FBIM Transactions
DOI 10.12709/fbim.07.07.02.08

# UPRAVLJANJE RIZIKOM – CYBER SIGURNOST

## RISK MANAGEMENT - CYBER SECURITY

**Branka Mijić**
Fakultet za kriminologiju i sigurnosne studije, Sarajevo, Bosna i Hercegovina


JEL kategorija rada: **G32**

***Apstrakt***

*Svjedoci smo velikog utjecaja interneta i informacijske tehnologije na ljudski život . U današnjem vremenu, za koje možemo sa sigurnošću reći da je postalo ovisno o informatičkoj tehnologiji i elektroničkim komunikacijama, poslovni subjekti i fizičke osobe sve više postaju izloženi raznim oblicima cyber napada i kriminala. Informacijsko - tehnološko doba sa sobom nosi određene izazove i rizike. Cyber napadi mogu imati razorne posljedice i velik utjecaj na državne, poslovne subjekte, njihove djelatnike, kupce ali i treće osobe. Takvi napadi i prijetnje danas su među najvećim rizicima s kojima se suočava korporativni sektor u svijetu i stalno se iznalaze neki novi modusi sigurnosti istih kako bi tržištu ponudila modernije i sofisticiranije proizvode koji sadrže pokrića za takve rizike. Upravljanje rizicima je moralna i zakonska obveza svake organizacije i društva. Upravljanje rizicima omogućuje organizaciji jasan pogled na rizike i mogućnost proaktivnog djelovanja u svrhu zaštite resursa i poslovanja organizacije. Cyber sigurnost je u posljednjih nekoliko godina nešto o čemu se napokon počelo više pričati i obraćati veća pozornost, a svjedoci smo sve brojnijih hakerskih napada kao jednog od najvećih izazova sa kojim se suočava menadžment najznačajnijih svjetskih kompanija.*

***Ključne riječi:*** *Cyber- sigurnost, cyber-kriminal, cyber-rizik, upravljanje rizikom.*

***Abstract***

*We are witnessing the great impact of the Internet and information technology on human life. Today, we can say with certainty that business entities and individuals are becoming more and more exposed to various forms of cyber-attacks and crime. The information and technology carry certain challenges and risks. Cyber-attacks can have devastating consequences and huge impact on government, businesses subjects, their employees, customers, but also third parties. Such attacks and threats are among the biggest risks facing the corporate sector in the world today, and different modes of Internet and information technology security are used to cover risks. Risk management is a moral and legal obligation of every organization and society. Risk management gives the organization a clear view of the risks and the ability to act proactively to protect the resources and operations of the organization. Cyber security has been something*

*Adresa autora:*
***Branka Mijić***
*brankica_mijic@net.hr*

*that has finally started to be talked about and paid more attention in recent years, as we are witnessing an increasing number of hacking attacks, which represent one of the biggest challenges for managements of most prominent global companies.*

***Keywords**: Cyber security; cybercrime; cyber risk; risk management;*

## 1 UVOD

Svjedoci smo da se modernizacijom i informatizacijom poslovanja sigurnosni rizik povećava, a kada informacije nisu adekvatno zaštićene postoji mogućnost da to ugrozi ne samo poslovne organizacije nego i cijelo društvo. Bez obzira kakva bila informacija ona je uvijek izložena različitim rizicima iz različitih izvora. Sa stalnim povećanjem korištenja novih tehnologija za pohranu, prijenos i pristup informacijama, informacije su postale mnogo ranjivije na povećan broj i vrstu prijetnji. Bez obzira koju formu ima ili na koji način je pohranjena ili na koji način se dijeli, informacija uvijek treba da bude zaštićena na odgovarajući način.

Prema riječima Roberta S. Mullera, direktora FBI-a koji navodi: „Postoje samo dvije vrste tvrtki: one koje su hakirane i one koje će biti hakirane. Pa čak i one konvergiraju u jednu kategoriju: tvrtke koje su hakirane i one koje će opet biti hakirane“ (Mueller, 2012).

Upravljanje rizicima je moralna i zakonska obveza svake organizacije i društva. Upravljanje rizicima omogućuje organizaciji jasan pogled na rizike i mogućnost pro aktivnog djelovanja u svrhu zaštite resursa i poslovanja organizacije.

