TALLINNA ÜLIKOOL

Informaatika instituut

Kristo Kaul

IT riskide hindamise metoodika väikeettevõtetele

Magistritöö

Juhendaja: Peeter Normak, professor

Tallinn 2008

Autor : ……..”……” ……. 2008.a.

Juhendaja : ….……..”……” ……. 2008.a.

Instituudi direktor : …….....”……” ……. 2008.a.

Sisukord

Sissejuhatus

Infotehnoloogia jätkab tungimist kõikvõimalikesse eluvaldkondadesse. Üks valdkond, kus infotehnoloogial on olnud tavapäraselt suur roll, on ettevõtlus. Kuigi ka tänapäeval on kindlasti võimalik ettevõtlusega tegeleda infotehnoloogia pakutavaid võimalusi kasutamata, annab paljudel tegevusaladel infotehnoloogia kasutamine nii suure ajasäästu, et konkurentsis püsida ilma IT vahendeid kasutamata on väga raske. Nicholas Carr on oma tuntud artiklis "IT Doesn't Matter" öelnud: "Kui üks ressurss muutub oluliseks konkurentsis püsimiseks, mitte enam strateegia valikul, on ka sellega seotud riskid olulisemal kohal kui selle pakutavad eelised" (Carr, 2003). Infotehnoloogia kui ressursi osas toetab statistika Carr'i väidet. The Computing Technology Industry Association'i 2007. aasta veebruaris läbi viidud uuring näitab, et kulutused IT riskihaldusele suurenevad aasta-aastalt: kui 2005. aastal oli vastanute IT-eelarvest keskmiselt 15% suunatud turvalisusele, siis 2006. aastal juba 20% (CompTIA, 2007). Suurima osa sellest kasvust annavad kulutused kasutajate koolitamisele. Kui 2005. aastal moodustasid kasutajate turvateadlikkuse tõstmiseks kulutatud summad 8% IT eelarvest, siis 2006. aastal oli selle osakaal juba 12% (CompTIA, 2007). Need arvud näitavad, et IT turvet võetakse väga tõsiselt. Koos investeeringute kasvuga sellesse valdkonda tuleb aga aina paremini teadlik olla, kuhu investeeringuid täpsemalt suunata, et riskitase optimaalne hoida.

Käesolev töö keskendub riskide hindamisele, mis on riskihalduse üks tähtsamaid osi. Sellele toetuvad teised riskihalduse protsessid – turvameetmete rakendamine, monitooring, talitluspidevuse planeerimine jne.

Teema valik tulenes autori pikaajalisest kogemusest erinevate väikefirmade IT tugiisikuna. Väikefirmades tehakse palju otsuseid lennult – strateegiliseks planeerimiseks lihtsalt ei leita igapäevatöö kõrvalt aega. Riskijuhtimine on üks valdkond, kus ei ole tavaliselt üht õiget vastust. Seetõttu on IT riskide juhtimine olnud autori jaoks pikka aega üks ebakindluse allikaid.

Kirjandust leidub inglise keeles suuremate organisatsioonide riskihalduse kohta väga palju – on erinevaid standardeid, metoodikaid ja parimate praktikate kogumikke. Eestis on Jüri Kivimaa tutvustanud SEB riskihindamise metoodikat (Kivimaa, 2007), ning eestikeelsena on saadaval mitu asjassepuutuvat rahvusvahelist standardit. Ka kirjutatakse aeg-ajalt artikleid koduse arvuti kasutajatele, milliste ohtude eest ennast lihtsate meetoditega kaitsta saab. Samas väikeettevõtete kohta on kirjandust tunduvalt vähem. Tüüpilises väikeettevõttes on kohtvõrgus mitu töökohaarvutit, võibolla server raamatupidamisandmete jaoks ning avalik veebileht. Kodukasutajale mõeldud turvameetmed jäävad siin väheseks, samas suurfirma jaoks sobiv riskide haldus neelaks võibolla rohkem ressursse, kui need riskid ise väärt on. Sellest tulenevalt täiendab käesolev töö IT riskide alast kirjandust väga olulisest vaatepunktist.

Käesoleva töö uurimisküsimus on "Milline on väikeettevõttele sobiv riskide hindamise metoodika?". Selline ülesandepüstitus tähendab, et pole ka teada, millised on kriteeriumid, mille järgi sobivust hinnata. Töös püütaksegi leida kriteeriumid ning seejärel nende järgi leida olemasolev sobivaim või konstrueerida uus metoodika.

Töö esimeses peatükis antakse lühiülevaade ettevõtte riskihaldusest ning IT riskihalduse paigutumisest üldise riskihalduse raamistikku.

Teises peatükis antakse ülevaade valdkonna terminoloogiast ning IT riskihalduse tahkudest ja võimalikest lähenemisnurkadest. Erialasest kirjandusest vaadeldakse kaht rahvusvahelist IT riskihalduse standardit ning mitmeid antud valdkonnas läbiviidud uuringuid maailmas. Peatükk lõpeb üheksa töösse valitud riskide hindamise metoodika tutvustusega.

Kolmandas peatükis kirjeldatakse töö raames läbiviidud uuringut ning selle tulemusi. Tulemuste põhjal konstrueeritakse väikefirma vajadusi ja võimalusi arvesse võttes riskide hindamise metoodika struktuur, võttes aluseks eelpool vaadeldud metoodikad.

