o hardveru i softveru koji se koristi, o uslugama koje nudi sustav, o povezanim dokumentima i osoblju potrebnom za rad. Rezultat je "razumijevanje" odgovarajućeg IT sustava, što je preduvjet za daljnje korake.
2. Identifikacija prijetnje
    - Prijetnje uključuju potencijalno sve događaje koji mogu oštetiti IT sustave ili informatičku imovinu. Kasnije u ovom poglavlju će ovaj korak biti detaljnije objašnjen.
3. Identifikacija slabih točaka
    - Slabe točke uključuju sva svojstva informacijskih resursa koja mogu biti iskorištena od trećih strana, što u konačnici uzrokuje štetu poduzeću. Primjeri slabih točaka su npr. pristup otpuštenom zaposleniku koji nije bio blokiran na vrijeme ili pogrešni skupovi pravila vatrozida.
4. Analiza postojećih kontrola i protumjera
    - Na temelju prijetnji identificiranih u koracima 2 i 3, sada se provjerava u kojoj mjeri postojeće kontrole i protumjere smanjuju moguće rizike.
5. Određivanje vjerojatnosti od pojave rizika
    - Da bi se utvrdila vjerojatnost da prijetnja nastupi, prijetnje identificirane u koraku 2 i njihovi uzroci, ranjivosti identificirane u koraku 3 te kontrole i protumjere identificirane u koraku 4 moraju se uzeti u obzir. Kasnije u ovom poglavlju će ovaj korak biti detaljnije objašnjen.
6. Analiza mogućeg utjecaja
    - Da bi se utvrdili mogući učinci, prije svega je potrebna klasifikacija podataka s obzirom na njihovu povjerljivost, cjelovitost i dostupnost, jer je to jedini način da se procijeni kakav bi učinak gubitak ovih ciljeva zaštite mogao imati. Pored ova tri klasična cilja zaštite, osjetljivost, koja predstavlja zahtjeve za povjerljivošću, i kritičnost, koja stoji za dostupnost zahtjeva, često se određuju kvantitativnim i kvalitativnim metodama.
7. Utvrđivanje nastalih rizika
    - Svrha ovog koraka je procjena razine rizika za IT sustav. Određivanje rizika za određeni par prijetnji / ranjivosti može se izraziti kao funkcija:

- Vjerojatnosti pokušaja određenog izvora prijetnje da iskoristi zadanu ranjivost
- Jačine utjecaja trebala bi biti izvor prijetnje koji uspješno provodi ranjivost
- Adekvatnosti planiranih ili postojećih sigurnosnih kontrola za smanjenje ili uklanjanje rizika.

Za mjerenje rizika potrebno je razviti ljestvicu rizika i matricu razine rizika.

8. Preporuke za daljnju kontrolu
   - Tijekom ovog koraka razvijaju se kontrole koje mogu umanjiti ili ukloniti identificirane rizike, ovisno o poslovanju poduzeća. Cilj preporučenih kontrola je smanjiti razinu rizika za IT sustav na prihvatljivu razinu. Sljedeći čimbenici trebaju se uzeti u obzir u preporučivanju kontrola i alternativnih rješenja radi minimiziranja ili uklanjanja utvrđenih rizika:
     - Učinkovitost preporučenih opcija
     - Zakonodavstvo i regulacija
     - Organizacijska politika
     - Operativni utjecaj
     - Sigurnost i pouzdanost
9. Dokumentacija
   - Svi provedeni koraci trebali bi biti dokumentirani. Takozvano "Izvješće o procjeni rizika" navodi sve prijetnje i slabosti utvrđene u prethodnim koracima, opisuje razine rizika korištene za daljnju analizu, a zatim sažima rizike identificirane iz tih baza i njihove moguće učinke. Na temelju tih podataka, tada se daju preporuke za kontrolu i mjere koje su prikladne za učinkovito smanjenje rizika na razinu prihvatljivu za organizaciju ili pojedine poslovne procese.

Peltier (2005). je, za razliku od prethodnih autora, podijelio procjenu rizika u 6 koraka:

1. Definicija imovine
2. Identifikacija prijetnje
3. Određivanje vjerojatnosti od pojave rizika
4. Određivanje utjecaja prijetnje
5. Kontrola rizika
6. Dokumentacija

U nastavku će biti opisani svaki od ovih šest koraka.

3.2.1. Definicija imovine

Da bi bili uspješni, taj prvi korak u postupku procjene rizika mora biti što temeljitiji. Teško će biti provedena točna procjena rizika ako svi članovi tima koji sudjeluju u procjeni nemaju istu viziju onoga što se preispituje.

Tijekom prvog koraka, vođa tima za procjenu rizika i vlasnik moraju definirati postupak, sustav ili imovinu koja se promatra. Ovdje je ključno uspostaviti granice onoga što se preispituje. Većina neuspjelih projekata događa se jer je opseg projekta bio slabo definiran ili zato što se opsegom nije dobro upravljao.

Kao i kod većine projekta, rezultat iz koraka definiranja imovine je postizanje dogovora s vlasnikom o svim relevantnim parametrima. Ovdje je cilj pismeno napisati izjavu o mogućnosti procjene rizika koja se sastoji od dva elementa: izjave o projektu (opsegu) i specifikacija. U izjavi za projekt treba odrediti željeni ishod.

Tijekom izrade izjave o opsegu potrebno je odvojiti dovoljno vremena za raspravu i pojašnjenje parametara projekta. Iako će se ovi parametri razlikovati od projekta do projekta, sljedeći parametri bi se trebali uzeti u obzir:

- svrha
- kupac
- predmeti isporuke
- resursi
- ograničenja
- pretpostavke
- kriteriji

3.2.2. Identifikacija prijetnje

Prijetnje mogu biti definirane kao nepoželjni događaj koji može utjecati na poslovne ciljeve ili misiju poslovne jedinice ili poduzeća. Neke prijetnje nastaju kada se postojeće kontrole, koje su ili primijenjene na pogrešan način ili je prošla njihova korisnost za poduzeće te sada pružaju

slabost ili prijetnju infrastrukturi, mogu iskoristiti kako bi se zaobišlo predviđeno ponašanje kontrole. Ovaj je postupak poznat kao iskorištavanje ranjivosti.

Izvor prijetnje definira se kao svaka okolnost ili događaj koji može uzrokovati štetu imovini koja se promatra. Morat će se kreirati što potpuniji popis izvora prijetnji. Postoje tri glavne kategorije izvora prijetnje:

- Prirodne prijetnje (eksterni) - poplave, zemljotresi, tornada, klizišta, lavine, električne oluje i drugi takvi događaji
- Ljudske prijetnje (interni) - događaji koje su omogućila ili uzrokovala ljudska bića, kao što su nenamjerna djela (pogreške i propusti) ili namjerna djela (prevara, zlonamjerni softver, neovlašteni pristup). Statistički, prijetnja koja uzrokuje najveći gubitak informacijskih resursa i dalje su ljudske pogreške i propusti
- Prijetnje okolišu - Dugotrajni prekidi struje, zagađenje, kemijska izlijevanja, istjecanje tekućine…

Još jedna metoda identificiranja prijetnji je ispitivanje povijesnih podataka. Istražuje se koje su se vrste događaja dogodile i koliko često su se događali.

3.2.3. Određivanje vjerojatnosti od pojave rizika

Nakon što je popis prijetnji finaliziran i tim se dogovorio o definicijama svake prijetnje, tada će biti potrebno utvrditi kolika je vjerojatnost da će se prijetnja dogoditi. Tim za upravljanje rizikom htio bi utvrditi opću vjerojatnost koja ukazuje na mogućnost da će se potencijalna prijetnja dogoditi. Bit će potrebno utvrditi definicije vjerojatnosti i niz drugih ključnih pojmova.

Tipovi vjerojatnosti:

- Velika vjerojatnost - Velika vjerojatnost da će se prijetnja pojaviti
- Srednja vjerojatnost - Moguće je da se prijetnja može pojaviti
- Mala vjerojatnost - Malo je vjerojatno da će se prijetnja pojaviti

		Utjecaj		
		Velika	Srednja	Mala
Vjerojatnost	Velika	A	B	C
	Srednja	B	B	C
	Mala	C	C	D

Legenda:
A - Mora se provesti korektivna akcija
B - Treba provesti korektivne akcije
C - Zahtijeva promatranje
D - Trenutno nije potrebno ništa poduzeti

Slika 2 Primjer 1 matrice vjerojatnosti i utjecaja
Izvor: Izrada autora prema Peltier (2005).

3.2.4. Određivanje utjecaja prijetnje

Nakon utvrđivanja vjerojatnosti da se prijetnja pojavi, bit će potrebno utvrditi utjecaj koji će potencijalna prijetnja imati na poduzeće.

Rezultati pregleda vjerojatnosti i utjecaja su identifikacija razine rizika koja se može dodijeliti svakoj prijetnji. Jednom kada se utvrdi razina rizika, tim može utvrditi odgovarajuće akcije. Koraci 3 i 4 određuju vjerojatnost da se može dogoditi određena prijetnja te jačinu učinka ako se prijetnja dogodi. Postupak procjene rizika može se provesti ponovno nakon odabira kontrole (peti korak). To će omogućiti timu da utvrdi pruža li odabrana kontrola željeno smanjenje razine rizika.

Proces razine rizika zahtijevat će upotrebu definicije utjecaja kao i matrične tablice koja će omogućiti timu da utvrdi razinu rizika. Slijedi definicija uzorka utjecaja:

- Utjecaj je mjera koja označava veličinu gubitka ili štete na vrijednost imovine. Razine utjecaja koje razlikujemo su:
    - Veliki utjecaj - zatvaranje kritične poslovne jedinice što dovodi do značajnog gubitka poslovnog i korporativnog imidža ili dobiti

- Srednji utjecaj - Kratki prekid kritičnog procesa ili sustava koji rezultira ograničenim financijskim gubitkom pojedine poslovne jedinice
- Slab utjecaj - Prekid bez financijskog gubitka

Još jedan primjer tablice vjerojatnosti i utjecaja mogao bi se stvoriti s utvrđenim razinama rizika kao što je prikazano na slici 4.

		Utjecaj		
		Velik	Srednji	Mali
Vjerojatnost	Velika	Velik	Velik	Srednji
	Srednja	Velik	Velik	Srednji
	Mala	Srednji	Srednji	Mali

Legenda:
Velik utjecaj - Mora se provesti korektivna akcija
Srednji utjecaj - Treba provesti korektivne akcije
Mali utjecaj - Nije potrebno ništa poduzeti

Slika 3 Primjer 2 matrice vjerojatnosti i utjecaja
Izvor: Izrada autora prema Peltier (2005).

3.2.5. Kontrola rizika

Nakon što je dodijeljena razina rizika, tim će utvrditi kontrole ili zaštitne mjere koje bi mogle otkloniti rizik ili barem smanjiti rizik na prihvatljivu razinu.

Potrebno je uvijek imati na umu da je jedan od ciljeva procjene rizika izraditi dokumentaciju prilikom donošenja poslovnih odluka. Stoga će biti važno utvrditi sve kontrole i zaštitne mjere za koje tim vjeruje da bi mogli smanjiti rizik na prihvatljivu razinu. Na taj način tim će moći dokumentirati sve mogućnosti koje su razmatrane te na kraju donijeti bolju odluku.

Pri odabiru bilo koje vrste kontrole bit će potrebno izmjeriti operativni utjecaj na poduzeće. Svaka kontrola na neki će način imati utjecaj. To bi mogli biti izdaci za samu kontrolu. To bi mogao biti utjecaj produktivnosti i prijelaznog vremena. Iako je kontrola novi postupak, učinak na zaposlenike mora se preispitati i upotrijebiti u odlučivanju hoće li ih provoditi.

U pitanju je sveukupna sigurnost intelektualnog vlasništva poduzeća. Posljednje što tim za upravljanje rizikom želi učiniti je provedba kontrole koja za poduzeće predstavlja veći rizik.

Rashodi na kontrole moraju se uravnotežiti u odnosu na stvarnu poslovnu štetu. Dobro pravilo je da, ako kontrola košta više od imovine koja bi se trebala zaštiti, tada će povrat ulaganja vjerojatno biti nizak.

Da bi bio učinkovit, postupak analize rizika trebalo bi se primijeniti na čitavo poduzeće. Odnosno, svi elementi i metodologija koja čine postupak analize rizika trebaju biti standardni, a sve poslovne jedinice osposobljene za njegovu upotrebu. Rezultat analize rizika dovest će poduzeće do prepoznavanja kontrola koje bi trebale smanjiti razinu pojavljivanja prijetnji.

3.2.6. Dokumentacija

Nakon dovršetka procjene rizika, rezultati moraju biti dokumentirani u standardnom formatu, a izvještaj se izdaje vlasniku. Ovo će izvješće pomoći višem menadžmentu i vlasniku poduzeća da donose odluke o promjenama politike, postupaka, proračuna i sustava te upravljanja. Izvješće o analizi rizika trebalo bi predstaviti na sustavan i analitički način koji procjenjuje rizik kako bi viši menadžment razumio rizike i dodijelio resurse za smanjenje istih na prihvatljivu razinu.