Srž programa upravljanja rizikom predstavlja stalni ili tekući proces procjene rizika. Ovo uključuje razumijevanje tolerancije rizika, znanje o vjerojatnim rizicima i prijetnjama, izmjerene procjene uspostavljenih kontrola, i izvršnih planova da bi se adresirale identificirane ranjivosti. Strategija upravljanja rizikom informacija je usmjerena na čuvanje povjerljivosti, održavanje cjelovitosti podataka i osiguranje dostupnosti informacija za korisnike koji imaju odobrenje njihove upotrebe. Efektivan program upravljanja rizikom informacija može biti jedino osiguran kroz marljivost i predanost svake osobe koja ima pristup povjerljivim informacijama. Zajedno sa osobnim integritetom, predanost je jedna od ključnih pretpostavki koja se tiče svake odgovorne osobe unutar organizacije. Pojam osobne odgovornosti je model koji se ima pratiti ukoliko se ima zaista zaštiti informacija. Ključ za pro aktivnu zaštitu je prepoznavanje stvarne dinamike prijetnje. Ona se stalno mijenja i prilagođava naporima da se sačuvaju vitalne informacije (Courtney, Haynes, Paradice, 2005).;

## 2 SIGURNOSNI RIZIK INFORMACIJA I UPRAVLJANJE RIZIKOM

Prijetnje u oblasti informacijske sigurnosti potječu iz raznih izvora, te se manifestiraju takvim aktivnostima koje su usmjerene na pojedince, poslovne subjekte, nacionalne infrastrukture i vlade. Njihovo djelovanja nosi značajan rizik po opću sigurnost, nacionalnu sigurnost i stabilnost međusobno umrežene međunarodne zajednice (UN General Assembly, 2010).

Ključni rezultati sedmog Allianzovog barometra rizika kojeg svake godine objavljuje u izvješću za 2018. Godinu, a temelji se na uvidu rekordnih 1.911 stručnjaka za rizike iz 80 zemalja. A to je da zastoji u poslovanju i cyber incidenti ostaju na prvom mjestu kao i lani, cyber incidenti su ove godine skočili s trećeg na drugo mjesto i ciljaju na temelje povezanih ekonomija radi čega mogu ugroziti najveće prijetnje globalnog poslovnog rizika, zaključeno je u istraživanju Allianzova barometra rizika 2018. (Allianz Global Corporate & Specialty (AGCS), 2018). Također, procjenjuje se da prosječan trošak ispada digitalnog oblaka koji traje više od 12 sati za tvrtke u financijskom, zdravstvenom i maloprodajnom sektoru može ukupno iznositi 850 milijuna USD u Sjevernoj Americi i 700 milijuna USD u Europi.

Kako bi se smanjili cyber rizici definirani su četiri temeljne aktivnosti (CROForum, 2014):

1. **Priprema** Potrebno je razumjeti svoju kritičnu imovinu; razvijati sposobnosti za rješavanje različitih razina rizika; utvrditi sklonost riziku i upravljanje rizicima ugraditi u cijelu organizaciju.
2. **Zaštita** Osigurati dobro utemeljenu i ponovljivu *cyber*-pripravnost; poduzeti ocjenjivanje prijetnji i kontrola: osigurati odgovarajućom pozornošću provjeru procesa za treće osobe; omogućiti i osnažiti

upravljanje incidentima i sposobnost odgovora; razvijati i provoditi plan odgovora na incident, kontinuirano se obrazovati i usavršavati.

3. **Detekcija** Razviti otkrivanje i kontinuirano praćenje sposobnosti za rješavanje nepravilnosti i prijetnji prema imovini tvrtke.
4. **Poboljšanje** Izgraditi sveobuhvatnu bazu podataka sigurnosnih incidenata koji podržavaju kontinuirano učenje i omogućiti oporavak od incidenta u najkraćemu roku.

## 3 IZLOŽENOST CYBER RIZIKU

Cyber rizici su još u 2014.godini ušli među deset (10) najvećih globalnih poslovnih rizika. Svjetska ekonomija zbog cyber kriminala i raznih napada godišnje gubi cca 445 milijardi $.

Gubitci koji proizlaze iz cyber napada, nenamjernih ili namjernih IT propusta mogu se kategorizirati u 11 grupa što je prikazano u tablici 1.