Töö uuringus kasutatakse andmete kogumiseks intervjuusid ning andmete analüüsiks põhistatud teooria meetodit. Põhistatud teooriat kui kvalitatiivset uurimismeetodit seostatakse põhiliselt sotsiaalteadustega, kuid meetod on edukalt rakendatav ka organisatsioonide uurimisel (Strauss, Corbin; 1990). Kvalitatiivse meetodi kasutamine

tulenes uurimisküsimuse püstitusest, mis ei sisalda ühtegi hüpoteesi. Pigem saab sellise probleemipüstituse lahenduseks olla kogumik hüpoteese.

Riskide hindamine on erinevates valdkondades traditsiooniliselt olnud kvantitatiivne. Lähtudes kirjandusest (Landoll, 2006; Elky, 2006), on IT riskihalduse puhul kvantitatiivse analüüsi läbiviimine suhteliselt keeruline, ning tihti annab kvalitatiivne riskide hindamine väiksema ajakuluga võrdväärse tulemuse.

Kirjanduse uurimine käesoleva töö temaatikaga tutvumiseks algas 2007. aasta algusest. 2008. aasta alguseks oli töö teoreetiline raamistik üldjoontes paigas, ning töös võrdlusse kaasatavad riskihindamise metoodikad välja valitud. Jaanuaris otsustati ka lõplik uurimismetoodika ning alustati intervjueeritavate otsimisega. Intervjuud toimusid jaanuarist märtsini, paralleelselt töö teoreetilise osa kirjutamise ning andmete analüüsiga. Aprillis 2008 formuleeriti uuringu tulemused ning vormistati töö.

Töö kirjutamise käigus esile kerkinud probleemidest oli suurim seotud uuringu andmete kogumisega. Esialgselt oli plaanis andmete kogumiseks kasutada ankeetküsitlust. Detsembris 2007 viidi läbi väike pilootküsitlus, kuid selle vastuste protsent oli nii madal, et otsustati ankeetküsitlusest loobuda ning kasutada andmete kogumiseks poolstruktureeritud intervjuusid. Üks madala vastuseprotsendi põhjustest võib olla asjaolu, et ei soovita uurimuse läbiviijaga isiklikult kohtumata avaldada informatsiooni aset leidnud turvaintsidentidest ja teadaolevatest turvaaukudest – usaldus on sellise temaatika puhul väga oluline.

Põhistatud teooria kasutamisel on oht, et autor “näeb” andmetes selliseid seaduspärasusi, mida ta tahab näha, või eeldab seal olevat. Võimalus on ka, et autor lihtsalt tõlgendab andmeid valesti. Autori isikliku kallutatuse vältimiseks ei võetud uuringusse ettevõtteid, millega autor viimase aasta jooksul seotud oli. Uuringu kvaliteedi tagamiseks järgis autor võimalikult täpselt klassikalist põhistatud teooria meetodit.

Samas, peaaegu kümneaastane töökogemus väikeettevõtete IT-probleemide lahendamisel annab autorile piisava “teoreetilise tundlikkuse” respondentide väljaöeldud mõtete tõlgendamisel.

Eetilisi probleeme õnnestus käesolevas töös vältida. Intervjuud põhinesid intervjueeritava ja intervjueerija vastastikusel usaldusel ning üks kokkuleppeid oli, et andmeid, mis võimaldaks töö lugejal ühe või teise konkreetse ettevõtte ära tunda, töös ei avaldata. Autori hinnangul see ka õnnestus, ilma et töö uuringutulemuste esitus selle all kannatab.

1. Ettevõtte riskihaldus

Käsitledes riskijuhtimist või riskihaldust, tuleb kõigepealt defineerida, mis on risk.

- Risk on võimalikkus, millega konkreetne oht kasutab ära nõrkused mingi vara kahjustamiseks ja seega otseselt või kaudselt organisatsiooni kahjustamiseks (ISO/IEC, 2004).
- Risk on ohtudest tulenevate kahjude statistiline mõõt, mida on kasulik teada objekti turvatarbe otsustamiseks ja turvameetmete valimiseks (Hanson et al., 1997).
- Risk on tõenäosus, et leiab aset kahju, "kaalutud muster võimalikest tulemitest ning nende tagajärgedest" (Munipalli, 2005).

Antud definitsioonide põhjal iseloomustab riski kaks tegurit: soovimatu intsidendi aset leidmise tõenäosus ja selle intsidendi toime. Need definitsioonid ei kata positiivset riski – võimalust, et leiab aset intsident, millel on organisatsioonile positiivne mõju. Ka käesoleva töö raames jäetakse positiivne risk vaatluse alt välja.

Ettevõtlust on ajast aega seostatud riski võtmise ning riskijuhtimisega. Riskid on mõnevõrra erinevad näiteks vabal turul konkureeriva firma ja monopoolse teenusepakkuja vahel, kuid efektiivne riskihaldus on igal juhul oluline aspekt pikaajaliselt edukate ettevõtete juhtimises.