3.3. ISO 27000 norme - standardi kod informacijske sigurnosti

Obitelj standarda ISO / IEC 270001, poznata i kao serija ISO 27000, niz je najboljih praksi koje pomažu poduzećima da poboljšaju svoju informacijsku sigurnost. Standardi su izdani od strane međunarodne organizacije za standardizaciju (eng. International Organization for Standardization) i međunarodne elektrotehničke komisije (eng. International Electrotechnical Commission), te serija objašnjava kako implementirati sustav upravljanja informacijskom sigurnošću (eng. Information security management system). ISMS je sustavni pristup upravljanju rizicima, koji sadrži mjere koje se odnose na tri stupa informacijske sigurnosti: ljude, procese i tehnologiju. Serija se sastoji od 46 pojedinačnih standarda, uključujući ISO 27000, koji pruža uvod u obitelj kao i pojašnjenje ključnih pojmova i definicija (Irwin, 2019).

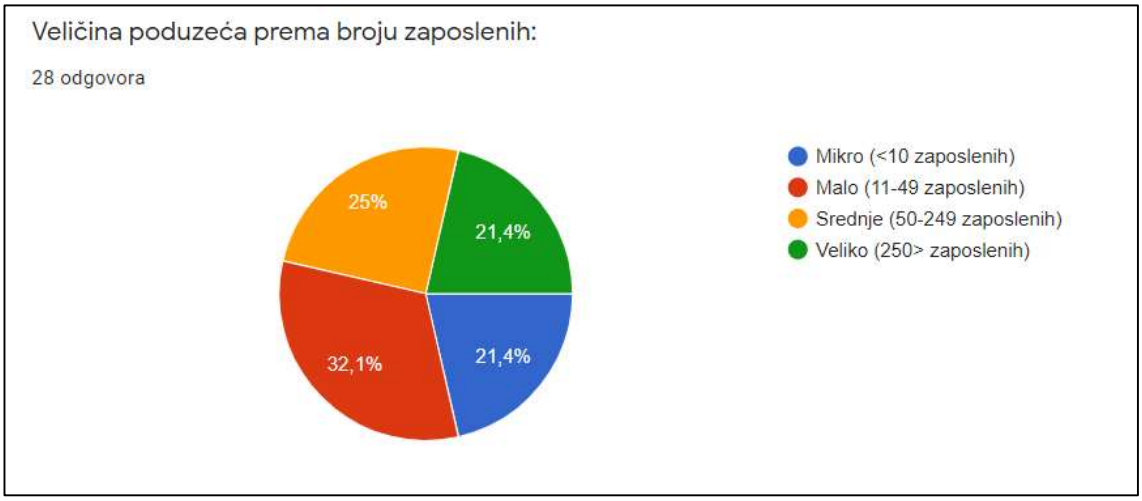
Obitelj ISO 27000 normi obuhvaćaju popis kontrola koje treba implementirati u informacijski sustav kako bi se sigurnosni rizik sveo na prihvatljivu razinu. ISO 27001 središnji je standard serije ISO 27000, koji sadrži zahtjeve za implementaciju ISMS-a.

4. EMPIRIJSKO ISTRAŽIVANJE

U empirijskom dijelu rada korišteno je anketno istraživanje. Cilj ankete bio je saznati da li poduzeća vode brigu o mogućim rizicima koji ih okružuju te ako da, na koji način i u kojoj mjeri ih identificiraju i analiziraju. Isto tako putem ankete dobit će se struktura poduzeća prema veličini te rezultati koji će pokazati koja poduzeća su najspremnija nosit se sa rizicima koji im u današnje vrijeme prijete. Anketa je provedena online putem Google obrazaca. Obuhvatila je uzorak od 28 poduzeća te je sadržavala 21 pitanje. Ispunjavanje anketnog obrasca bilo je u potpunosti anonimno. U nastavku će biti prikazani te analizirani rezultati dobiveni putem anketnog obrasca.

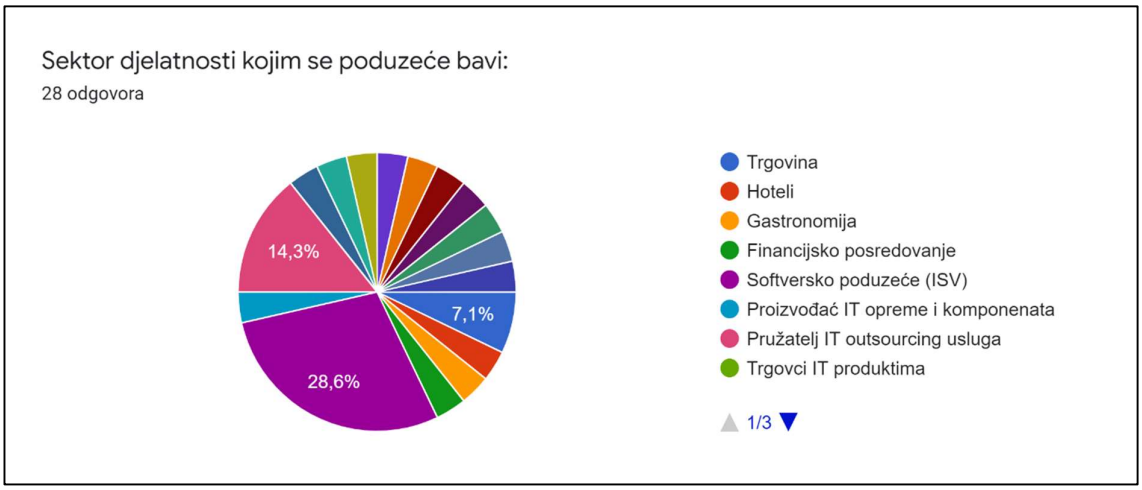
4.1. Prikaz rezultata ankete

U prvom dijelu ankete ispitanici su imali mogućnost višestrukog odabira. Na početku je prikazana strukturu poduzeća iz kojih ispitanici dolaze prema broju zaposlenih.



Grafikon 5 Veličina poduzeća prema broju zaposlenih
Izvor: Izrada autora prema anketi

Iz grafikona 5 evidentan je podjednak postotak tj. podjednaka zastupljenost poduzeća (sudionika) koji su ispunili upitnik. Ipak, njih najviše, 32.1% je zaposleno u malom poduzeću. Mikro i veliko poduzeće jednako su zastupljeni sa 21,4%.

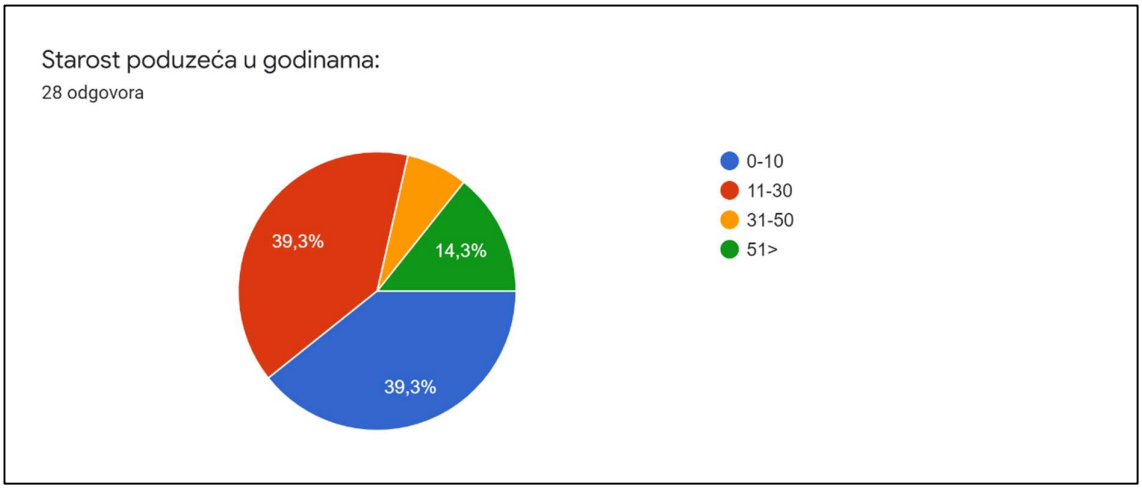


Grafikon 6 Sektor djelatnosti kojim se poduzeće bavi
Izvor: Izrada autora prema anketi

Sa grafikona 6 uočljivo je kojim se djelatnostima bave poduzeća u kojima ispitanici rade. Tako su najviše, sa 28,6% zastupljena softverska poduzeća (eng. (Independent Software Vendor – ISV). Iza toga slijede pružatelji IT outsourcing usluga sa 14,3% te trgovina sa 7,1%. Sve ostale djelatnosti zastupljene su podjednako. Popis svih djelatnosti kojima se poduzeća bave je:

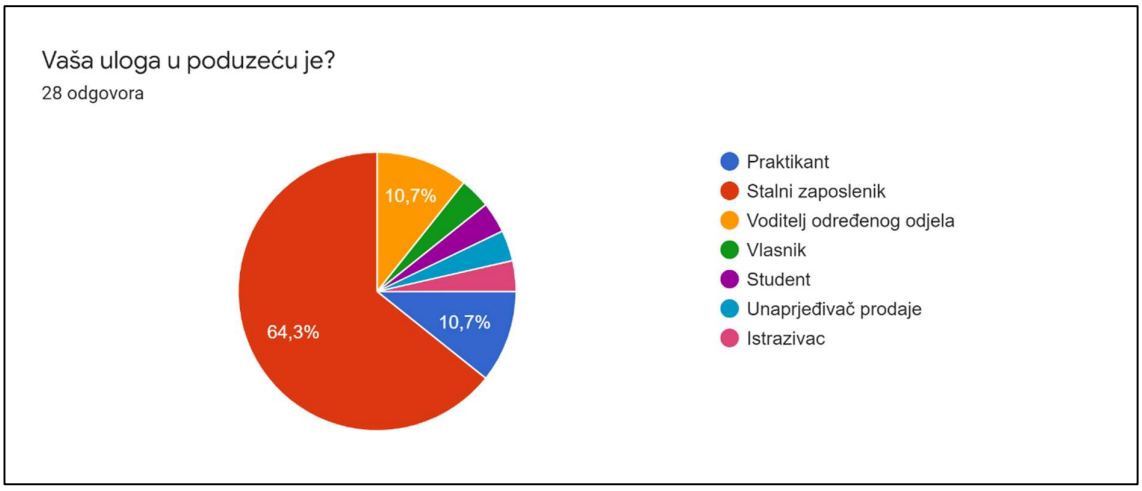
- Trgovina – 7,1%
- Hoteli – 3,6%
- Gastronomija – 3,6%
- Financijsko posredovanje – 3,6%
- Softversko poduzeće (ISV) – 28,6%
- Proizvođač IT opreme i komponenata – 3,6%
- Pružatelj IT outsourcing usluga – 14,3%
- Trgovci IT produktima – 3,6%
- Farmacija – 3,6%
- Telekomunikacije – 3,6%
- Nekretnine – 3,6%
- Consulting – 3,6%
- Zaštita na radu – 3,6%
- Turizam – 3,6%
- Marketinška agencija – 3,6%
- Autoindustrija – 3,6%
- Mesna industrija – 3,6%

- Građevinarstvo – 3,6%
- Projektiranje – 3,6%
- Projektiranje elektroenergetskih mreža – 3,6%



Grafikon 7 Starost poduzeća u godinama
Izvor: Izrada autora prema anketi

Prema starosti poduzeća vidimo da prevladavaju mlada poduzeća starosti do 10 godina te starosti između 11 i 30 godina. 79,3% mlađe je od 30 godina, samo 14,3% poduzeća ima tradiciju dužu od 50 godina.

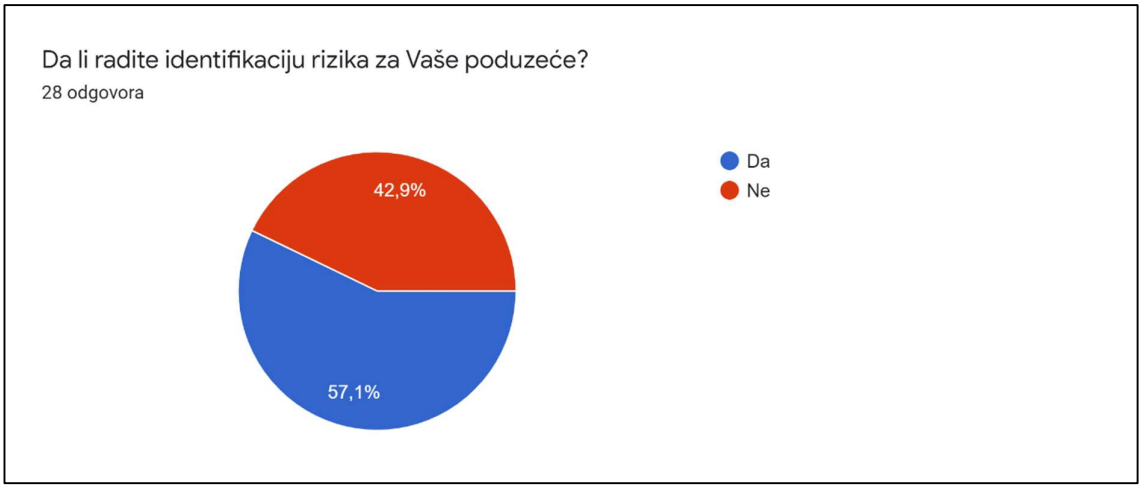


Grafikon 8 Uloga ispitanika u poduzeću
Izvor: Izrada autora prema anketi

Anketa se također osvrnula na ulogu ispitanika u samom poduzeću kako bih se bolje shvatilo razumijevanje o riziku od strane samih zaposlenika.