*Tablica 1. Kategorije gubitaka koji proizlaze iz cyber-napada i nenamjernih IT propusta. (Mersc, 2015).*

| | KATEGORIJA GUBITKA | OPIS |
|---|---|---|
| 1. | Krađa intelektualnoga vlasništva | Gubitak vrijednosti imovine intelektualnoga vlasništva, izraženo u smislu gubitka prihoda kao rezultat smanjenoga udjela na tržištu. |
| 2. | Prekid poslovanja | Izgubljena dobit ili drugi troškovi nastali zbog nedostupnosti IT sustava ili podataka kao posljedica *cyber*-napada ili ostalih zlonamjernih IT propusta. |
| 3. | Gubitak podataka i aplikacija | Trošak rekonstrukcije podataka ili softvera koji je izbrisan ili korumpiran. |
| 4. | *Cyber*-iznuda | Trošak stručnjaka za rukovanje incidentom *cyber*-iznude, u kombinaciji s iznosom plaćanja otkupnine. |
| 5. | *Cyber*-kriminal/*cyber*-prijevara | Izravni financijski gubitak koji je pretrpjela organizacija, a koji proizlazi iz korištenja računala za počinjenje prijevare ili krađe novca, vrijednosnih papira ili druge imovine. |
| 6. | Događaj povrede privatnosti | Trošak istraživanja i odgovora na događaj povrede privatnosti, uključujući i IT forenziku i obavještavanje zahvaćenih nositelja podataka. Odgovornosti potraživanja trećih strana koje proizlaze iz istoga incidenta. Kazne od regulatora i udruga. |
| 7. | Mrežne pogreške | Obveze trećih strana koje proizlaze iz nekih sigurnosnih događaja koji se javljaju u organizaciji IT mreže ili prolaze kroz nju da bi napali treću osobu. |
| 8. | Utjecaj na reputaciju | Gubitci prihoda koji proizlaze iz povećanja odljeva kupaca ili smanjenja volumena transakcija, koji se mogu izravno pripisati objavi događaja povrede sigurnosti. |
| 9. | Fizičko oštećenje imovine | Gubitak prve strane zbog uništenja fizičke imovine koji proizlazi iz *cyber*-napada. |
| 10. | Smrt i tjelesna oštećenja | Odgovornost trećih osoba za smrt i tjelesne ozljede proizašle iz *cyber*-napada. |
| 11. | Istraživanje incidenta i troškovi odgovora | Izravni troškovi nastali istraživanjem i zatvaranjem incidenta i smanjivanje gubitaka nakon incidenta. Odnosi se na sve ostale kategorije/događaje. |

Povećanje međusobne povezanosti, globalizacija i komercijalizacija cyber-kriminala dovode do veće učestalosti i ozbiljnosti cyber-incidenata, uključujući povrede podataka. Privatnost i zaštita podataka jedan je od ključnih cyber-rizika (European Cybercrime Centre - Europol., 2014).

Prekid poslovanja, krađe intelektualnoga vlasništva i cyber-iznude, bilo za financijsku, bilo za nefinancijsku dobit, povećavaju potencijalni rizik. Troškovi prekida poslovanja mogu biti jednaki ili čak premašiti izravne gubitke od povrede podataka. Utjecaj prekida poslovanja pokrenut tehničkim kvarom često je podcijenjen u odnosu na cyber-napad (Allianz, 2015).

Važno je napomenuti kako velike kompanije i državne tvrtke nisu jedine ranjive na razorne cyber-napade. Podatak je taj koji čini posao atraktivnim, a ne veličina — pogotovo ako je riječ o zanimljivim podatcima, kao što su kontakt-informacije o kupcima, podatci o kreditnim karticama, zdravstveni podatci ili vrijedno intelektualno vlasništvo (Armerding, 2015).

Manje su tvrtke atraktivne jer nemaju iste resurse kao velika poduzeća, stoga imaju tendenciju ka slabijoj strategiji cyber-sigurnosti. Zbog niskih troškova prodaje više posluju online[1] i putem različitih cloud-usluga[2]. Te se tvrtke koriste slabijom sigurnosnom zaštitom i slabijom tehnologijom enkriptiranja, tako da su izloženije riziku.

Danas, kako su rizici i prijetnje postali mnogo sofisticiraniji, javljaju se i dva dodatna temeljna zadatka (Yildirim, 2017):

- definirati ekosistem organizacije,
- predstaviti i uvesti obuku sigurnosne svjesnosti za zaposlenike

Upravljanje rizikom informacijskog sustava neizostavni je dio gotovo svakog okvira upravljanja informacijskom sigurnošću i zaštite osobnih podataka. Kao temelj za donošenje odluka, procjena rizika, a i cijeli proces upravljanja rizikom igra važnu ulogu u postupku implementacije sustava upravljanja informacijskom sigurnošću. Na temelju procjene rizika odabiru se financijski i poslovno opravdane sigurnosne kontrole koje će sigurnosni rizik umanjiti na prihvatljivu razinu.