Ettevõtte riskijuhtimine (ERM, Enterprise Risk Management) tähistab meetodeid ja protsesse riskide haldamiseks kooskõlas ettevõtte eesmärkide saavutamisega. Tüüpiliselt sisaldab see sündmuse või asjaolu identifitseerimist, selle aset leidmise tõenäosuse ning mõju hinnangut, millele järgneb meetmete või tegevuskava väljatöötamine ning rakendamine. Protsess on pidev, peale riskihalduse meetmete rakendamist hinnatakse jääkriski ning tsükkel kordub. Igale leitud ja analüüsitud riskile rakendatakse üht neljast strateegiast:

1) vältimine: riskitaset tõstvast tegevusest hoidumine

2) leevendamine: negatiivse sündmuse aset leidmise tõenäosuse või mõju vähendamine
3) jagamine: riski või osa sellest ülekandmine teisele osapoolele (tüüpiliselt kindlustamine)
4) aktsepteerimine: lähtuvalt kulu/tulu analüüsist ei rakendata täiendavaid meetmeid.

Riskianalüüsi tegematajätmist võib tinglikult sellesse nimekirja lisada kui "riski ignoreerimine" – tegutsemine, nagu oldaks riskivabas keskkonnas - mida vastavalt autori isiklikule kogemusele Eesti väikeettevõtetes sageli juhtub.

Kaks tähtsaimat ERM raamistikku on COSO ERM ja RIMS riskihalduse küpsusmudel. Esimene neist kirjeldab riskihalduse põhimõtteid vastavalt ettevõtte sise- ja väliskeskkonnale ning teine võimaldab ettevõtte riskihalduse taset formaalselt hinnata.

1.1 COSO – Enterprise Risk Management

2004. aastal COSO (Committee of Sponsoring Organizations of the Treadway Commission) tellimusel välja antud "Ettevõtte riskihalduse integreeritud raamistik" (Enterprise Risk Management - Integrated Framework) defineerib ettevõtte riskihaldust kui nõukogu, juhatuse ja muu töötajaskonna kaasabil toimuvat protsessi, mida kasutatakse strateegiate paikapanemisel ning kõigil ettevõtte juhtimistasemetel, identifitseerimaks potentsiaalseid sündmusi, mis võivad ettevõtet mõjutada ning haldamaks riske, et hoida neid riskivalmiduse piires, ja anda mõistuspärast kindlust ettevõtte eesmärkide saavutamiseks (Committee of Sponsoring Organizations of the Threadway Commission, 2004). COSO riskihalduse raamistikus on kaheksa riskihalduse komponenti, mida rakendades organisatsioon püüab nelja kategooriasse jaotatud eesmärke saavutada.

Komponendid on:

- Sisekeskkond
- Eesmärkide seadmine
- Sündmuste identifitseerimine
- Riskide hindamine

- Riskile vastamine, tegutsemine
- Kontrolltegevused
- Informatsioon ja kommunikatsioon
- Monitooring

Neli eesmärkide kategooriat on:

- Strateegia – organisatsiooni eesmärkidega kooskõlas olevad riskijuhtimise eesmärgid
- Tegevused – efektiivne ja säästlik ressursside kasutamine
- Finantsaruandlus – usaldusväärsus aruandluses
- Kooskõlalisus – kooskõla asjassepuutuvate seaduste ja regulatsioonidega (Committee of Sponsoring..., 2004)

Nagu ka definitsioonis on kirjas, seatakse loetletud eesmärke ja rakendatakse riskihalduse komponente kõigil ettevõtte juhtimistasemetel.

1.2 RIMS Risk Maturity Model for Enterprise Risk Management

Risk and Insurance Management Society (RIMS) on USA mittetulundusühing, mille eesmärgiks on riski ja kindlustuse juhtimise valdkonna arendamine. Ühingu väljaantav riskijuhtimise küpsusmudel defineerib ettevõtte riskihaldust kui kultuuri, protsesse ja vahendeid leidmaks strateegilisi võimalusi ja vähendamaks ebakindlust – seda nii strateegilisest kui operatsioonilisest perspektiivist. Küpsusmudel hindab seitsme atribuudi alusel kui hästi on riskijuhtimine ettevõtte juhtimisse ja põhitegevustesse integreeritud. Riskiküpsus leitakse nõrgima atribuudi järgi.

Seitse atribuuti on:

- **ERM-põhine juhtimine.** Kui tugev on tippjuhtkonna ning kogu töötajaskonna toetus ERM rakendamisele kõigis funktsioonides, protsessides, tegevusvaldkondades?
- **ERM protsessi juhtimine.** Kui tihedalt on ERM põimitud äriprotsessidesse?

- **Riskivalmiduse juhtimine.** Kui hästi kommunikeerib tippjuhtkond organisatsiooni riskivalmidust ning annab juhiseid otsuste tegemiseks?
- **Algpõhjuse distsipliin.** Kui põhjalikult käsitletakse iga probleemi algpõhjust ning sellega kaasnevaid sündmusi?
- **Riskide avastamine.** Millisel tasemel ja kui põhjalikult leitakse, hinnatakse ja dokumenteeritakse riske ja võimalusi?
- **Saavutuste juhtimine.** Kui edukas on organisatsiooni visiooni ja strateegia elluviimine erinevatest vaatevinklitest (finants, kasv, kliendipoolne vaade jne)?
- **Äri jätkusuutlikkus.** Kui tihedalt on ERM jätkusuutlikkusega seotud aspektid integreeritud planeerimistegevusse? Kas on olemas ka plaanid edasi tegutsemiseks väljaspool normaalseid äritingimusi? (Better Business Bureau, 2006)

RIMS veebilehel *http://www.rims.org/rmm* oleva küsimustiku abil on võimalik oma organisatsiooni riskijuhtimise küpsustaset hinnata. Tulemus antakse viie palli skaalas ning seda saab anonüümselt võrrelda kõigi seni küsimustiku täitnutega.

