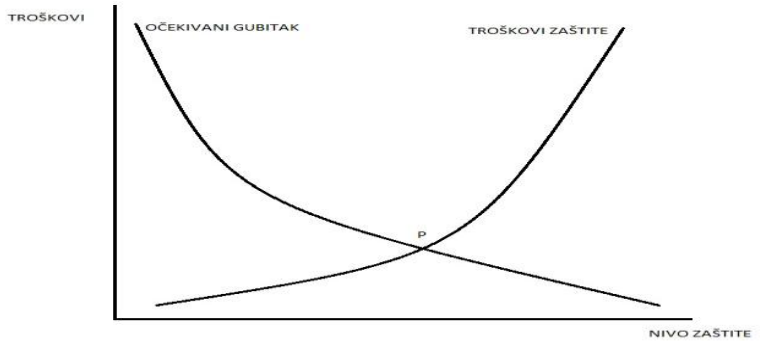
# STRATEGIJE ZAŠTITE INFORMACIONIH SISTEMA

Sa ovakvom tabelom menadžment firme se može lako opredeliti za neku od sledećih strategija:

- ***Izbegavanje rizika***: Privremeno odricanje od određenih funkcija i/ili komponenata sistema koji su najugroženiji i bez kojih ostatak sistema može da radi(*svesna i privremena degradacija sistema*),
- ***Prihvatanje rizika***: Ne preduzimanje bilo kakvih mera zaštite u odnosu na označene pretnje, (šteta izazvana tim pretnjama manja od troškova preduzimanja mera),
- ***Prenošenje rizika***: Prenošenje posledica štetnog događaja na nekog drugog(garantni rok, ugovor o održavanju, polise osiguranja),
- ***Kontrolisanje(limitiranje rizika)***: Preduzimanje odgovarajućih mera zaštite u odnosu na identifikovane pretnje u cilju anuliranja ili svođenja rizika na prihvatljiv nivo, kao i redukcije verovatnoće njihovog nastajanja. Ova strategija ima najveću težinu.

**Sigurnost** je proces održavanja prihvatljivog nivoa rizika i zahteva vreme i resurse da se ti zahtevi i odgovornosti ostvare. Ostvarivanje sigurnosti podrazumeva održavanje sistema u stanju prihvatljivog rizika, tj. kompromis između potrebnih ulaganja i smanjenja mogućnosti da nastane šteta koje se tim ulaganjem postiže. Veće ulaganje u sigurnost smanjuje izloženost sistema ili računarske mreže riziku. S druge strane, ono izlaže vlasnika većim troškovima i smanjuje profitabilnost i udobnost rada. Zato je veoma značajno da se odredi tačka u kojoj se postiže ravnoteža između ulaganja u sigurnost i postignutih efekata(slika 3). Presek krivih(tačka P) označava optimalni nivo zaštite.




Slika 3. Odnos potencijalnog gubitka i troškova zaštite

Sigurnost kao proceszasniva se na četiri osnovna koraka: **procena**(planiranje), **zaštita**(sprečavanje), **otkrivanje** i **odgovor**.

1. **Procena**(engl. *assessment*) je u vezi sa pravilima, procedurama, pravnom i drugom regulativom, određivanjem budžeta. i još je povezana s tehničkom procenom stanja sigurnosti. Greška u proceni može naškoditi svim operacijama koje slede.
2. **Zaštita**(engl. *protection*) tj.sprečavanje, podrazumeva primenu protivmera kako bi se smanjila mogućnost ugrožavanja sistema. Ukoliko zaštita zakaže, primenjuje se sledeći korak – otkrivanje.
3. **Otkrivanje**(engl. *detection*) predstavlja proces identifikacije upada, tj. povrede sigurnosnih prava na nezakonit, neovlašćen ili neprihvatljiv postupak koji je preduzet nad računarskim sistemom ili nad mrežom.
4. **Odgovor**(engl. *response*) ili reakcija predstavlja proces oporavka, tj. lečenja posledica upada. U aktivnosti reakcije spadaju postupci „zakrpi i nastavi“, ili „goni i sudi“. Ranije se na prvo mesto stavljalo oporavljanje funkcionalnosti oštećenih resursa, kao što je korišćenje rezervnih kopija podataka za vraćanje sistema u stanje pre izvršenog napada. U novije vreme sve češće se koriste pravna sredstva(sudski proces protiv onoga ko ugrožava sigurnost), među koja spada prethodno prikupljanje dokaza metodama digitalne forenzike pomoću kojih se potkrepljuje tužba.

U realizaciji sistema zaštite treba težiti uspostavljanju ravnotežnog stanja i između veličine rizika i ostvarenog nivoa zaštite koji može biti standardni, srednji, viši i najviši nivo, sagledavajući pritom i troškove.