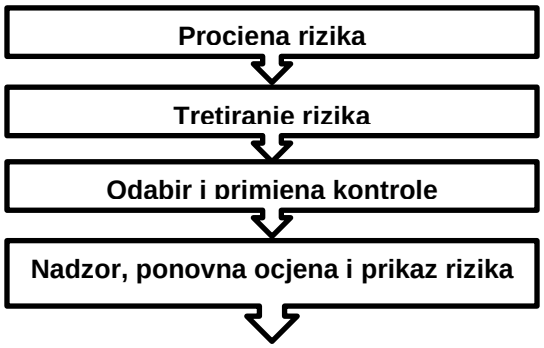
Učinkovito upravljanje rizicima započinje identificiranjem neposrednih rizika za poslovanje te educiranjem odbora i voditelja o tome što ti rizici predstavljaju i čime mogu rezultirati. Svi su odgovorni učinkovito upravljati rizicima. Neovlašteni pristup podacima može uzrokovati ogromnu financijsku štetu i dovesti do narušavanja ugleda. Upravljanje rizicima treba biti dio sveobuhvatnog programa procjene postupaka za upravljanje rizicima, primjene principa za upravljanje rizicima te, u konačnici, osvještavanja zaposlenika u vezi toga kako uočavanje rizika nije neuspjeh, već potvrda dogovorenih postupaka.


*Slika 1.* Komponente upravljanja rizikom

*Izvor* (Yildirim, 2017)

Upravljanje rizikom je ključ upravljanja organizacijom i ključ zaštite njenih informacionih kapaciteta. Ukoliko organizacija nije svjesna rizika sa kojima se susreće ona neće biti u stanju primijeniti odgovarajuću efektivnu zaštitu. Proces identifikacija rizika možemo prikazati kako slijedi na slici 2.

Uopćeno, opširna procjena rizika informacione sigurnosti je neophodna da bi se uspostavilo razumijevanje faktora rizika koji štete organizaciji. Dalje, takva procjena mora biti urađena sa uvažavanjem politika zasnovanih na riziku i standardima odsustva upotrebljive statistike o incidentima. Usvajanje procesa rigoroznog pristupa svim rizičnim poveznicama vezanim uz prijetnje informacionoj sigurnosti je ključno u razvoju koherentne strategije sigurnosnog upravljanja rizikom informacija (Young, 2010).




*Slika 2. Proces upravljanja rizikom*
*Izvor: (Humphreys, 2008)*

[1] Onlajn-poslovanje - obavljanje poslovnih procesa na internetu. http://searchcio.techtarget.com/definition/e-business,

[2]Cloud-opći termin koji se upotrebljava za pružanje iznajmljenih usluga putem interneta. http://searchcloudcomputing.techtarget.com/definition/cloud-computing

Svi sudionici u procesu, bilo organizacije ili individualne osobe, trebaju provoditi periodične procjene rizika kojima se identificiraju prijetnje i ranjivosti. Procjene rizika trebaju biti dovoljno široko usmjerene kako bi obuhvatile ključne unutarnje i vanjske faktore, kao što su tehnologije, fizički i ljudski faktori, politike i treća strana pružanja usluga. Procjene rizika trebaju omogućiti određivanje prihvatljive razine rizika, te pomoći u odabiru odgovarajućih kontrola za upravljanje rizikom od potencijalne štete informacijskim sistemima i mrežama u svjetlu prirode i važnosti informacija koje trebaju biti zaštićene.

| KLJUČNI PRINCIPI UPRAVLJANJA RIZIKOM | PRIMIJENJENI NA KIBER CYBER RIZIK |
|---|---|
| **1. Fokus na ono što je najvažnije** Mora se poklapati sa vašom jedinstvenom kulturom posla i rizika | **Poznajete svoje kritične informacione kapacitete.** Identifikacija kritičnih poslovnih kapaciteta najranjivijih na cyber napade |
| **2. Mjerenje i izvještavanje** Uključuje kvalitativne obračune i kvantitativna mjerenja | **Učinite cyber napade opipljivijim.** Jasno definirati cyber rizik i osnovne matrice |
| **3. Opširnost u suštini.** Treba pokriti sve vrste rizika, trenutne i one koje očekujemo | **Uskladiti sa postojećim okvirima rizika.** Financijskim, operativnim, regulatornim, okvirom potražnje, reputacionim, itd. |
| **4. Raspoređivanje apetita za rizik** Raspoređivanje apetita na poslovne jedinice i vrste rizika. | **Učinite cyber rizike relevantnim u skladu s poslom.** Povezati rizike organizacionih nivoa sa individualnim poslovnim jedinicama i njihovim informacionim kapacitetima |
| **5.Integracija sa poslovnim planiranjem** Regulacije sve više traže dokaze | **Ugraditi rizične želje u investicione odluke.** Prioritizirati investicije gdje je kritično, ojačati poslove da se informiraju lokalne odluke. |