2. IT riskihaldus ettevõtte riskihalduse osana

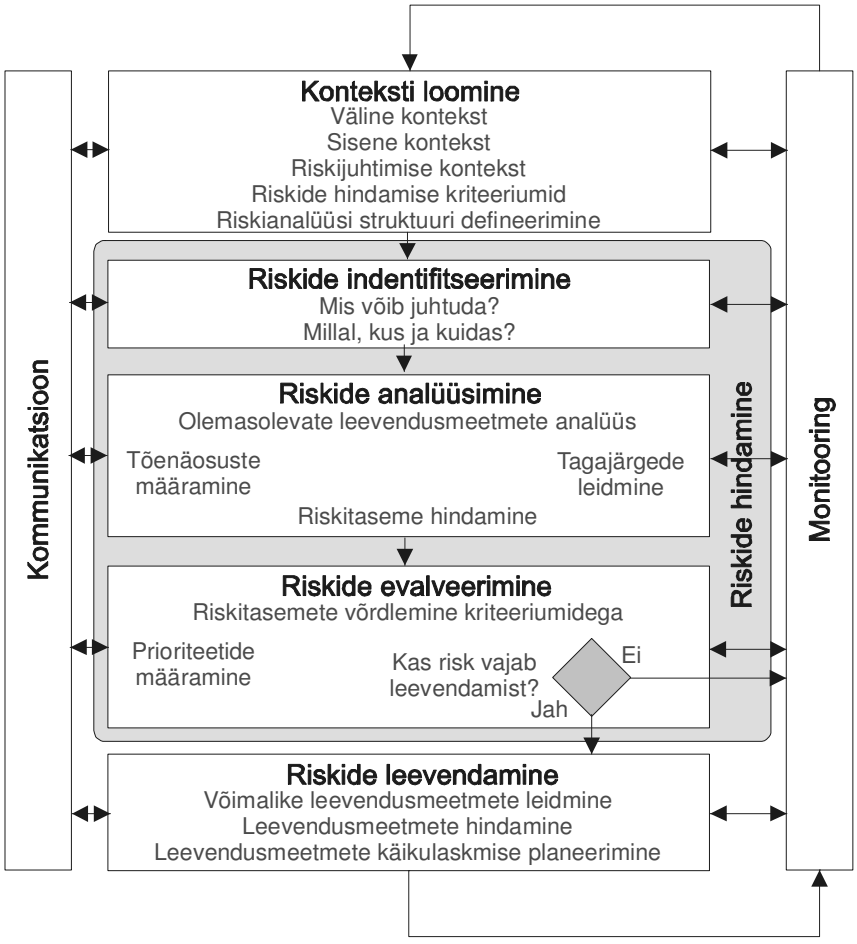
Ettevõtte riskid olenevad suurel määral tegevusalast. Siiski saab välja tuua põhilised riskide kategooriad. Uus-Meremaa New South Wales'i regionaalarengu ministeerium on koostanud riskide haldamise juhendi väikefirmadele. Selles on ära toodud põhilised riskide kategooriad, millega väiksemad ettevõtted tavaliselt silmitsi on:

Finants	Rahavood, eelarve ja omakapitali nõuded, kreeditoride ja deebitoride haldus.
Tootmisvahendid	Tootmiseks või teenuse osutamiseks vajalikud seadmed – kasutamine, korrashoid, sobivus, vananemine, uuendamine.
Organisatsioon	Inimestevahelised suhted, kultuurilised ja organisatsiooni struktuuriga seotud.
Füüsiline turve	Tootmisvahendite, varade ja inimressursi turve.
Juriidiline vastavus	Vastavus seadustele ja standarditele ning lepingutes ettenähtud tingimustele, samuti sotsiaalse keskkonna ootustele.
Reputatsioon	Oht organisatsiooni reputatsioonile organisatsiooni või mõne sellega seotud isiku tegevusest, toodete omadustest jne.
Tegevusrisk	Eduka toote/teenuse pakkumiseks vajalik planeerimine, tegevused ja ressursid ning toetavad protsessid.
Teenuse osutamine	Teenuse sobivus ja kvaliteet klientidele.
Kommerts	Riskid seoses turul positsioneerimisega, kasvuga ja toote edukusega.
Projektidega seotud	Projekti eelarve, vahendite, ressursside, tehnoloogia ja ajagraafikute haldus.
Tööohutus	Töötajate individuaalne ohutus, tööruumide ohutus, pakutavate toodete ja teenuste ohutus.
Huvigruppide haldus	Erinevate huvigruppide identifitseerimine ning nendega sobiva suhte loomine ja hoidmine.
Strateegiline	Ettevõtte jätkusuutliku tegevuse või kasvu planeerimine.

Tehnoloogiline Tehnoloogia kasutuselevõtt, haldus, korrashoid ja uuendamine (Turner, Keetelaar; 2005).