Ispitanici su u 64,3% slučajeva stalni zaposlenici te ih u jednakom postotku sa 10,7% prate praktikanti te voditelji odjela. Ostale uloge su zastupljene sa 3,6%.

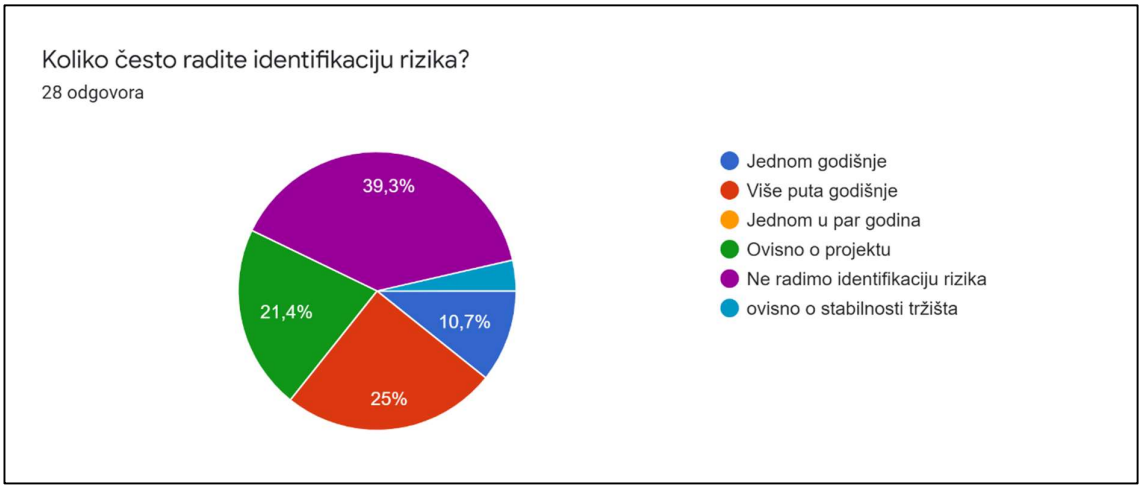
Idući blok pitanja za ispitanike odnosio se na identifikaciju rizika u poduzeću.



Grafikon 9 Postotak poduzeća koja rade identifikaciju rizika
Izvor: Izrada autora prema anketi

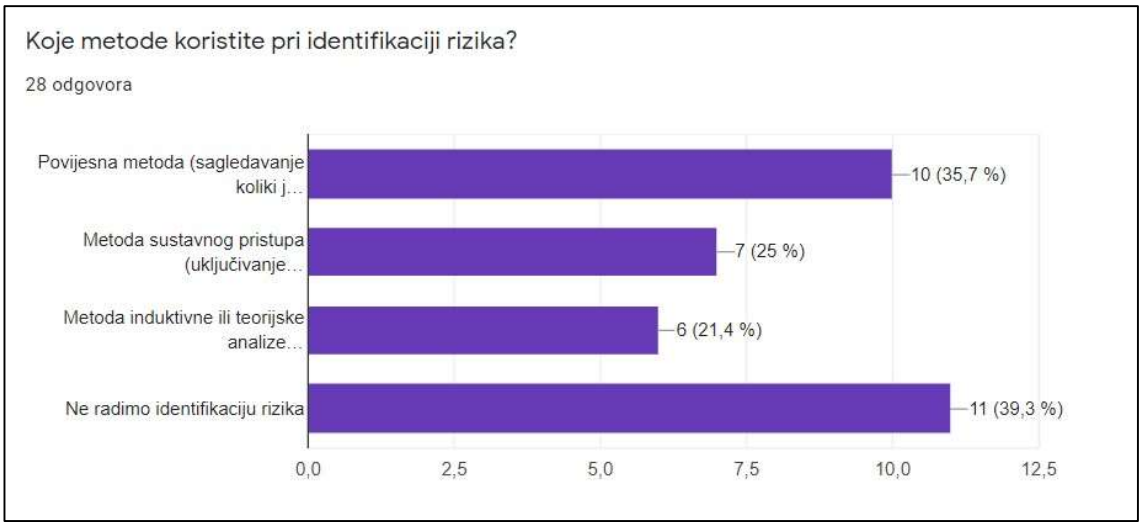
Od ispitanih poduzeća, njih 57,1% tj. 16 poduzeća radi identifikaciju rizika, ali kao što će se vidjeti na grafikonu 10, taj broj je ipak veći za 1 tj. 17 poduzeća radi identifikaciju rizika. Jedan odgovor koji je negativno označen ovdje u detaljnijoj analizi pokazuje da to poduzeće ipak radi identifikaciju rizika ovisno o projektu te je taj odgovor ovdje uzeti kao greška pri ispunjavanju ankete. Ispravni postoci su sljedeći:

- Poduzeća koja rade identifikaciju rizika – 60,7%
- Poduzeća koja ne rade identifikaciju rizika – 39,3%



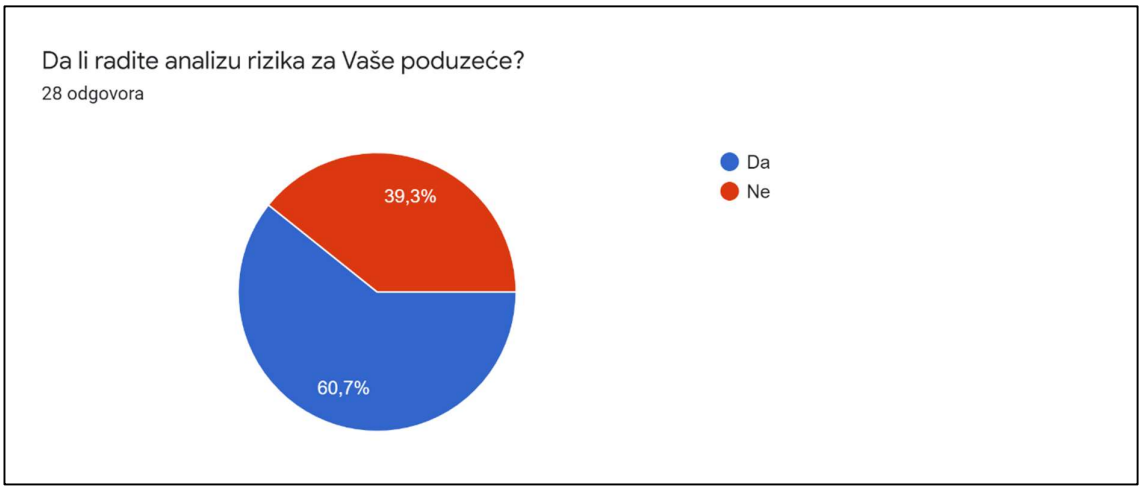
Grafikon 10 Učestalost izrade identifikacije rizika
Izvor: Izrada autora prema anketi

Poduzeća koja rade identifikaciju rizika većinom to rade više puta godišnje (njih 25%) ili u ovisnosti o projektu (njih 21,4%). Jednog godišnje to radi 10,7% poduzeća dok 3,6% poduzeća to radi ovisno o stabilnosti tržišta.



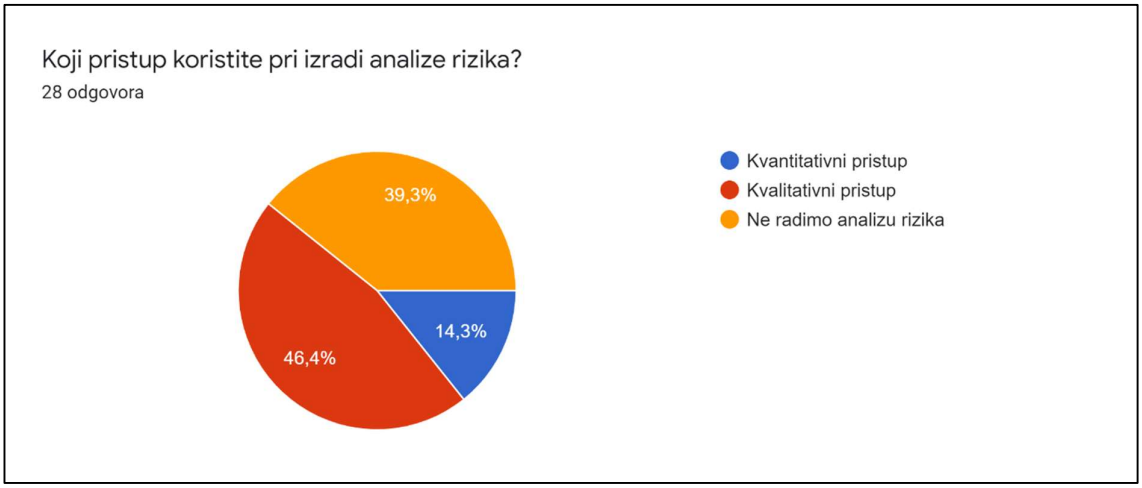
Grafikon 11 Metode pri izradi identifikacije rizika
Izvor: Izrada autora prema anketi

Poduzeća najviše koriste povijesnu metodu za izradu identifikacije rizika. Tu metodu koristi 35,7% poduzeća. Nju slijedi metoda sustavnog pristupa sa 25% te zatim metoda induktivne ili teorijske analize sa 21,4%.



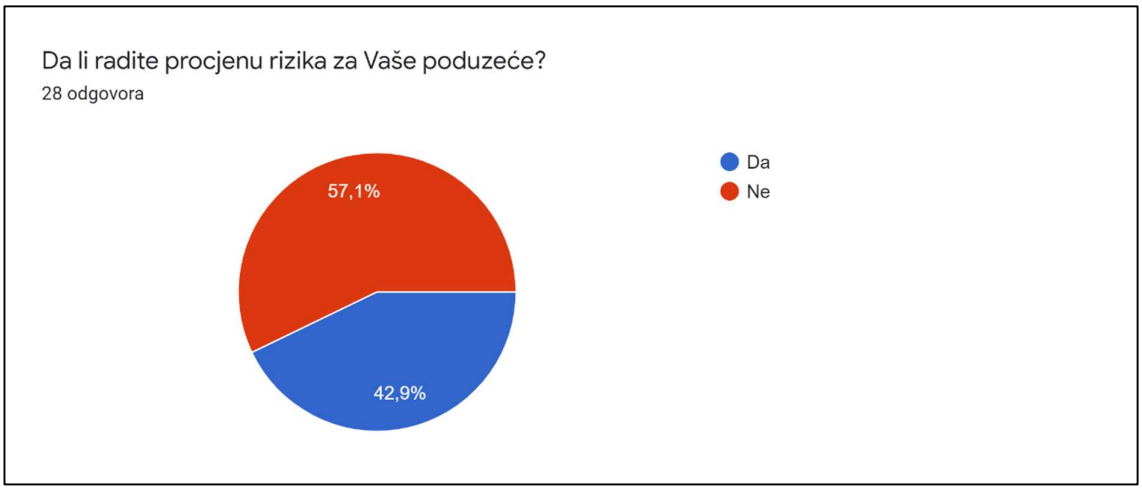
Grafikon 12 Postotak poduzeća koja rade analizu rizika
Izvor: Izrada autora prema anketi

Postotak poduzeća koja rade analizu rizika jednak je onom koji rade i identifikaciju rizika tj. on iznosi 60,7%.

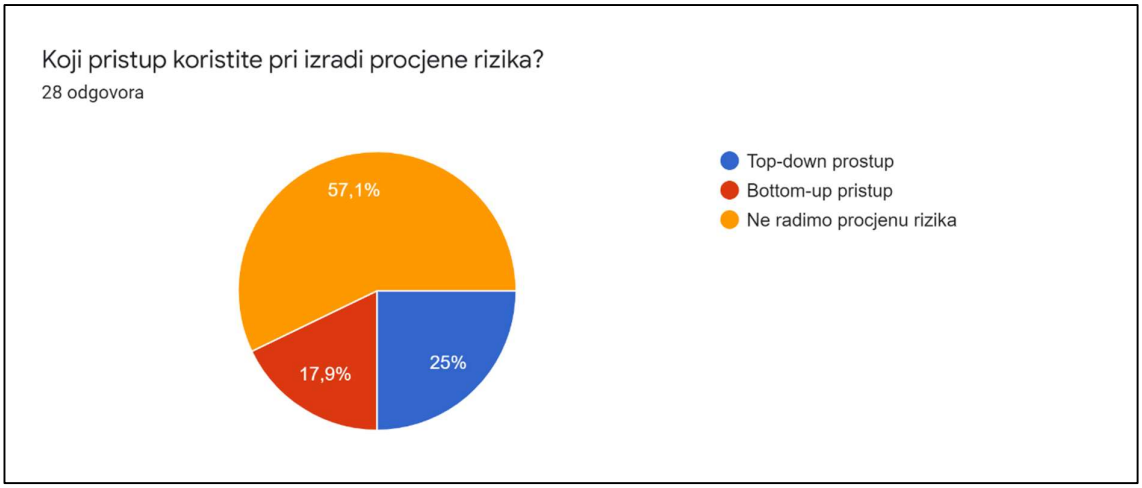


Grafikon 13 Pristup pri analizi rizika
Izvor: Izrada autora prema anketi

Poduzeća koja rade analizu rizika koriste u 46,4% slučajeva kvalitativni pristup, dok njih 14,3% koristi kvantitativni pristup.