*Slika 3.* Principi upravljanja rizikom
*Izvor:* (Carol, Siegel, Serritella, Serritella, 2002)

## 4 STANDARDI INFORMACIONE SIGURNOSTI (ISO 27001)

Standard ISO 27001 primorava organizacije da pripreme upravljanje rizikom i planove procesuiranja rizika, dužnosti i odgovornosti, planove poslovnog kontinuiteta, upravljačke proceduru u slučaju hitnog stanja i da vode zabilješke o njima. Organizacija, odnosno poduzeće moraju objaviti politike informacione sigurnosti i navesti njihov personal na zaključke o informacionoj sigurnosti i prijetnjama toj sigurnosti. Kao stalan proces, rukovodstvo informacione sigurnosti u organizaciji pokriva odabrane ciljeve kontrole i njihovu procjenu. Prikladnost kontrole njenom cilju i njena učinkovitost se neprestano nadziru i ovo može biti ostvareno jedino aktivnom podrškom rukovodstva i učešćem personala (Vural, Sagıroglu, 2008).

Informacioni sigurnosni standardi moraju biti primijenjeni u svim organizacijama radi upravljanja rizikom na svim nivoima. Ukoliko je upravljanje rizikom dobro rukovođeno, informaciona sigurnost će biti efektivnija. Svi nivoi unutar organizacije trebaju biti uređeni kako slijedi (Saint-Germain, 2005):

- Na organizacionom nivou, određuje odgovornosti i garantirane koristi od primjene poduzetničke/organizacijske informacione sigurnosti na svakom nivou.
- Na pravnom nivou, pokazuje vlastima da je poduzeće ili organizacija prihvatila sva važeća pravila i regulative i da ispunjava sve standarde i principe.
- Na poduzetničkom nivou, upućuje poduzetništvo na informacione sisteme, na njihove slabosti i kako će biti zaštićeni, pa se na taj način osigurava siguran pristup za informacioni sistem poduzetnika

- Na komercijalnom nivou, poslovni partneri, dioničari i kupci podižu stepen svog povjerenja prema poduzetniku; zahvaljujući važnosti koju je poduzetnik dao zaštiti informacija postiže se bolja pozicija na tržištu i povećava se konkurentnost.
- Na financijskom nivou, kao posljedica identificiranja sigurnosnih propusta (rupa) i poduzimanje mjera za njihovo saniranje, troškovi će se smanjiti.
- Na zaposleničkom nivou, povećava se znanje zaposlenika u sigurnosnim subjektima i njihove lične odgovornosti unutar organizacije i doprinosi tome da svaki zaposlenik bude svjesna jedinka.

## 5 DISKUSIJA

Sve organizacije ili institucije su izložene riziku, i najveći broj njih ima neku vrstu upravljanja rizikom. Ipak, ukoliko nastojimo točno razumjeti vrste i prirodu rizika, te ukoliko hoćemo da ih uredimo na sistematičan i efektivan način, trebamo dobro definiran proces za upravljanje rizikom. Nadalje, trebamo da razumijemo osnovne principe i okvire vezane uz proces upravljanja rizikom (Refsdal, Solhaug, Stølen, 2015).