Sellest käsitlusest on IT riskihaldus eraldi punktina välja jäänud, kuid see on peidus mitmete teiste punktide eeldusena (nt. tootmisvahendid, tegevusrisk, tehnoloogiline, projektidega seotud). Tuleb aga silmas pidada, et IT valdkond on viimasel kümnendil läbi teinud tormilise arengu. Väga kiiresti on muutunud ohtude struktuur ning diapasoon. Märkamatult on ettevõtted saanud IT-st nii sõltuvaks, et intsident, mis mõned aastad tagasi oleks tähendanud vaid väikest ebamugavust, võib nüüd kaasa tuua kogu äritegevuse seiskumise.

Riskijuhtimine toimub üldjuhul igas loetletud valdkonnas sarnase loogika alusel. Skemaatiliselt võtab ühe valdkonna riskijuhtimise kokku joonis 1.



Joonis 1. Riskijuhtimise protsess ettevõttes (Turner, Keetelaar; 2005).

2.1 IT Riskihalduse mõiste

Aja jooksul on IT riskide valdkonna kirjanduses erinevaid mõisteid erinevalt kasutatud. Käesolevas töös juhindutakse eeskätt ISO standardist ISO/IEC 13335-1. See standard on tõlkemeetodil üle võetud ka Eesti standardiks.

Riskihaldus on protsess, mille raames leitakse, vähendatakse ning elimineeritakse juhuslikke sündmusi, mis võivad IKT ressursse mõjutada (ISO/IEC, 2004).

Tipton ja Krause on andnud arusaadava ja lihtsa jaotuse, millistest tegevustest IT riskihaldus koosneb:

- **Tööta välja IT riskihalduse poliitika**
- **Määra riskihalduse eest vastutaja ja anna volitused**
- **Tööta välja sobiv riskihalduse metoodika ja protseduurid**
- **Teosta riskide hindamine**
- **Tööta välja riski aktsepteeritavad tasemed**
- **Leevenda riske, mis ületavad aktsepteeritava taseme**
- **Monitoori riskihalduse protsessi toimivust** (Tipton, Krause; 2000)

IT riskihaldus hõlmab kolme komponenti: inimene, tehnoloogia ja protsess (Snedaker, 2006). National Security Agency (NSA) ja National Institute of Standards and Technology kasutavad veidi teistsugust terminoloogiat: inimese asemel juhtimine (management) ning protsessi asemel tegevus (operations), kuid mõista tuleks neid ühtviisi – terviklik IT riskihaldus keskendub inimesele (hooletus, teadmatus, kuritahtlikkus), tehnoloogiale (riist- ja tarkvara) ning protsessile (turvapoliitika ja protseduurid) (Snedaker, 2006). Nõrgim lüli neist on tavapäraselt inimesed. Haavatavuste nimekirjas on alati kõrgel kohal inimestega manipuleerimine (social engineering), madal teadlikkus ning pahatahtlikkus.

Tulenevalt sellest võib IT riskihaldust vaadelda kihilisena. Näiteks: turbe esimese liini moodustavad poliitika, protseduurid ja kasutajateadlikkus. See moodustab tugeva

aluse kogu andmeturbele, sest inimene ja protsess on turbe kaks põhikomponenti (Snedaker, 2006). Sellele järgneb füüsiline turve ning viimasena loogiline turve.

Riskihalduse taset näitab selle formaliseerimise aste, s.t. kui formaalne on lähenemine (Turner, Keetelaar; 2005). Kui kujutada formaliseerimist kolmeastmelisena, on astmed:

• Intuitiivne – mõttes ja suuliselt toimuv riskihaldusprotsess, kus kirjalikult midagi ei fikseerita. Sellise lähenemise eelis on kiirus - selle tõttu sobib see kriisisituatsioonidesse ja kiiresti muutuvatesse keskkondadesse. Kõige vähem ressursinõudlikuma lähenemisena sobib see ka näiteks kodu-arvutikasutajatele, kus suurim võimalik kahju pole piisavalt kõrge, et see nõuaks suuremat pühendumist.

• Planeeritud – kasutab mõnd samm-sammulist riskijuhtimise juhendit. Riskide haldus on süstemaatiline ning riskitase optimumi lähedal.

• Kalkuleeritud – kõige põhjalikum lähenemine riskijuhtimisele. Formuleeritud on turvapoliitikad ning protseduurid. Riskide hindamine toimub regulaarselt või mõne uue tehnoloogia kasutuselevõtuga. Kasutatakse erinevaid riskianalüüsi meetodeid, s.h. detailset riskianalüüsi. Andmeid kogutakse mitmetest erinevatest allikatest (küsitlus, vaatlus, eksperdid, testimine, dokumentatsioon). Olemasolevate turvameetmete efektiivsuse monitooring käib pidevalt.

2.2 Riskide hindamine ja riskianalüüs

Riskide hindamist (risk assessment) ja riskianalüüsi (risk analysis) kasutatakse sünonüümidena paljudes eesti- ja inglisekeelsetes allikates, k.a. Eesti Vabariigi ministeeriumide dokumendid. Siiski, ISO/IEC 13335-1 teeb neil selgesõnaliselt vahet:

- **Riskianalüüs** - süstemaatiline protsess riskitasemete leidmiseks.
- **Riskide hindamine** - protsess, mis kombineerib endas riskide identifitseerimise, riskianalüüsi ning evalveerimise (ISO/IEC, 2004).