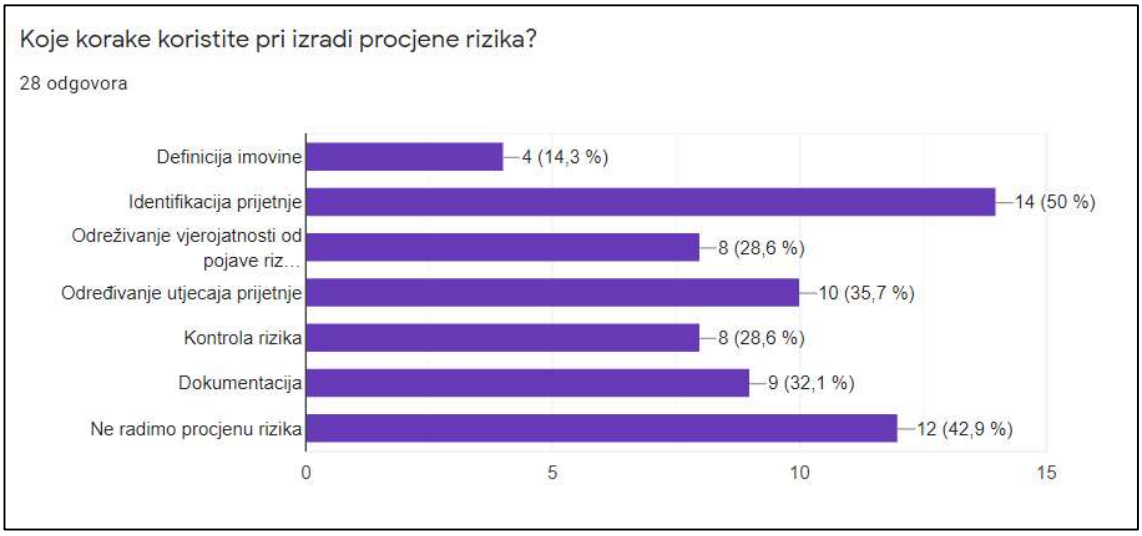


Grafikon 14 Postotak poduzeća koja rade procjenu rizika
Izvor: Izrada autora prema anketi



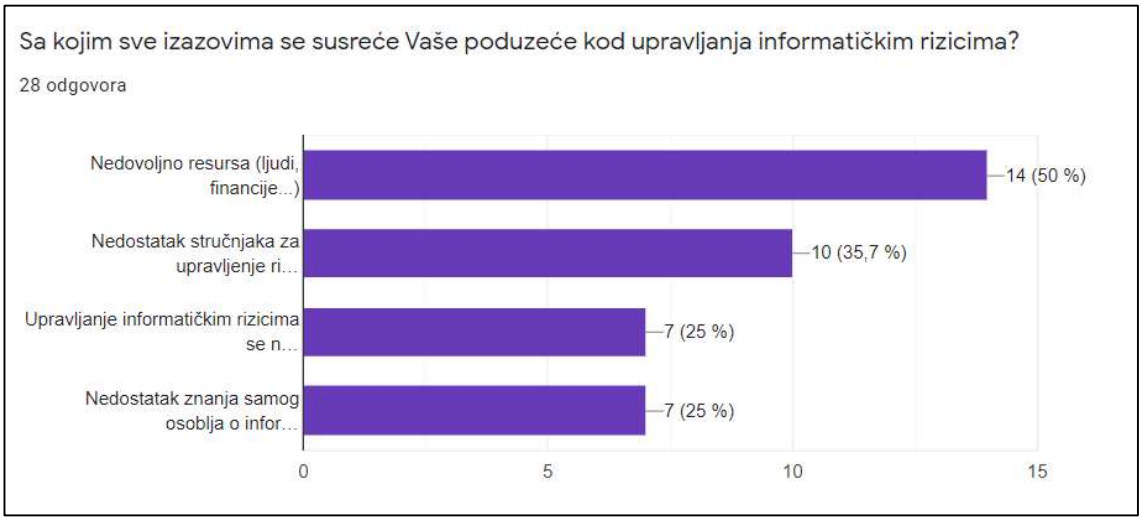
Grafikon 15 Pristup pri izradi procjene rizika
Izvor: Izrada autora prema anketi

Procjenu rizika radi 42,9% poduzeća te njih 25% pri tome koristi top-down pristup, dok njih 17,9% koristi bottom-up pristup. Zanimljivo je da veći postotak poduzeća radi analizu rizika ali potom ne nastavlja dalje u procesu životnog ciklusa informacijske sigurnosti tj., ne radi procjenu rizika.



Grafikon 16 Koraci pri izradi procjene rizika
Izvor: Izrada autora prema anketi

Grafikon 16 prikazuje da poduzeća koja rade procjenu rizika ne koriste sve korake koji se, prema teoriji, rade pri procjeni rizika. Većina ih radi identifikaciju prijetnji ali onda se ne odrađuje određivanje vjerojatnosti od pojave rizika te određivanje utjecaja prijetnji. Isto tako, samo njih 32,1% radi dokumentaciju procesa. U detaljnijoj analizi vidjet će se koliko to utječe na ranjivost poduzeća.



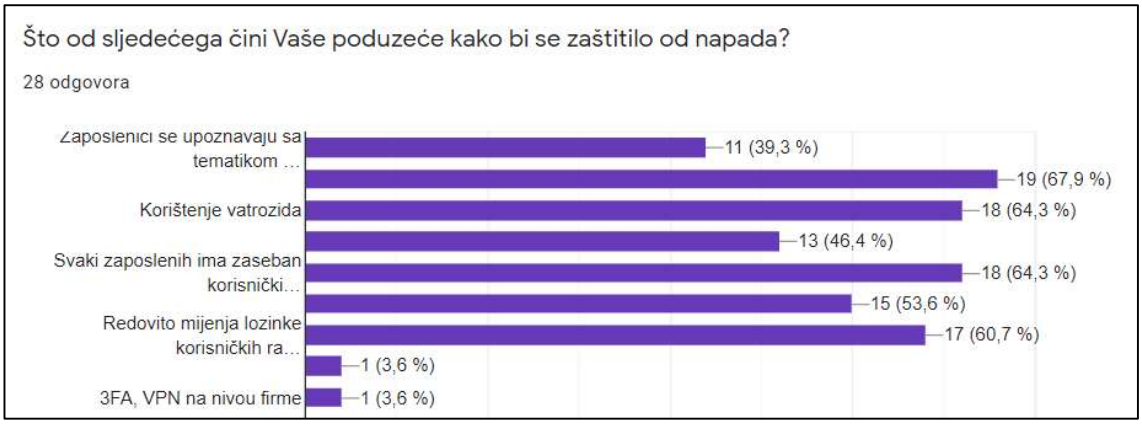
Grafikon 17 Izazovi kod upravljanja informatičkim rizicima
Izvor: Izrada autora prema anketi

Poduzeća se najčešće susreću sa sljedećim izazovima kod upravljanja informatičkim rizicima:

- Nedovoljno resursa (ljudi, financije...) – 50% poduzeća
- Nedostatak stručnjaka za upravljanje rizicima – 35,7 %
- Upravljanje informatičkim rizicima se ne shvaća ozbiljno – 25%
- Nedostatak znanja samog osoblja o informatičkim rizicima – 25%

Grafikon 18 Hakerski napad u poduzeću
Izvor: Izrada autora prema anketi

64,3% poduzeća koje je sudjelovalo u anketi, nije doživjelo hakerski napad dok je njih 14,3% doživjelo to neugodno iskustvo hakerskog napada. 21,4% ispitanika nije znalo tu informaciju.¸

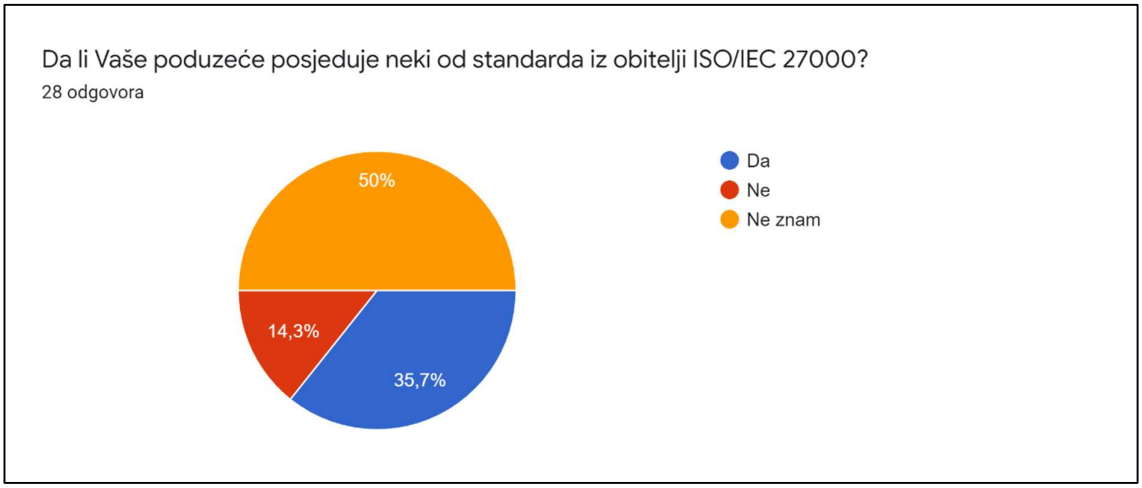


Grafikon 19 Što poduzeća čine kako bi se zaštitila od napada
Izvor: Izrada autora prema anketi

Kako bih se poduzeća zaštitila od napada ona poduzimaju sljedeće korake:

- Zaposlenici se upoznavaju sa tematikom informatičkih rizika

- Redovito ažuriranje antivirusnih sustava na svakom računalu u poduzeću
- Korištenje vatrozida
- Redovita izrada sigurnosnih kopija bitnih podataka
- Svaki zaposlenih ima zaseban korisnički račun
- Redovito mijenja lozinke korisničkih računa
- Ograničava zaposlenicima pristup određenim podacima
- 3FA, VPN na nivou firme
- Poduzeće ne poduzima ništa po tom pitanju



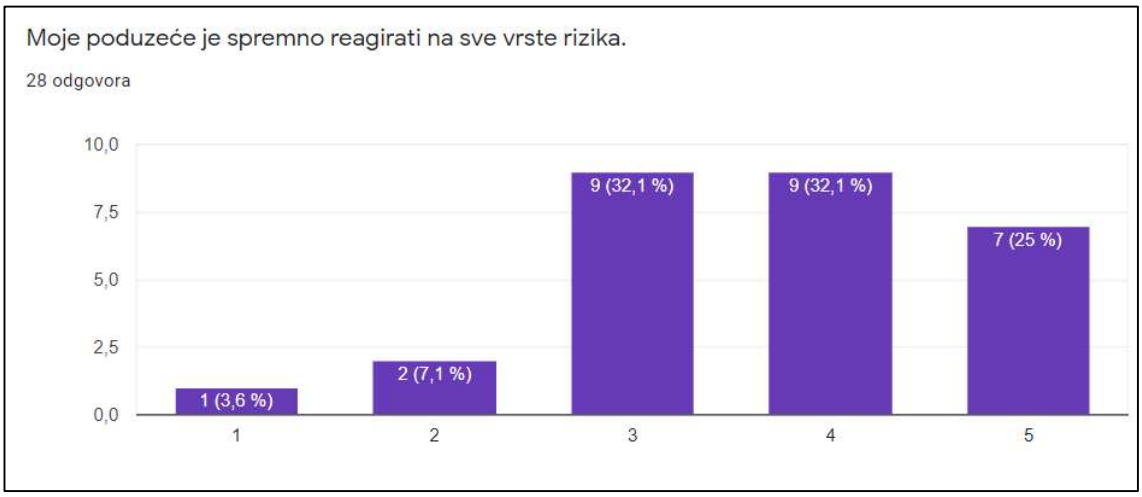
Grafikon 20 ISO/IEC 27000 standardi
Izvor: Izrada autora prema anketi

Polovica ispitanika ne posjeduje informaciju da li njihovo poduzeće ima standard iz serije ISO 27000, niza najboljih praksi koje pomažu poduzećima da poboljšaju svoju informacijsku sigurnost. 35,7% poduzeća posjeduje certifikat iz serije ISO 27000 standarda, a 14,3% poduzeća nema takav certifikat.