Obzirom da možemo pretpostaviti da organizacije ne mogu prevenirati sve incidente, tradicionalna disciplina sigurnosti, izdvojena iz opširnijeg pristupa baziranom na riziku, nije dovoljna da se zaštiti od prijetnji. Unapređujući informaciono upravljanje rizikom ne znači uvijek trošenje više novca, te podjednako tome ne znači ni samo kupovinu posjednih tehnologija i alata upravljanja rizikom. Da bi bio efektivan, program upravljanja rizikom zahtijeva efektivno menadžersko znanje i sposobnosti, prosudbe i donošenje odluka što sve zajedno predstavlja pokretače uspješne dinamike sistema upravljanja rizikom. Sistemski faktori kao što je procijenjeni rizik od strane menadžmenta, željeni nivoi investicije upravljanja rizikom, kapaciteti detekcije rizika i povjerenje personala su u dinamičnoj interakciji i mogu stvoriti povratne sprege koje ili ojačavaju kapacitete smanjenja rizika ili proizvode i izlažu organizaciju unutrašnjim prijetnjama. Smanjenje takve ranjivosti na napade od unutrašnjih prijetnji uključuje unapređenje prikupljanje informacija o riziku, upravljanje takvim informacijama i ciljanu obuku personala u prosudbama i donošenju odluka (Martinez-Moyano, 2006). Uopćeno, opširna procjena informacionog sigurnosnog rizika je neophodna da bi se uspostavilo razumijevanje faktora rizika koji štete organizaciji. Dalje, takva procjena mora biti urađena u odnosu na standarde i politike koje su donesene po osnovu procijenjenih rizika uz odsustvo iskoristivih statistika o incidentima. Usvajajući proces rigoroznog pristupa rizik povezan sa sigurnosnom prijetnjom informacijama je ključan da bi se razvila konherentna strategija upravljanja rizikom kod sigurnosti informacija (Young, 2014). Efektivan proces unapređuje organizacijske sposobnosti u odnosu na suradnju sa vanjskim partnerima. Informaciona sigurnost osiguravajućih kompanija je, npr., je značajno i naglo porasla i postala sofisticiranija obzirom na njihove zahtijeva u kojima osiguravajuće kompanije, da bi bile profitabilne, zahtijevaju od svojih klijenata koji su pravna lica da im dostave svoje programe menadžmenta upravljanja rizikom. Osiguravatelji tako kreiraju izuzetke za pokriće na rizična ponašanja. Dodatno, rad za treće osobe kao pružač usluga, ili čak dolazak u priliku da se postane stalni suradnik, i sl. postaje mnogo lakše ukoliko se posjeduje utemeljen proces cyber sigurnosti. Praktično, danas svaki sporazum koji rezultira dobrom poslovnom transakcijom ima bitne zahtjeve vezane za predstavljanje i aktivnost informacione sigurnosti. Ovo pitanje se često previđa od strane kompanije sve dok dogovor ne postane konačan i kada jedna strana u svojoj predanosti poslu ne shvati da je druga strana zanemarila cyber sigurnost i da ih tim izlaže velikom riziku. Ovakav ishod je velika tragedija u vremenu kada je većina strategija start up kompanija vezana za ovo pitanje da ih kupe velike kompanije (Miller, 2011). Studija EY Globalne informacione sigurnosti iz 2015. godine, koja je ujedno jedna od najpriznatijih studija na godišnjem nivou unutar globalne informaciono-sigurnosne arene, istraživala je kreiranje povjerenja u svijetu digitalne sigurnosti, te ujedno i najvažnija pitanje cyber sigurnosti s kojima se susreću poslovi današnjice (Ernst, Young, 2015). Kao rezultat, ona pomaže kupcima da se fokusiraju na rizike koji identificiraju prednosti i manjkavosti njihovog informacionog sistema upravljanja rizikom i da daju analizu glede ovog pitanja. Jedno pitanje postavljeno u istraživanju kako bi se naglasila efektivnost informacione sigurnosti je bilo sljedeće: „Koju bi od pobrojanih

područja iz informacione sigurnosti definirali kao „važnu, srednje važnu ili nisku“ za vašu organizaciju, a u narednih 12 mjeseci? Rezultati su pokazali da su unutrašnji rizici i prijetnje odnijeli polovinu odgovora „srednje važno“ (Ernst, Young, 2015). Prema Deloitte (2014) „istraživanje informacione sigurnosti“ u Centralnoj Aziji ima tendenciju povećanja nivoa razumijevanja informacionih sigurnosnih programa i rukovodne strukture u organizaciji. Njihovo istraživanje se fokusiralo na informacione sigurnosne rizike u oko stotinu kompanija kroz online anketni upitnik. Rezultati su pokazali da su IT sektori kompanija svjesni sigurnosnih rizika vezanih uz informacije, dok je svijest poslovnog rukovodstva i krajnjih korisnika na niskom nivou, odnosno nedovoljna (Yildirim, 2016). Također, istraživanje je pokazalo da je svjesnost rizika na cyber prijetnje od strane IT odjela najviše proizvod javno dostupnih informacija. Pored toga, generalni je zaključak da se mnoge organizacije još uvijek muče da dostignu strateški nivo informacione sigurnosti. Ljudski faktor ostaje najslabija karika u cyber sigurnosti. Mnoge organizacije su nevoljne da iz vanjskih izvora potraže pomoć u aktivnostima zaštite informacija (Yildirim, 2017).