Ka käesolevas töös kasutatakse neid mõisteid edaspidi selliselt. Sellises määratluses tähistab riskide hindamine riskihalduse osa, mille käigus leitakse riskidele väärtused. Protsess koosneb üldjuhul sammudest:

1) varade kindlaksmääramine
2) haavatavuste leidmine
3) ohtude kindlaksmääramine
4) ohu realiseerumise tõenäosuse ning tagajärje hindamine/leidmine ning
5) riski suuruse leidmine (riskianalüüs), kasutades selleks kaht komponenti, tõenäosust ning tagajärje kaalukust (Munipalli, 2005).

Erinevates allikates on riskianalüüs väga erinevalt defineeritud. Võrdlusena ISO/IEC 13335-1 määratlusele toome ära mõned IT riskianalüüsi definitsioonid erialasest kirjandusest:

- Riskianalüüs on võimalike riskide suuruse määramine, nõrkuste kindlakstegemine ning igale neist prioriteedi määramine (Gregg, Kim; 2005).

- Riskianalüüs on protsess, milles analüüsitakse uuritava objekti riskidega seotud omadusi ning nendevahelisi seoseid. Analüüsi käigus leitakse ohud ning erinevate varadega seostatud nõrkused, ebasoovitavate sündmuste tõenäosused ning mõju suurus ja iseloom. Seejärel leitakse võimalikud leevendusmeetmed ning hinnatakse nende otstarbekust erinevate kriteeriumide järgi (Tipton, Krause; 2000).

- Riskianalüüs on teadaolevate riskide uurimine, nende olulisuse määramine ja dokumenteerimine (Munipalli, 2005).

- Riskianalüüs on hetkel kasutuses olevate turvameetmete efektiivsuse analüüs ning organisatsiooni varadele mõjuda võiva kahju tõenäosuse leidmine (Landoll, 2006).

IT riskide alases kirjanduses on kasutatud riskianalüüsiks erinevaid indikaatoreid – ilmselt pole olemas üht ning parimat mudelit mis sobiks kõigile. Payson Hall pakub

välja kolme muutujaga riskimaatriksi - oodatav mõju, tõenäosus ning ootamatuse faktor - näiteks negatiivse sündmuse õigeaegse avastamise keerukus (Hall, 2003). Rex Black on kasutanud tagajärje "tõsidust" (severity), tõenäosust ja prioriteetsust (Black, 2002). Tõsidus erineb oodatavast mõjust selle poolest, et näitab tagajärje traagilisust, ohtu inimelule – eriti oluline on see indikaator meditsiiniga seotud süsteemide riskianalüüsil. Steve Goodwin kasutab oma artiklis " Tarkvara riskihaldus on hea äritava" riskianalüüsiks ainult tõsidust (Goodwin, 2000). Yamini Munipalli kombineerib aga kõige rohkem indikaatoreid riskimaatriksisse: tõenäosus, oodatav mõju, süsteemi keerukus, tõsidus. Keerukuse indikaatori kasutamine põhineb hüpoteesil, et mida keerulisem süsteem, seda rohkem on selles ka (avastamata) vigu. Tema töö (Munipalli, 2005) keskendub tarkvaraprojekti riskidele ning keerukuse indikaatorina kasutab McCabe välja töötatud tsüklomeetrilise keerukuse näidikut.

Eksisteerib rida sisult ja vormilt sarnaseid mõisteid, mis on ka siinkohal ära toodud. Siiski, ainult riskianalüüs identifitseerib nõrkused ja pakub soovituslikud vastumeetmed vastavalt hinnatud riskitasemetele.

Gap – analüüs on võrdlus olemasoleva olukorra (riskitaseme) ning soovitava olukorra vahel. Sel puhul on soovitav lõppresultaat väga täpselt paigas, näiteks mingile regulatsioonile vastamine.

Vastavusaudit on objektiivne ülevaade organisatsiooni vastavusest andmeturbe standarditele. See ei anna hinnangut riskitasemele organisatsiooni varade suhtes.

Turvaaudit on põhjalik ülevaade olemasolevatest turvameetmetest ning kontroll nende rakendamise efektiivsusest.

Eelnevas punktis esitatud riskihalduse formaliseerituse astmega on väga tihedalt seotud ka riskihindamise lähtepunkt. Intuitiivse riskihalduse puhul on ainuvõimalik alt-üles suunatud riskide hindamine, ning vastupidi – formaliseeritud riskihalduse puhul on ka riskide hindamise loogika vastupidine. Allpool on toodud kolm võimalikku lähenemist IT riskide hindamisele:

Ülalt alla lähenemine – selle eelduseks on korporatiivsed IT poliitikad, standardid, protseduurid ja juhendid. Baaskonfiguratsioonides on etalonturve juba ette nähtud. Kui selline IT turvaraamistik on paigas, on kõige otstarbekam alustada nõrkuste hindamisega just neist dokumentidest ning jätkata infrastruktuuri hindamisega vastavuses nende dokumentidega.

Alt üles lähenemine – kui organisatsioonis puuduvad kirjapandud poliitikad, standardid, protseduurid, viiakse läbi IT infrastruktuuri süstemaatiline nõrkuste hindamine ning IT turbe arhitektuur tuleneb ja töötatakse välja riskianalüüsi tulemustest.