U drugom dijelu ankete ispitanici su ocijenili od 1 do 5 njihov stupanj slaganja sa navedenim tvrdnjama. Ocjene su označavale:

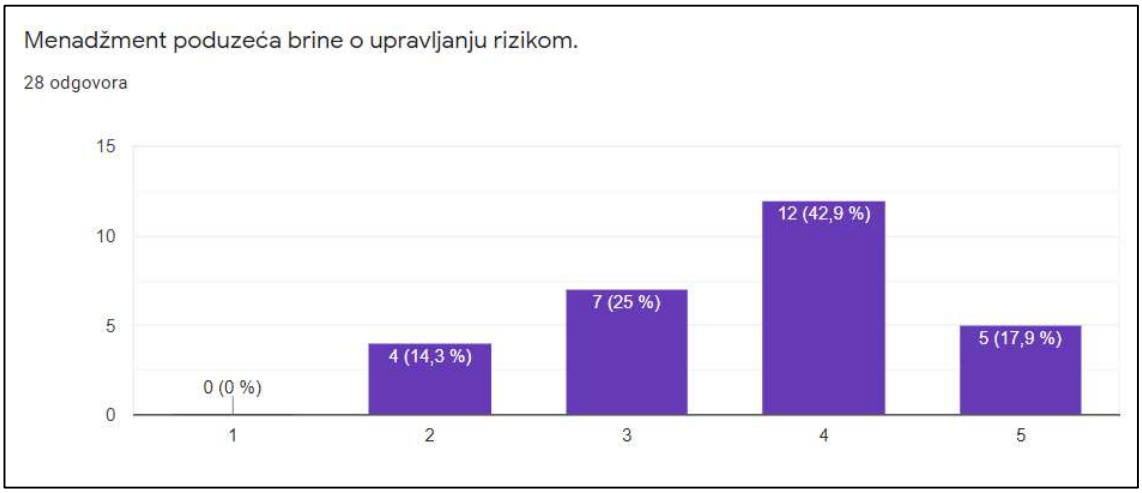
- 1 – uopće se ne slažem
- 2 – uglavnom se ne slažem
- 3 – niti se slažem, niti se ne slažem
- 4 – uglavnom se slažem

- 5 – potpuno se slažem



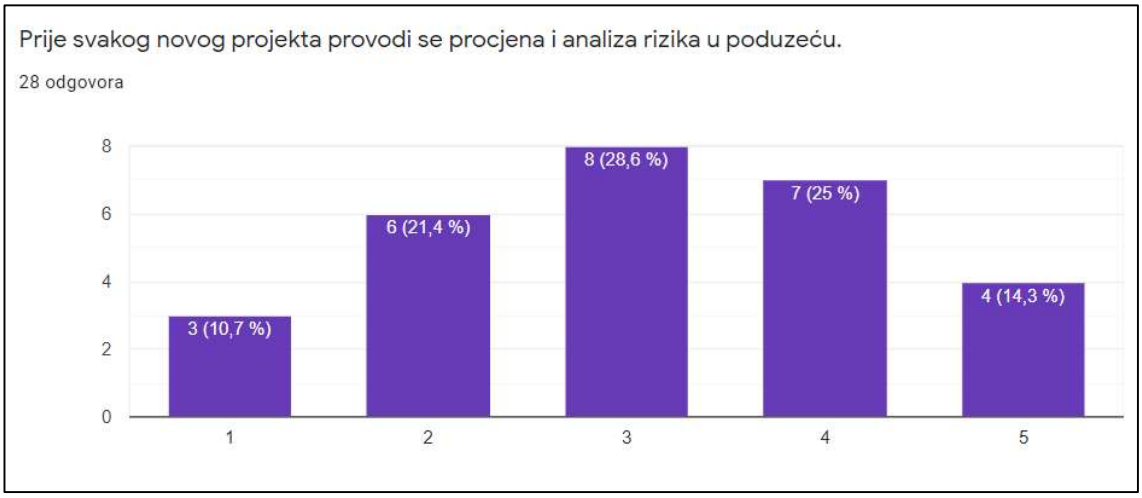
Grafikon 21 Spremnost poduzeća za reagiranje na rizike
Izvor: Izrada autora prema anketi

Preko polovice ispitanika smatra kako je njihovo poduzeće spremno reagirati na rizike koji im mogu prijetiti dok je njih 32,1% neodlučno. 10,7% ispitanika nije uvjereno u to da se njihovo poduzeće može nositi sa rizicima koji ih okružuju.



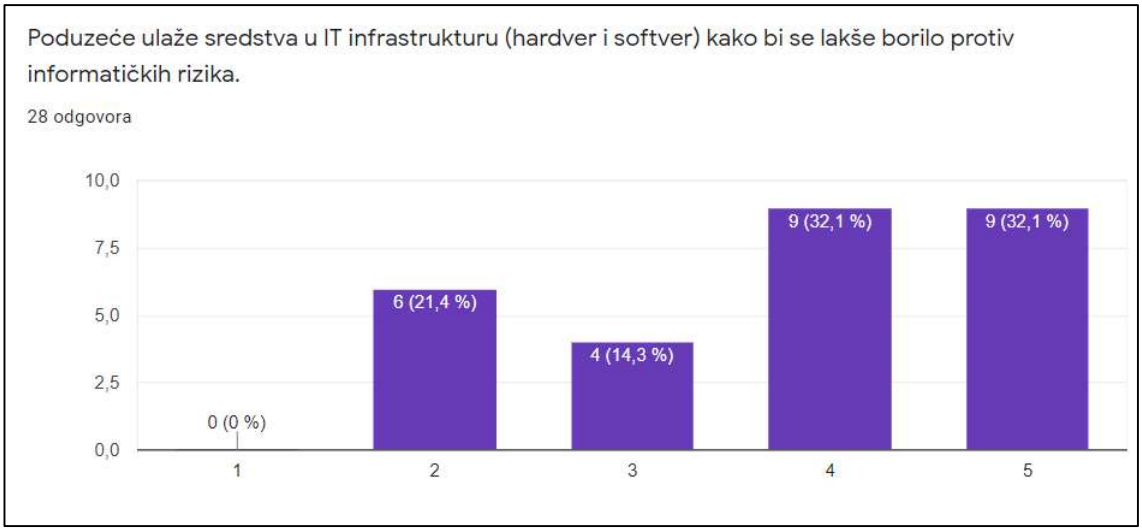
Grafikon 22 Briga menadžmenta o upravljanju rizikom
Izvor: Izrada autora prema anketi

Ispitanici su u preko 50% slučajeva zadovoljni kako njihov menadžment brine o upravljanju rizikom. Nema nitko tko smatra da njihov menadžment uopće ne brine o upravljanju rizikom ali je i 25% ispitanika neodlučno kod njihove izjave o brizi menadžmenta kod upravljanja rizikom.



Grafikon 23 Provođenje analize i procjene rizika prije novog projekta
Izvor: Izrada autora prema anketi

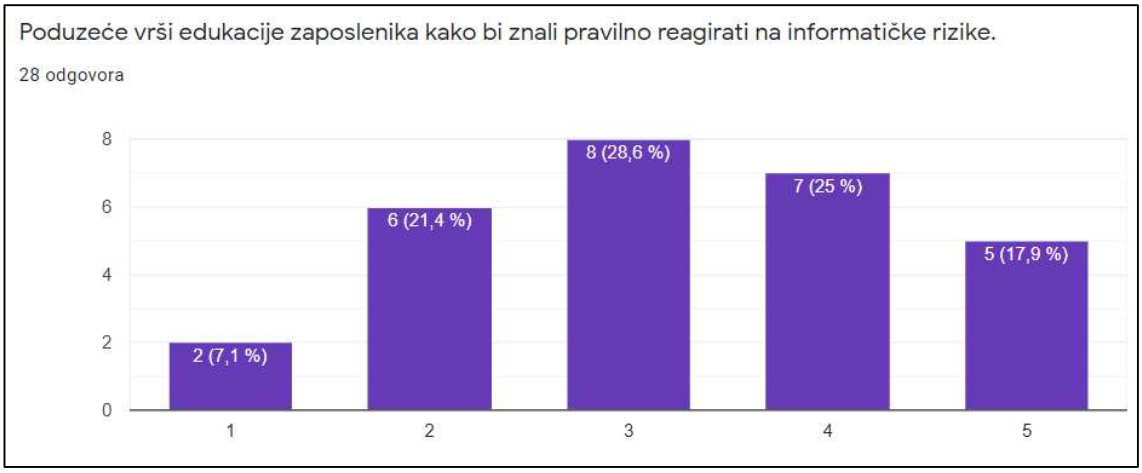
Većina ispitanika, njih 28,6%, se niti slaže niti ne slaže sa izjavom da se provodi procjena i analiza rizika prije svakog novog projekta. Ostali ispitanici su relativno ravnomjerno raspoređeni. Njih 32,1% se ne slaže sa ovom izjavom dok se njih 39,3% slaže sa time da se provodi procjena i analiza rizika prije novih projekata.



Grafikon 24 Ulaganje u IT infrastrukturu
Izvor: Izrada autora prema anketi

Kada se radi o ulaganju u IT infrastrukturu može se zaključiti da su ispitanici zadovoljni kako se prema tome odnosi njihovo poduzeće. To je bitno kod sprječavanja rizika od napada trećih

strana (npr. hakera). 21,4% ispitanika se uglavnom ne slaže sa time da njihovo poduzeće brine o IT infrastrukturi dok se njih 14,3% niti slaže niti ne slaže sa tom izjavom.



Grafikon 25 Edukacije zaposlenika o informatičkim rizicima
Izvor: Izrada autora prema anketi

Pri izjavi da poduzeće vrši edukacije svojih zaposlenika kako bi znali pravilno reagirati na informatičke rizike ispitanici su u 28,6% bili neodlučni dok njih 42,9% smatra da poduzeće to dobro odrađuje. Taj postotak je dosta visok ali kod ovako ozbiljne teme poduzeća bi svakako trebala poraditi na tome da se taj postotak poveća.

4.2. Analiza rezultata ankete

Kod analize rezultata koristit će se Spearmenov koeficijent korelacije. Koeficijent korelacije pokazuje u kojoj mjeri se dvije varijable zajedno mijenjaju. Koeficijent opisuje i snagu i smjer odnosa. On može biti pozitivan i negativan tj. može ići od -1 do +1 te pokazuje u kojoj su mjeri promjene vrijednosti jedne varijable povezane s promjenama vrijednosti druge varijable.

Udovčić et al. (2007) kaže da se Spearmanov koeficijent relacije izračunava kada jedan od skupa podataka slijedi ordinalnu ljestvicu ili kada raspodjela podataka značajno odstupa od normalne raspodjele te postoje podatci koji značajno odstupaju od većine izmjerenih te se Spearmenov koeficijent može računati i na manjim uzorcima (N<35). Spearmenov koeficjent relacije označava se sa r_s.

Prema intenzitetu korelacija može biti:

- $|r_s| \geq 0{,}8$ tj. jaka korelacija
- $0{,}5 < |r_s| < 0{,}8$ tj. srednje jaka korelacija

- $|r_s| \leq 0{,}5$ tj. slaba korelacija

U analizi odgovora korištena je korelacija podataka te klasterizacija podataka. Kako bih se rezultati mogli statističku obraditi njima su dodijeljeni rangovi (brojevi). Popis pitanja te način na koji su odgovori rangirani prikazani su u Prologu 1.

Pomoću klaster analize je određen skup objekata, u ovom slučaju su to odgovori ankete tj. ispitanici, grupiran u dvije grupe. Cilj je bio dobiti dvije grupe koje će formirati nisku i visoku razinu upravljanja rizikom. Svaka od tih grupa ima svoja obilježja kako se nosi tj. da li se nosi sa rizikom koji ih okružuje.

Radi što boljeg rezultata klasterizacije, odgovori iz ankete su izvezeni u Excel datoteku te kao što je već prethodno navedeno oni su numerički rangirani (vidi Prilog 1). Nakon što su rangovi bili određeni, podaci su obrađeni putem programa RapidMiner te IBM SPSS. Kao primarni ključ bio je zadan broj poduzeća tj. redni broj odgovora ankete. Oba programa su pronašla i svrstala odgovore (u ovom slučaju poduzeća) u dvije grupe gdje se moglo utvrditi prema danim odgovorima da jedna grupa poduzeća brine o rizicima dok druga grupa ne brine o rizicima. Dvije grupe koje su dobivene putem klaster analize biti će detaljnije opisane u nastavku poglavlja.

U drugom dijelu ankete ispitanici su ocijenili od 1 do 5 njihov stupanj slaganja sa navedenim tvrdnjama te su odgovori tako i rangirani pri analizi.