## 6 ZAKLJUČAK

Ovim radom se željelo prikazati osnove za uspostavu i zaštitu informacijskog sustava. Činjenica je da uvijek postoji mogućnost za opasnosti sustava pogotovo u suvremenom poslovanju pa stoga organizacije moraju biti toga svjesne i spremne na reakciju protiv mogućih prijetnji. Svjedoci smo da modernizacijom i informatizacijom poslovanja sigurnosni rizik se povećava, a kada informacije nisu adekvatno zaštićene postoji mogućnost da to ugrozi ne samo poslovne organizacije nego i cijelo društvo.

Zanemarimo li sustav informacijske sigurnosti, u smislu ne kontroliranja problema sigurnosti, vrlo lako možemo postati žrtvom napada. Sigurnosti sustava bi trebali pristupiti periodičnom kontroliranju, tražiti načine kako sustav učiniti još sigurnijim, otpornijim te implementirati dodatne sigurnosne kontrole koje savjetuju stručnjaci za informacijsku sigurnost. Nadalje, smo pokušali prikazati potencijalne gubitke koji proizlaze iz cyber napada. Poanta je da poslovne aktivnosti moraju biti zaštićene sa efektivnim sistemom upravljanja rizikom i da se ovaj sistem mora primjenjivati u ozbiljnom poslovanju, a prema standardu ISO 27001, a što je najvažnije da mora sve mora biti pokriveno zakonskim propisima.

Bitno je da se unutar poslovanja primjene ISMS standardi, da budu objašnjeni svim strankama u poslovanju, te da se uposle stručnjaci iz polja sigurnosti u aktivnosti poduzeća ili organizacije. Neophodnost upravljanja rizikom u cyber sigurnosti se odnosi i na obuku korisnika, tehničkog personala i menadžera ili uopćavanja savjetodavnih servisa. Nakon što su ISMS aplikacije primijenjene uspješno od strane poduzetnika, važno je da poduzetnici imaju međunarodno priznat certifikat za upravljanje informacionom sigurnošću (Yildirim, 2016). Aplikacijska sigurnost je proces koji se obavlja kako bi se primijenile odgovarajuće kontrole i mjerenja na organizacijske aplikacije, a s ciljem upravljanja rizikom njihovog korištenja. Kontrole i mjerenja mogu se primijeniti na samu aplikaciju (njene procese, komponente, softver i rezultate), na njene podatke (konfiguracijske podatke, korisničke podatke, organizacijske podatke), te na sve tehnologije, procese i aktere uključene u životni ciklus aplikacije.

Da bi omogućio visok nivo cyber sigurnosti u poduzeću, vrlo je važno razumijevanje i primjena standarda informacione sigurnosti kao i poznavanje trenutnih prijetnji. Pokazalo se, da bi se omogućio visok nivo cyber sigurnosti, da je neophodan pristup u trokutu tehnologija-čovjek-edukacija i da se on uvijek mora prvi razmatrati. Neophodno je za poduzetnike da se primjeni upravljanje rizikom u cyber sigurnosti u svrhu minimiziranja nivoa rizika i povećanja sigurnosti, te omogućavanja poslovnog kontinuiteta.

## CITIRANA DELA

Allianz Global Corporate &Security (2015). *A Guide to Cyber Risk, Managing the Impact of Increasing Interconnectivity*, Editor: Greg Dobie (greg.dobie@allianz.com). https://www.agcs.allianz.com/news-and-insights/reports/a-guide-to-cyber-risk.html

Armerding, T. (2015). *Why criminals pick on small business*. http://www.csoonline.com/article/2866911/cyber-attacks-espionage/ why-criminals-pick-on-small-business.html

Carol A. Siegel, T. R., Serritella, S., Serritella, P. (2002). *Information Security Management Practices, Cyber-Risk Management:Technical and Insurance Controls for Enterprise-Level Security*, EBSCO,

Courtney, J. F., Haynes, J.D. , Paradice, B. D. (2005). Inquiring Organizations: Moving from Knowledge Management to Wisdom. England: Idea Group Inc (IGI),