Hübriid-lähenemine – mõnel juhul on organisatsioonil olemas formaalne IT turbe raamistik, kuid see pole täielikult rakendatud. Teisel puhul on olemas vaid mõned poliitikad, standardid ja protseduurid. Sellises olukorras on parim lahendus läbi töötada olemasolevad formaalsed materjalid ning samal ajal teha ka analüüs IT infrastruktuuris ja varades (Gregg, Kim; 2005).

2.3 Infoturve ja selle komponendid

Infoturve sisaldab endas kõik konfidentsiaalsuse, tervikluse ja käideldavuse määratlemise, saavutamise ja säilitamisega seotud aspektid. Infoturbe alamprotsessideks on IT riskihaldus, konfiguratsioonihaldus, muutuste haldus, talitluspidevuse plaanimine, turvateadlikkuse tõstmine jt. (ISO/IEC, 2004).

Nagu ISO/IEC definitsioonist näha, sisaldab infoturbe määratlus kolme eesmärki.

- **Käideldavus** on omadus olla volitatud olemi nõudmisel kättesaadav ja kasutuskõlblik; omadus väljendub nende andmete õigeaegses ja hõlpsas kättesaadavuses volitatud isikutele (ISO/IEC, 2004).

- **Andmeterviklus** on omadus, mis näitab, et andmeid ei ole volitamatul viisil muudetud ega hävitatud (ISO/IEC, 2004).

- **Konfidentsiaalsus** on omadus, mis näitab, et informatsioon ei ole tehtud kättesaadavaks volitamata isikuile, olemitele või protsessidele ega neile avalikustatud. (ISO/IEC, 2004)

Neid kolme eesmärki – terviklust, käideldavust ja konfidentsiaalsust – ei saa üksteisest päris lahutada. Nende määratlus ja lahendused võivad osaliselt kattuda. Mõnedes käsitlustes kasutatakse lisaks neile veel mõningaid andmete turvalisuse aspekte, nagu näiteks autentsus, jälitatavus, toimivus, usaldatavus, töökindlus jne. Samas on need siiski kõik kolme eelnimetatu kombinatsioonid või erinevad rõhuasetused.

Infoturbe temaatika sisaldab veel mitmeid üldisest riskijuhtimisest tuttavaid termineid, mille määratlust seoses IT valdkonnaga on kitsendatud. Käesoleva töö seisukohalt olulisimad on siinkohal ka ära toodud:

Turvapoliitika on kirja pandud reeglid, juhtnöörid ja praktikad infovarade haldamiseks, kaitsmiseks ning organisatsiooni sees ja IT süsteemide vahendusel jagamiseks (ISO/IEC, 2004).
Tähtsamad punktid, mida turvapoliitika hõlmab:

- Paroolide haldus
- Isikuandmete kaitse
- Kasutajarollide, privileegide haldus
- Regulaarsed turvaauditid
- Turvaintsidentidele reageerimise põhimõtted
- Kasutajate poolt oodatava ja vajatava teenustaseme kindlaksmääramine
- IT turbe seadmete, tarkvara, vahendite ostupõhimõtted
- Seadmetele füüsilise ligipääsu piiramine
- Turvapoliitika rikkumistest teatamine ja karistused
- Seadustest ja regulatsioonidest tulenevate nõuete täitmine
- Talitluspidevuse plaanid

(Tulloch, 2003)

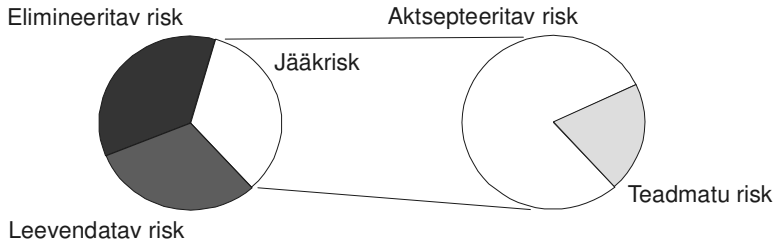
Infovara tähistab kõige üldisemas tähenduses infokogumit, mis on vajalik organisatsioonile oma tegevuseks. Näiteks klientide andmebaas, tööstusseadme programm mingi detaili tootmiseks jne. Üldiselt mõistetakse infovara all ka rakendustarkvara (Tipton, Krause; 2000). Mitmes käsitluses on infovarade mõiste laiendatud, mõistes selle nimetuse all ka ettevõtte jaoks väärtusliku informatsiooni nõuetekohast töötlemist tagavad seadmed, IT inimesed ning ainetud varad (maineväärtus). Käesolevas töös käsitletakse infovaradena andmeid ja infosüsteeme ning tarkvara. Infovara kasutamise eelduseks on riistvara ning IT infrastruktuur.

Oht on süsteemi või organsatsiooni kahjustada võiva soovimatu intsidendi potentsiaalne põhjus (ISO/IEC, 2004). Ohud võivad pärineda looduslikust või inimallikast ning olla juhuslikud (näit. vääramatu looduslik jõud, kulumine, inimlik eksitus) või sihilikud (lähtuvad inimesest, kellel on motivatsioon kahju tekitada). Sihilikke ohte saab omakorda liigitada passiivseteks (side, infokogumi jälgimine) ning aktiivseteks (info, oleku või talitluse muutmine). Ohuallika järgi eristatakse ka siseseid (süsteemi osad või legitiimsed kasutajad) ja väliseid ohte (süsteemivälised tegurid, volitamatud kasutajad) (Hanson et al., 1997).