Tablica 3 Korelacija podataka 1

Korelacije

			Veličina poduzeća prema broju zaposlenih:	Da li radite identifikaciju rizika za Vaše poduzeće?	Da li radite analizu rizika za Vaše poduzeće?	Da li radite procjenu rizika za Vaše poduzeće?
Spearman	Veličina poduzeća prema broju zaposlenih:	Correlation Coefficient	1.000	-.286	-.356	-.231
		Sig. (2-tailed)	.	.140	.063	.236
		N	28	28	28	28
	Da li radite identifikaciju rizika za Vaše poduzeće?	Correlation Coefficient	**-.286**	1.000	.701**	.697**
		Sig. (2-tailed)	.140	.	.000	.000
		N	28	28	28	28
	Da li radite analizu rizika za Vaše poduzeće?	Correlation Coefficient	**-.356**	**.701****	1.000	.697**
		Sig. (2-tailed)	.063	.000	.	.000
		N	28	28	28	28
	Da li radite procjenu rizika za Vaše poduzeće?	Correlation Coefficient	**-.231**	**.697****	**.697****	1.000
		Sig. (2-tailed)	.236	.000	.000	.
		N	28	28	28	28

**. Correlation is significant at the 0.01 level (2-tailed).

Izvor: Izrada autora

Tablica 3 pokazuje da veličina poduzeća ima slabu negativnu korelaciju sa ostalim varijablama što pokazuje da veličina poduzeća ne utječe na to da li se radi identifikacija, analiza ili procjena rizika. Ali zato je uočljiva srednje jaka pozitivna korelaciju između identifikacije, analize te procjene rizika. Najveća korelacija je između analize rizika te identifikacije rizika, što znači da ako poduzeće radi identifikaciju rizika, odradit će i analizu ali isto tako je vrlo vjerojatno da ako poduzeće radi analizu da će odraditi i procjenu rizika.

Tablica 4 Korelacija podataka 2

Korelacije

			Menadžment poduzeća brine o upravljanju rizikom.	Prije svakog novog projekta provodi se procjena i analiza rizika u poduzeću.	Poduzeće ulaže sredstva u IT infrastrukturu (hardver i softver) kako bi se lakše borilo protiv informatičkih rizika.	Poduzeće vrši edukacije zaposlenika kako bi znali pravilno reagirati na informatičke rizike.
Spearmen	Menadžment poduzeća brine o upravljanju rizikom.	Correlation Coefficient	1.000	.571**	.557**	.726**
		Sig. (2-tailed)	.	.001	.002	.000
		N	28	28	28	28
	Prije svakog novog projekta provodi se procjena i analiza rizika u poduzeću.	Correlation Coefficient	**.571****	1.000	.847**	.694**
		Sig. (2-tailed)	.001	.	.000	.000
		N	28	28	28	28
	Poduzeće ulaže sredstva u IT infrastrukturu (hardver i softver) kako bi se lakše borilo protiv informatičkih rizika.	Correlation Coefficient	**.557****	.847**	1.000	.629**
		Sig. (2-tailed)	.002	.000	.	.000
		N	28	28	28	28
	Poduzeće vrši edukacije zaposlenika kako bi znali pravilno reagirati na informatičke rizike.	Correlation Coefficient	**.726****	.694**	.629**	1.000
		Sig. (2-tailed)	.000	.000	.000	.
		N	28	28	28	28

**. Correlation is significant at the 0.01 level (2-tailed).

Izvor: Izrada autora

Odnos menadžmenta prema upravljanju rizikom vrlo je bitan, što je vidljivo iz tablice 4. Ako menadžment poduzeća brine o upravljanju rizikom tada se provode procjena i analiza rizika prije novih projekata, poduzeća više ulažu u IT infrastrukturu te poduzeća vrše edukacije zaposlenika kako bi isti znali pravilno reagirati na informatičke rizike. Kako bih se pobliže naglasila važnost menadžmenta prikazana je i klasterizacija podataka na slici 4.

Attribute ↓	cluster_0	cluster_1
Menadžment poduzeća brine o upravljanju rizikom.	2.636	4.294
Da li radite procjenu rizika za Vaše poduzeće?	2	1.294
Da li radite identifikaciju rizika za Vaše poduzeće?	1.818	1.118
Da li radite analizu rizika za Vaše poduzeće?	1.909	1.059

Slika 4 Klasterizacija podataka: Odnos menadžmenta prema upravljanju rizikom
Izvor: Izrada autora

Na slici 4 su prikazana dva klastera. U anketi su ispitanici glasali ocjenama od 1 do 5 ovisno o tome koliko smatraju da menadžment brine o upravljanju rizikom. Prvi klaster ima prosječnu ocjenu 2,6 što govori da u tim poduzećima menadžment ne brine o upravljanju rizikom a sukladno tome se ne rade identifikacija, analiza i procjena rizika (odgovori su rangirani prema

1- DA te 2 - NE). Sa druge strane je drugi klaster gdje menadžment brine o upravljanju rizikom (prosječna ocjena 4,3) te se u tim poduzećima radi identifikacija, analiza te procjena rizika.

Tablica 5 Razine upravljanja rizikom

Razine upravljanja rizikom		
	Klasteri	
	Niska razina	Visoka razina
Veličina poduzeća prema broju zaposlenih:	1	4
Starost poduzeća u godinama:	2	4
Da li radite identifikaciju rizika za Vaše poduzeće?	2	1
Da li radite analizu rizika za Vaše poduzeće?	2	1
Da li radite procjenu rizika za Vaše poduzeće?	2	1
Da li Vaše poduzeće posjeduje neki od standarda iz obitelji ISO/IEC 27000?	2	1
Da li je Vaše poduzeće doživjelo hakerski napad?	2	2
Moje poduzeće je spremno reagirati na sve vrste rizika.	2	4
Sa kojim sve izazovima se susreće Vaše poduzeće kod upravljanja informatičkim rizicima?	9	2

Izvor: Izrada autora

U tablici 5 kreirana su dva klastera koja grupiraju poduzeća prema razini upravljanja rizikom. Rezultati ankete su rangirani kako bih se mogla izvršiti statistička analiza, a rangovi odgovora se nalaze u Prilogu 1.

U nižoj razini se pretežito nalaze mikro poduzeća koja imaju manje od 10 zaposlenih dok su u višoj razini srednja (50-249 zaposlenih) i velika poduzeća (250> zaposlenih). Starost poduzeća se u nižoj razini nalazi između 11-30 godina, dok su poduzeća u višoj razini starija od 50

godina. Poduzeća koja se nalaze u nižoj razini ne rade identifikaciju, analizu te procjenu rizika dok poduzeća u višoj razini provode sve ove procese.

Standarde iz obitelji ISO 27000 posjeduju poduzeća više razine dok poduzeća niže razine nemaju ove standarde te se sukladno tome i sami ispitanici slažu da poduzeća niže razine nisu spremna reagirati na sve vrste rizika dok su zaposlenici poduzeća koja spadaju u višu razinu sigurni u to da se njihovo poduzeće može nositi sa rizicima. Ispitanici iz poduzeća u nižoj razini kao najveći izazov smatraju da njihovo poduzeće upravljanje informatičkim rizicima ne shvaća ozbiljno, a ispitanici poduzeća iz više razine smatraju da im u poduzeću nedostaje stručnjaka za upravljanje rizicima te da sami zaposlenici nemaju dovoljno znanja o informatičkim rizicima.

5. NAČINI ZA UPRAVLJANJE INFORMATIČKIM RIZICIMA

Analizirajući dobivene rezultate ankete te proučavanjem dva dobivena klastera tj. dvije dobivene razine upravljanja rizikom u nastavku će biti prikazano kako ta poduzeća upravljaju rizikom.

Dobiveni rezultati mogu služit kao smjernice ostalim poduzećima koja se žele zaštitit od rizika koji im prijete.

Tablica 6 Načini upravljanja rizikom

Načini upravljanja rizikom		
	Klasteri	
	Niska razina	Visoka razina
Koliko često radite identifikaciju rizika?	2	5
Koje metode koristite pri identifikaciji rizika?	3	7
Koji pristup koristite pri izradi analize rizika?	3	2
Koji pristup koristite pri izradi procjene rizika?	3	1
Koje korake koristite pri izradi procjene rizika?	10	2
Poduzeće ulaže sredstva u IT infrastrukturu (hardver i softver) kako bi se lakše borilo protiv informatičkih rizika.	2	5
Poduzeće vrši edukacije zaposlenika kako bi znali pravilno reagirati na informatičke rizike.	2	3

Izvor: Izrada autora

U tablici 6 je analizirano na koje načine poduzeća po razinama (niska i visoka razina) upravljaju sa rizikom.

Poduzeća koja su rangirana u nižu razinu upravljanja rizikom:

- Ne rade identifikaciju rizika
- Sukladno tome ne koriste metode za identifikaciju rizika
- Ne rade analizu rizika te ne koriste niti jedan od pristupa analizi rizika
- Isto tako ne rade procjenu rizika te tako ne koriste pristupe niti korake za procjenu rizika
- Prema mišljenu ispitanika, poduzeća iz niže razine ne ulažu sredstva u IT infrastrukturu kako bi se lakše borila sa informatičkim rizicima
- Te poduzeća iz niže razine upravljanja rizikom ne vrše edukacije svojih zaposlenika kako bi oni znali pravilno reagirati i prepoznati rizike

Poduzeća koja su rangirana u višu razinu upravljanja rizikom:

- Rade identifikaciju rizika više puta godišnje
- Pri tome najčešće koriste povijesnu metodu te metodu sustavnog pristupa
- Pri analizi rizika koriste kvantitativan pristup
- Pri procjeni rizika koriste bottom-up pristup
- Korake koje koriste pri izradi procjene rizika su:
    - Definicija imovine
    - Identifikacija prijetnje
    - Određivanje vjerojatnosti od pojave rizika
    - Određivanje utjecaja prijetnje
    - Kontrola rizika
    - Dokumentacija
- Poduzeća svrstana u višu razinu upravljanja rizikom, prema mišljenju ispitanika, ulažu u IT infrastrukturu
- Ispitanici smatraju da bi i ova poduzeća trebala više ulagati u edukacije zaposlenika kako bi se oni znali bolje nositi te reagirati na rizike

DISKUSIJA REZULTATA

Simon i Moucha (2019) u svojem radu, kao izazov kod upravljanja sa sigurnošću informacija, navode činjenicu da se danas još uvijek na informacijsku sigurnost gledao kao na jednokratnu akciju. Oni kažu da često potrebne sigurnosne akcije započinju kasno, a zatim naglo završavaju te se često poznate pogreške ponavljaju zbog nedostatka ili nedovoljnog određivanja sigurnosnih zahtjeva na početku projekta.

Proučavajući analizirane podatke ankete, može se primijetiti da se rezultati podudaraju sa poduzećima koja su u ovom radu svrstana u nižu razinu upravljanja rizikom. Ta poduzeća ne rade identifikaciju, analizu te procjenu rizika što znači da prije projekata ne rade sigurnosne zahtjeve. Ovakvo ophođenje prema riziku dovodi, ne samo projekt već i cijelo poduzeće u situaciju gdje može doći do velikih financijskih gubitaka pa čak i do bankrota. Sa druge strane, poduzeća koja su svrstana u višu razinu upravljanja rizikom su ovdje u nešto povoljnijem položaju tj. oni radi sigurnosne zahtjeve nekoliko puta godišnje.

Vincent, Higgs i Pinsker (2018) istraživali su utječe li umiješanost odbora poduzeća, stručnost odbora i kultura visokog menadžmenta na zrelost kod prakse za upravljanje rizikom. Njihovi rezultati pokazuju da sudjelovanje odbora i stručnost pozitivno utječu na zrelost, ali uključivanje odbora važnije je za zrelost od razine IT stručnosti tog istog odbora.

Rezultati ankete ovog rada također pokazuju kako je uključenost menadžmenta bitna za upravljanje rizikom tj. ako menadžment brine o upravljanju rizikom onda je mnogo veća vjerojatnost da će se provoditi identifikacija, analiza i procjena rizika. Isto tako će se vršiti i edukacije samih zaposlenika kako bi bili upoznati sa rizikom.

Ovaj rad nije istražio da li je za poduzeće bitna sama uključenost menadžmenta kod upravljanja rizikom ili i njihova stručnost kako su to u svom radu analizirali Vincent, Higgs i Pinsker (2018) te zaključili da je stručnost odbora manje važna od same uključenosti. Rezultati ovog rada pokazuju kako poduzeća koja su svrstana u višu razinu upravljanja rizikom kao jedan od izazova navode to da u poduzeću nedostaje stručnjak za upravljanje rizikom što nas može navesti na zaključak da menadžment nije dovoljno stručan ali ta činjenica bi se trebala dodatno i dublje istražiti prije donošenja konačnog zaključka.

ZAKLJUČAK

U današnje doba, koje neki nazivaju i digitalno doba, gdje skoro svatko poduzeće posluje preko interneta te barata velikom količinom informacija vrlo je bitno da ima znanja nosit se sa informatičkim rizicima. Kada poduzeće može osigurati informatičku sigurnost to znači da je je osiguralo i sigurnost podataka i informacija.

Vrlo je bitno da su poduzeća ali i korisnici usluga (ili kupci proizvoda) tog poduzeća svjesni rizika koji ih okružuju. Svako poduzeće je različito te bi moralo raditi zasebno identifikaciju, analizu i procjenu rizika. Nije dovoljno kopirati ostala poduzeća za koja se smatra da su "jednaka" jer to može dovesti do velike ranjivosti i napada trećih strana na samo poduzeće.