CROForum (2014). „Cyber Resilience-The cyber risk challenge and the role of insurance", KPMG Advisory N.V. http://www.munichre.com/site/corporate/get/ ocuments_E-558890045/ mr/assetpool. shared/Documents/0_Corporate%20Website/1_The%20Group/Emerging-Risks/CRO-Forum-cyber -risk-paper -2014-12.pdf

Deloitte. (2016). Information Security Survey Report 2014,

Ernst & Young. EY's Global İnformation security Survey Report 2015: Creating trust in the digital world. (2016) http://www.ey.com/Publication/vwLUAssets/ey-globalinformation-security-survey-2015/$FILE/ey-globalinformation-security-survey-2015.pdf

European Cybercrime Centre (EC3) - Europol (2014). „The Internet Organised Crime Threat Assesment (iOCTA) ". file:///Users/Air/ Downloads/europol_iocta_web.pdf

Humphreys, E. (2008). Information Security Technical Report, Elsevier, "Information Security Management Standards: Compliance, Governance and Risk Management",

Martinez-Moyano, I. J. (2006). *Modeling the Emergence of Insider Threat*

*Vulnerabilities*. Proceedings of the 2006 Winter Simulation Conference,

Miller, K. L. (2016). *About "Reasonable Cybersecurity: A Proactive and Adaptive Approach*. The Florida Bar Journal/September/October, vol. 90,

Mueller, R., S.(2012). FBI Director speech on RSA Cyber Security Conference, San Fracisko, CA. http://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies

Refsdal, A., Solhaug, B., Stølen, K. (2015). *Cyber-Risk Management*. SpringerBriefs in Computer Science,

Saint-Germain, R. (2005). *Information Security Management Best Practice Based on ISO/IEC 17799*.The Information Management Journal, vol. 39,

Sutton, D. (2010). *Information Risk Management a Practitioner's Guide*. Bcs the Chartered Institute for IT,

UN General Assembly. (2010). *A/65/201 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*.

Vural, Y., Sagıroglu, S. (2008). *A Review on Enterprise Information Security and Standarts*. J. Fac. Eng. Arch., Gazi Univ., Vol. 23,

Yildirim, E. Y. (2016). *Advances in Human Factors in Cybersecurity*. The Importance of Information Security Awareness for the Success of Business Enterprises, vol.501, Springer, USA,

Yildirim, E. Y. (2017). *The importance of risk management in information security.* International Journal of Advances in Electronics and Computer Science, Vol. 4, Issue 1,

Yildirim, E. Y. Akalp, G,. Aytac, S., Bayram, N. (2011). *Factors Influencing Information Security Management in Small and Medium-sized Enterprises:A Case Study from Turkey*. International Journal of Information Management, Elsevier,

Young, C. (2010). *Metrics and Methods for Security Risk Management*. Boston, Yngres,

Young, C. (2014). *The science and technology of counterterrorism; measuring physical and electronic security risk*.

Datum prve prijave: 16.08.2019.
Datum prijema korigovanog članka: 02.09.2019.
Datum prihvatanja članka: 11.10.2019.

**Kako citirati ovaj rad? / How to cite this article?**

***Style – APA Sixth Edition:***

Mijić, B. (2019, 10 15). Upravljanje rizikom – Cyber sigurnost. (Z. Čekerevac, Ed.) *FBIM Transactions, 7*(2), 69-77. doi:10.12709/fbim.07.07.02.08

***Style – Chicago Sixteenth Edition:***

Mijić, Branka. 2019. "Upravljanje rizikom – Cyber sigurnost." Edited by Zoran Čekerevac. *FBIM Transactions* (MESTE) 7 (2): 69-77. doi:10.12709/fbim.07.07.02.08.

***Style – GOST Name Sort:***

**Mijić Branka** Upravljanje rizikom – Cyber sigurnost [Journal] // FBIM Transactions / ed. Čekerevac Zoran. - Beograd : MESTE, 10 15, 2019. - 2 : Vol. 7. - pp. 69-77.

***Style – Harvard Anglia:***

Mijić, B., 2019. Upravljanje rizikom – Cyber sigurnost. *FBIM Transactions,* 15 10, 7(2), pp. 69-77.

***Style – ISO 690 Numerical Reference:***

*Upravljanje rizikom – Cyber sigurnost.* **Mijić, Branka**. [ed.] Zoran Čekerevac. 2, Beograd : MESTE, 10 15, 2019, FBIM Transactions, Vol. 7, pp. 69-77.