Iz ankete koja je provedena nad 28 različitih poduzeća proizašle su dvije skupine tj. razine poduzeća. Niža razina gdje spadaju poduzeća koja ne mare o rizicima koji ih okružuju te viša razina gdje spadaju poduzeća koja mare o rizicima koja iz okružuju. Tako u nižu razinu spadaju mikro poduzeća koja su mlada, a u visokoj razini imamo velika poduzeća koja su starija od 50 godina. Anketa je distribuirana i slana na više poduzeća. Pokušalo se razmotriti tj. dobiti povratno odgovore od što više "različitih" poduzeća. Pod različito smatraju se obilježja poduzeća (veličina, grana industrije, starost poduzeća itd.). Odaziv poduzeća nije bio velik, ali dobila se željena raznolikost te se iz tog razloga rezultati relevantni za rad.

Rezultati su pokazali da je vrlo bitno kada je menadžment poduzeća svjestan problematike informatičkih rizika te se sukladno tome može ustanoviti da velika poduzeća spadaju u višu razinu načina upravljanja sa rizicima. Ta poduzeća imaju razvijen menadžment koji ulaže sredstva u IT infrastrukturu, u edukacije zaposlenika i u tim poduzećima se provodi identifikacija, analiza te procjena rizika. Isto tako velika poduzeća imaju certifikate ISO 27000 norme. Sa druge strane imamo mikro poduzeća gdje je pretežito samo jedan vlasnik koji ne mari toliko o informatičkim rizicima što njegovo poduzeće čini mnogo ranjivijim ali isto tako i odvlači kupce koje se boje krađe njihovih podataka. Najveći izazov u sistematizaciji rizika u mikro poduzećima je činjenica da se rizici ne shvaćaju ozbiljno tj. menadžment (vlasnik) ne mari o toj problematici.

Shvaćanje opasnosti od rizika te pravilno ophođenje i zaštita od rizika može zaštiti poduzeća od gubitaka kupca, novaca, zaposlenika pa čak i bankrota i stečaja. Bitno je i za velika poduzeća koja više ulažu u projekte ali i za mala poduzeća koja se tek žele probiti na tržištu.

Ostvariti potpuno “stanje IT sigurnosti“ je vrlo teško, pa možda čak i nemoguće. Pogotovo u vrijeme kada tehnologija napreduje iz dana te se sukladno tome mijenjaju eksterni i interni uzroci koji mogu doprinijeti ranjivosti sustava. Poduzeća koja se nalaze u višoj razini su na dobrom putu da ostvare “stanje IT sigurnosti“ ali borba protiv rizika je iterativan proces te poduzeća moraju dalje nastaviti radit na svim procesima.

Uzimajući u obzir ciljeve rada, uspjelo se identificirati informatičke rizike te iz rezultata ankete, putem klasterizacije, klasificirate rizike i poduzeća u dvije grupe. Tako se, iz grupe koja je svrstana kao viša razina upravljanja rizikom, mogu izvući dobre prakse i donijeti određene načine za upravljanje informatičkim rizicima te se oni mogu primijeniti na poduzeća koja su svrstana u nižu razinu. U empirijskom djelu rada su također utvrđeni izazovi sa kojima se poduzeća susreću pri upravljanju informatičkim rizikom.

Budući smjer istraživanja trebala bi biti dublja analiza dva dobivena načina upravljanja rizikom. Treba istražiti koji su razlozi da mikro poduzeća ne rade identifikaciju, analizu i procjenu rizika. Kada bi se otkrili konkretni razlozi, onda bih se moglo radit na tome da se mikro poduzeća motiviraju te da im se pokaže kako se mogu nositi sa rizicima. U većim poduzećima treba istražiti kako se točno odvija proces identifikacije, analize i procjene rizika te vidjeti da li se taj proces može optimizirati i koliko se velike razlike u borbi protiv rizika između poduzeća sličnih obilježja (broj zaposlenih, starost poduzeća, grana industrije, organizacija poduzeća…).

Ograničenje ovog rada bio je slab odaziv poduzeća pri ispunjavanju ankete što je rezultiralo manjim brojem odgovora. To može implicirati na činjenicu da određena poduzeća ne mare na istraživanja ove vrste jer također ne provode mjere zaštite od rizika u poduzeću no pravi razlog slabijeg odaziva teško je utvrditi bez dodatnog istraživanja.

Također, kao budući smjer istraživanja, trebali bi se istražiti konkretni rizici koji su identificirani od strane poduzeća te odraditi procjenu složenosti tih istih rizika te snagu njihovog utjecaja na poslovanje poduzeća. Tako bi se mogli odrediti veće prijetnje na koje poduzeća moraju reagirati.

Teorijski dio će poduzeća koristiti kao uvod u problematiku informatičkih rizika, uvidjet će važnost provođenja identifikacije, analize i procjene rizika te će vidjeti načine i metoda putem kojih se to može raditi. Empirijski dio rada daje sliku o trenutnom stanju tj. trenutnom načinu na koji se poduzeća odnose prema rizicima te mišljenja zaposlenika poduzeća koji iz prve ruke

govore o problematici informatičkih rizika iz perspektive samog poduzeća. To će poslužiti menadžmentu poduzeća kao smjernica na koji način poboljšati odnos prema problematici sa informatičkim rizicima. Ovaj rad također daje smjernice u kojima bi trebala ići daljnja detaljnija istraživanja. Ta istraživanja se mogu nadovezat na rad te bi tako mogla dati još konkretniji uvid u izazove upravljanja informatičkim rizicima te ponuditi rješenja kako se sa njima nositi.

SAŽETAK

U današnjem umreženom svijetu informacijska sigurnost (IS) i upravljanje rizikom (eng. Risk Management (RM)) informacijskog sustava potrebni su za svako poduzeće koje želi opstati u poslovanju i biti konkurentno. Digitalno doba u kojem se nalazimo čini poduzeća ranjivima ako ignoriraju informatičke rizike. Poduzeća se bore sa time kako sistematizirati upravljanje rizikom te na koji način to učiniti kada su u pitanju informatički rizici. Predmet istraživanja ovog rada je istražiti što bi to bilo "stanje IT sigurnosti" te koji se sve izazovi javljaju kod upravljanja informatičkim rizicima. Ovaj rad omogućuje poduzećima da na jednom mjestu imaju detaljan i transparentan pregled na to što im pomaže u razvijanju akcijskih mjera prema prijetećim rizicima te mogu procijeniti u koji način upravljanja rizikom spadaju. Isto tako rad pruža uvid u procese identifikacije, analize i procjene te glavne izazove se kojima se nose današnja poduzeća u borbi protiv informatičkih rizika.

KLJUČNE RIJEČI: RIZIK, SIGURNOST, UPRAVLJANJE

SUMMARY

In today's networked world, information security (IS) and risk management (RM) of the information system are necessary for every company that wants to survive in business and be competitive. The digital age we are in makes companies vulnerable if they ignore IT risks. Companies are struggling with how to systematize risk management and how to do it when it comes to IT risks. The subject of this paper is to investigate what would be the "state of IT security" and what are the challenges in information risk management. This paper allows companies to have a detailed and transparent overview in one place, which helps them to develop action measures against threatening risks, and they can assess how well they manage risk in compare to other business. The paper also provides insight into the processes of identification, analysis and assessment and the main challenges that today's companies are facing in the fight against information risks.

KEY WORDS: RISK, SAFETY, MANAGEMENT

LITERATURA

Časopis:

1. Blake, R. and Ayyagari, R. (2012). Analyzing Information Systems Security Research to Find Key Topics, Trends, and Opportunities. Journal of Information Privacy and Security, 8(3), pp.37-67.
2. Dietrich, M., Reckert, H. and Salomon, K., 2003. Risikoanalyse und Risikobewertung. Xpert.press, pp.101-130.
3. Fenz, S., Parkin, S. and Moorsel, A. (2011). A Community Knowledge Base for IT Security. IT Professional, 13(3), pp.24-30.
4. Hechenblaikner, A., 2006. Operational Risk in Banken. pp.8-30.
5. Kesh, S. and Ratnasingam, P. (2007). A knowledge architecture for IT security. Communications of the ACM, 50(7), pp.103-108.
6. Mayer, N., Aubert, J., Grandry, E., Feltus, C., Goettelmann, E. and Wieringa, R. (2018). An integrated conceptual model for information system security risk management supported by enterprise architecture management. Software & Systems Modeling, 18(3), pp.2285-2312.
7. Mayer, N., Dubois, E., Matulevicius, R., & Heymans, P. (2008). Towards a Measurement Framework for Security Risk Management. MODSEC@MoDELS.
8. Podziņš, O. and Romānovs, A., (2017.) IT RISK IDENTIFICATION AND ASSESSMENT METHODOLOGY. Environment. Technology. Resources. Proceedings of the International Scientific and Practical Conference, 2, p.124.
9. Rainer, R., Snyder, C. and Carr, H., 2015. Risk Analysis for Information Technology. Journal of Management Information Systems, 8(1), pp.129-147.
10. Simon, K., Moucha, C., 2019. Sicherheit und Datenschutz im Lebenszyklus von Informationssystemen. Datenschutz und Datensicherheit - DuD, 43(2), pp.97-101.
11. Tchankova, L., 2002. Risk identification – basic stage in risk management. Environmental Management and Health, 13(3), pp.290-297.
12. Vincent, N., Higgs, J. and Pinsker, R., 2018. Board and Management-Level Factors Affecting the Maturity of IT Risk Management Practices. Journal of Information Systems, 33(3), pp.117-135.
13. Werners, B. and Klempt, P., 2005. Risikoanalyse und Auswahl von Maßnahmen zur Gewährleistung der IT-Sicherheit. Operations Research Proceedings, pp.545-550.

Izvor s interneta:

1. Bilton, R., 2009. BBC NEWS | UK | Blackmail Fear Over Lost RAF Data. [Internet] News.bbc.co.uk. Raspoloživo na: http://news.bbc.co.uk/2/hi/uk_news/8066586.stm [06.06 2020].
2. Bugajenko, O. and Kwong, W., n.d. Risk Identification: Definition, Purpose & Examples. [Internet] Study.com. Raspoloživo na: https://study.com/academy/lesson/risk-identification-definition-purpose-examples.html [07.06 2020].
3. Charette, R., 2008. The Software Issues Behind Heathrow's T5 Meltdown. [Internet] IEEE Spectrum: Technology, Engineering, and Science News. Raspoloživo na: https://spectrum.ieee.org/riskfactor/computing/it/the_software_issues_behind_hea [06.06 2020].
4. Copeland, J., 2020. Risk Analysis Vs. Risk Assessment: What's The Difference?. [Internet] Fairinstitute.org. Raspoloživo na: https://www.fairinstitute.org/blog/risk-analysis-vs.-risk-assessment-whats-the-difference [25.04.2020].
5. Enciklopedija.hr. 2020. Informacijski Sustav | Hrvatska Enciklopedija. [Internet] Raspoloživo na: <https://www.enciklopedija.hr/Natuknica.aspx?ID=27410> [21.06.2020].
6. Fildes, J., 2009. Phishing Attack Targets Hotmail. [Internet] News.bbc.co.uk. Raspoloživo na: http://news.bbc.co.uk/2/hi/8291268.stm [06.06 2020].
7. Gabriel, R. (2020). Definition: IT-Sicherheit. [Internet] Gabler Banklexikon. Raspoloživo na: https://www.gabler-banklexikon.de/definition/it-sicherheit-70719 [29.02.2020].
8. GDPR Informer. 2020. Vodič Kroz GDPR Za Početnike - GDPR Informer. [Internet] Raspoloživo na: https://gdprinformer.com/hr/vodic-kroz-gdpr [21.03.2020].
9. Institute, F., 2020. The Importance And Effectiveness Of Cyber Risk Quantification. [Interneet] Fairinstitute.org. Raspoloživo na: <ttps://www.fairinstitute.org/what-is-fair [25.04.2020].
10. Internetworldstats.com. (2019). World Internet Users Statistics and 2019 World Population Stats. [Internet] raspoloživo na: https://www.internetworldstats.com/stats.htm [07.09.2019].
11. Irwin, L., 2019. What Is The ISO 27000 Series Of Standards? - IT Governance UK Blog. [Internet] IT Governance UK Blog. Raspoloživo na:

https://www.itgovernance.co.uk/blog/what-is-the-iso-27000-series-of-standards [13.06 2020].

12. SearchCompliance. 2020. What Is A Risk Assessment? - Definition From Whatis.Com. [Internet] Raspoloživo na: https://searchcompliance.techtarget.com/definition/risk-assessment [25.04.2020].
13. Security-insider.de. 2017. Was Ist Ein Hacker?. [Internet] Raspoloživo na: https://www.security-insider.de/was-ist-ein-hacker-a-596399 [21.03.2020].
14. Spacey, J. (2020). What is Information Security Risk?. [Internet] Simplicable. Raspoloživo na: https://simplicable.com/new/information-security-risk [27.01.2020].
15. Statista. 2019. Europe: Number Of Smes | Statista. [Internet] Raspoloživo na: https://www.statista.com/statistics/878412/number-of-smes-in-europe-by-size/ [13.06 2020].
16. Udovičić, M., Baždarić, K., Bilić-Zulle, L. and Petrovečki, M., 2007. Što Treba Znati Kada Izračunavamo Koeficijent Korelacije?. [Internet] Hrcak.srce.hr. Raspoloživo na: https://hrcak.srce.hr/12855 [12.07.2020].

Knjiga:

1. Becker, J., Bergener, P., Eggert, M., Heddier, M., Hofmann, S., Knackstedt, R. and Räckers, M., (2010). IT-Risiken. Münster: Inst. für Wirtschaftsinformatik.
2. Gantz, S. and Philpott, D. (2013). FISMA and the risk management framework [recurso electrónico]. Estados Unidos: Syngress.
3. Gordon, LA, Loeb, MP, Lucyshyn, W, Richardson, R (2005) CSI/FBI Computer Crime and Security Survey, Computer Security Institute.
4. Hopkin, P., (2017). Fundamentals Of Risk Management. 4th ed. United States: Kogan.
5. Kluge, F. and Seebold, E., (2011). Etymologisches Wörterbuch Der Deutschen Sprache. Berlin: De Gruyter.
6. Palomares Carrascosa, I., Kalutarage, H. and Huang, Y., (2017). Data Analytics And Decision Support For Cybersecurity. Belfast: Springer.
7. Panian, Z., Spremić, M., Groznik, A., Kostić, D., Osterman, M., Perica, I., Perko, V., Popović, M. and Smojver, S. (2007). Korporativno upravljanje i revizija informacijskih sustava. Zagreb: Zgombić.
8. Pereža, D. (2017). 'INTERNET SIGURNOST I E-TRGOVINA : Završni rad', Završni rad, Sveučilište u Splitu, Ekonomski fakultet
9. Piaz, J., (2002). Operational Risk Management Bei Banken. Zürich: Versus.

10. Rudel, S., Rieb, A., Dännart, S. and Lechner, U. (2018). Case Kritis - Fallstudien zur IT-Sicherheit in Kritischen Infrastrukturen.
11. Spremić, M. (2017). Digitalna transformacija poslovanja. Zagreb: Sveučilište u Zagrebu, Ekonomski fakultet.
12. Spremić, M., (2017). Sigurnost I Revizija Informacijskih Sustava U Okruženju Digitalne Ekonomije. Zagreb: Sveučilište u Zagrebu, Ekonomski fakultet.
13. Talabis, M. and Martin, J., (2013). Information Security Risk Assessment Toolkit. 1st ed. Waltham: Syngress.
14. Wegener, C., Milde, T. and Dolle, W., 2016. Informationssicherheits-Management. Berlin: Springer Vieweg.

E-Book:

1. 2011. Attitudes On Data Protection And Electronic Identity In The European Union. [ebook] Brussels: TNS Opinion & Social. Raspoloživo na: https://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_359_en.pdf [21.03.2020].

POPIS SLIKA

POPIS GRAFIKONA

POPIS TABLICA

PRILOZI RADU

Prilog 1: Popis pitanja te rangiranje odgovora pri statističkoj obradi

Redni broj ispred odgovora predstavlja i rang toga odgovora u rezultatima:

- Veličina poduzeća prema broju zaposlenih
    1. Mikro (<10 zaposlenih)
    2. Malo (11-49 zaposlenih)
    3. Srednje (50-249 zaposlenih)
    4. Veliko (250> zaposlenih)
- Sektor djelatnosti kojim se poduzeće bavi
    1. Autoindustrija
    2. Consulting
    3. Mesna industrija
    4. Financijsko posredovanje
    5. Gastronomija
    6. Gradjevinarstvo
    7. Hoteli
    8. Marketinška agencija
    9. Najam apartmana
    10. Proizvođać IT opreme i komponenata
    11. Projektiranje
    12. Projektiranje elektroenergetskih mreža
    13. Pružatelj IT outsourcing usluga
    14. Softversko poduzeće (ISV)
    15. Telekomunikacije
    16. Trgovina
    17. Zaštita na radu
- Starost poduzeća u godinama
    1. 0-10
    2. 11-30
    3. 31-50
    4. 51>

- Vaša uloga u poduzeću je?
    1. Istraživač
    2. Praktikant
    3. Stalni zaposlenik
    4. Student
    5. Unaprjeđivač prodaje
    6. Vlasnik
    7. Voditelj određenog odjela
- Da li radite identifikaciju rizika za Vaše poduzeće?
    1. Da
    2. Ne
- Koliko često radite identifikaciju rizika?
    1. Jednom godišnje
    2. Ne radimo identifikaciju rizika
    3. Ovisno o projektu
    4. ovisno o stabilnosti tržišta
    5. Više puta godišnje
- Koje metode koristite pri identifikaciji rizika? (mogućnost višestrukog odabira)
    1. Metoda induktivne ili teorijske analize
    2. Metoda sustavnog pristupa
    3. Ne radimo identifikaciju rizika
    4. Povijesna metoda
    5. Povijesna metoda , Metoda induktivne ili teorijske analize
    6. Povijesna metoda , Metoda sustavnog pristupa
    7. Povijesna metoda, Metoda sustavnog pristupa, Metoda induktivne ili teorijske analize
- Da li radite analizu rizika za Vaše poduzeće?
    1. Da
    2. Ne
- Koji pristup koristite pri izradi analize rizika?
    1. Kvalitativni pristup
    2. Kvantitativni pristup
    3. Ne radimo analizu rizika

- Da li radite procjenu rizika za Vaše poduzeće?
    1. Da
    2. Ne
- Koji pristup koristite pri izradi procjene rizika?
    1. Bottom-up pristup
    2. Top-down prostup
    3. Ne radimo procjenu rizika
- Koje korake koristite pri izradi procjene rizika? (mogućnost višestrukog odabira)
    1. Definicija imovine, Identifikacija prijetnje, Određivanje vjerojatnosti od pojave rizika, Određivanje utjecaja prijetnje, Kontrola rizika
    2. Definicija imovine, Identifikacija prijetnje, Određivanje vjerojatnosti od pojave rizika, Određivanje utjecaja prijetnje, Kontrola rizika, Dokumentacija
    3. Identifikacija prijetnje
    4. Identifikacija prijetnje, Dokumentacija
    5. Identifikacija prijetnje, Određivanje utjecaja prijetnje, Dokumentacija
    6. Identifikacija prijetnje, Određivanje utjecaja prijetnje, Kontrola rizika
    7. Identifikacija prijetnje, Određivanje vjerojatnosti od pojave rizika, Određivanje utjecaja prijetnje
    8. Identifikacija prijetnje, Određivanje vjerojatnosti od pojave rizika, Određivanje utjecaja prijetnje, Kontrola rizika, Dokumentacija
    9. Kontrola rizika
    10. Ne radimo procjenu rizika
    11. Određivanje vjerojatnosti od pojave rizika
- Sa kojim sve izazovima se susreće Vaše poduzeće kod upravljanja informatičkim rizicima? (mogućnost višestrukog odabira)
    1. Nedostatak stručnjaka za upravljenje rizicima
    2. Nedostatak znanja samog osoblja o informatičkim rizicima
    3. Nedovoljno resursa (ljudi, financije...)
    4. Nedovoljno resursa (ljudi, financije...), Nedostatak stručnjaka za upravljanje rizicima
    5. Nedovoljno resursa (ljudi, financije...), Nedostatak stručnjaka za upravljanje rizicima, Upravljanje informatičkim rizicima se ne shvaća ozbiljno

6. Nedovoljno resursa (ljudi, financije...), Nedostatak stručnjaka za upravljanje rizicima, Upravljanje informatičkim rizicima se ne shvaća ozbiljno, Nedostatak znanja samog osoblja o informatičkim rizicima
7. Nedovoljno resursa (ljudi, financije...), Upravljanje informatičkim rizicima se ne shvaća ozbiljno
8. Upravljanje informatičkim rizicima se ne shvaća ozbiljno
9. Upravljanje informatičkim rizicima se ne shvaća ozbiljno, Nedostatak znanja samog osoblja o informatičkim rizicima

- Da li je Vaše poduzeće doživjelo hakerski napad?
    1. Da
    2. Ne
    3. Ne znam
- Što od sljedećega čini Vaše poduzeće kako bi se zaštitilo od napada? (mogućnost višestrukog odabira)
    1. Ne znam
    2. Korištenje vatrozida, Redovita izrada sigurnosnih kopija bitnih podataka
    3. Korištenje vatrozida, Svaki zaposlenih ima zaseban korisnički račun
    4. Redovito ažuriranje antivirusnih sustava na svakom računalu u poduzeću, Korištenje vatrozida
    5. Redovito ažuriranje antivirusnih sustava na svakom računalu u poduzeću, Korištenje vatrozida, Ograničava zaposlenicima pristup određenim podacima
    6. Redovito ažuriranje antivirusnih sustava na svakom računalu u poduzeću, Korištenje vatrozida, Redovita izrada sigurnosnih kopija bitnih podataka, Svaki zaposlenih ima zaseban korisnički račun, Ograničava zaposlenicima pristup određenim podacima, Redovito mijenja lozinke korisničkih računa
    7. Redovito ažuriranje antivirusnih sustava na svakom računalu u poduzeću, Korištenje vatrozida, Svaki zaposlenih ima zaseban korisnički račun, Ograničava zaposlenicima pristup određenim podacima
    8. Redovito ažuriranje antivirusnih sustava na svakom računalu u poduzeću, Korištenje vatrozida, Svaki zaposlenih ima zaseban korisnički račun, Ograničava zaposlenicima pristup određenim podacima, Redovito mijenja lozinke korisničkih računa

9. Redovito ažuriranje antivirusnih sustava na svakom računalu u poduzeću, Redovita izrada sigurnosnih kopija bitnih podataka, Svaki zaposlenih ima zaseban korisnički račun, Ograničava zaposlenicima pristup određenim podacima, Redovito mijenja lozinke korisničkih računa
10. Redovito ažuriranje antivirusnih sustava na svakom računalu u poduzeću, Redovita izrada sigurnosnih kopija bitnih podataka, Svaki zaposlenih ima zaseban korisnički račun, Redovito mijenja lozinke korisničkih računa
11. Redovito ažuriranje antivirusnih sustava na svakom računalu u poduzeću, Redovito mijenja lozinke korisničkih računa
12. Redovito mijenja lozinke korisničkih računa
13. Svaki zaposlenih ima zaseban korisnički račun
14. Zaposlenici se upoznavaju sa tematikom informatičkih rizika
15. Zaposlenici se upoznavaju sa tematikom informatičkih rizika, Korištenje vatrozida, Redovita izrada sigurnosnih kopija bitnih podataka, Svaki zaposlenih ima zaseban korisnički račun, Ograničava zaposlenicima pristup određenim podacima, Redovito mijenja lozinke korisničkih računa
16. Zaposlenici se upoznavaju sa tematikom informatičkih rizika, Redovita izrada sigurnosnih kopija bitnih podataka
17. Zaposlenici se upoznavaju sa tematikom informatičkih rizika, Redovito ažuriranje antivirusnih sustava na svakom računalu u poduzeću, Korištenje vatrozida, Ograničava zaposlenicima pristup određenim podacima, Redovito mijenja lozinke korisničkih računa
18. Zaposlenici se upoznavaju sa tematikom informatičkih rizika, Redovito ažuriranje antivirusnih sustava na svakom računalu u poduzeću, Korištenje vatrozida, Redovita izrada sigurnosnih kopija bitnih podataka, Svaki zaposlenih ima zaseban korisnički račun
19. Zaposlenici se upoznavaju sa tematikom informatičkih rizika, Redovito ažuriranje antivirusnih sustava na svakom računalu u poduzeću, Korištenje vatrozida, Redovita izrada sigurnosnih kopija bitnih podataka, Svaki zaposlenih ima zaseban korisnički račun, Ograničava zaposlenicima pristup određenim podacima, Redovito mijenja lozinke korisničkih računa
20. Zaposlenici se upoznavaju sa tematikom informatičkih rizika, Redovito ažuriranje antivirusnih sustava na svakom računalu u poduzeću, Korištenje

vatrozida, Redovita izrada sigurnosnih kopija bitnih podataka, Svaki zaposlenih ima zaseban korisnički račun, Redovito mijenja lozinke korisničkih računa

21. Zaposlenici se upoznavaju sa tematikom informatičkih rizika, Redovito ažuriranje antivirusnih sustava na svakom računalu u poduzeću, Korištenje vatrozida, Svaki zaposlenih ima zaseban korisnički račun, Ograničava zaposlenicima pristup određenim podacima, Redovito mijenja lozinke korisničkih računa
22. Zaposlenici se upoznavaju sa tematikom informatičkih rizika, Redovito ažuriranje antivirusnih sustava na svakom računalu u poduzeću, Korištenje vatrozida, Svaki zaposlenih ima zaseban korisnički račun, Ograničava zaposlenicima pristup određenim podacima, Redovito mijenja lozinke korisničkih računa
23. Zaposlenici se upoznavaju sa tematikom informatičkih rizika, Redovito ažuriranje antivirusnih sustava na svakom računalu u poduzeću, Svaki zaposlenih ima zaseban korisnički račun, Ograničava zaposlenicima pristup određenim podacima, Redovito mijenja lozinke korisničkih računa, 3FA, VPN na nivou firme
24. Poduzeće ne poduzima ništa po tom pitanju

- Da li Vaše poduzeće posjeduje neki od standarda iz obitelji ISO/IEC 27000?
    1. Da
    2. Ne
    3. Ne znam