Nõrkus on (info)vara nõrk koht, mille kaudu saab realiseeruda üks või mitu ohtu (ISO/IEC, 2004). Nõrkused jagunevad infrastruktuuri-, infotehnilisteks, personali- ja organisatsioonilisteks nõrkusteks (Hanson et al., 1997).

Turvameede on teoviis, protseduur või mehhanism riski vähendamiseks (ISO/IEC, 2004). See võib toimuda nõrkuste, ohtude või tagajärgede kaalukuse vähendamisena.

Jääkrisk on riskitase peale turvameetme(te) rakendamist (ISO/IEC, 2004). Sisaldab teadaolevat riski, mida on võimalik hinnata ning teadmatut riski. Ideaaljuhul, õigesti läbiviidud riskihindamise ja turvameetmete rakendamise korral võrdub jääkrisk aktsepteeritava riskiga. Aktsepteeritav riskitase on punktis, kus täiendavad leevendusmeetmed nõuavad rohkem ressursse kui oodatav kahju riski realiseerumisest (Hanson et al., 1997). Joonisel 2 on ära toodud riski komponendid.



Joonis 2. Riski komponendid (Federal Aviation..., 2005).

Käesolevas peatükis on põhiliselt vaatluse all olnud **tehniline risk**, mis ohustab infovarade konfidentsiaalsust, terviklust ning käideldavust. Lisaks sellele eksisteerib veel vähemalt kaks riskide kategooriat:

Äririsk eksisteerib juhul, kui protsessid ja süsteemid ei täida äripoole nõudeid (liiga kõrged kulud, väike produktiivsus, vähene lisaväärtus). Äripoole riske saab vähendada põhjaliku modelleerimise abil süsteemi disaini faasis ning käikulaskmise ajal.

Organisatsioonirisk tähistab olukorda, kus kasutajad keelduvad süsteemi planeeritud viisil kasutamast. Seda saab paljuski ära hoida, kaasates kasutajad süsteemi kasutuselevõtu protsessi ning näidates neile, milleks uued nõuded vajalikud on. Samuti on võimalik süsteemi sisse planeerida automaatsed kontrollimehhanismid, mis registreerivad iga väära kasutuse (Braunstein, 2003).

2.4 Ülevaade valdkonna erialakirjandusest

Käesolevas peatükis antakse ülevaade kahest tähtsamast rahvusvahelisest infoturbe standardist ning mõnedest teemaga haakuvatest uuringutest. Maailmas on välja töötatud palju IT riskihindamise metoodikaid. Need erinevad üksteisest formaliseerituse astme, põhjalikkuse, rõhuasetuse ning sihtgrupi poolest. Siin on ära toodud neist väike valik. Vaatamata metoodikate rohkusele on teaduslikke uuringuid selles valdkonnas läbi viidud väga vähe, võrreldes näiteks projektijuhtimise riskihalduse valdkonnaga. Tehakse statistikat erinevate turvaintsidentide aset leidmise kohta, kuid see on reeglina üldist laadi, hõlmates nii suuri kui väikeseid organisatsioone. Uuringute tegemist raskendab asjaolu, et paljud väiksemad

intsidendid jäävad tõenäoliselt avalikustamata või siis suisa märkamata, ning valdkonna kiire arengu tõttu pole ajaloolistest andmetest tihti kasu, kuna olukord muutub näiteks uut tüüpi viiruse või ründetaktika kiire leviku tõttu hüppeliselt.

2.4.1 IT riskihalduse standardid

ISO/IEC 13335 "Infotehnoloogia. Infoturbe halduse suunised"

Standardi eesmärk on anda suuniseid infoturbe halduse aspektide kohta, alustades mõistete struktuuri selgitamisest ja lõpetades konkreetsete rakendusjuhiste ning dokumendi näidisstruktuuridega. See standard on tõlkemeetodil üle võetud ka Eesti standardiks EVS-ISO/IEC 13335. Standard koosneb järgmistest osadest :

- ISO/IEC 13335-1 "Infoturbe mõisted ja mudelid"
- ISO/IEC 13335-2 "Infoturbe haldus ja plaanimine"
- ISO/IEC TR 13335-3 "Infoturbe halduse meetodid"
- ISO/IEC TR 13335-4 "Turvameetmete valimine"
- ISO/IEC TR 13335-5 "Võrguturbe halduse suunised"

Standardi esimene osa annab definitsioonid infoturbe valdkonnas kasutatavatest põhimõistetest ja mudelitest, järgmised osad kirjeldavad detailsemalt, kuidas neid mõisteid ja mudeleid saab asutuses tõhusalt kasutada. Standard on antud küllaltki tehniliselt ja konkreetseid suuniseid andes.

ISO/IEC 27002 "Infotehnoloogia. Infoturbe halduse praktilised juhised"

ISO/IEC 27002 sai oma praeguse nime juulis 2007, mil see nimetati ümber standardist ISO/IEC 17799. Standard on alguse saanud Briti standardina BS 7799 *British Standards Institute* poolt. Ka see standard on nime all EVS-ISO/IEC 17799:2003 tõlkemeetodil üle võetud Eesti standardiks. Standardis käsitletavad teemad on turvapoliitika, turvaorganisatsioon, varade klassifitseerimine ja juhtimine, personali turvalisus, füüsiline ja keskkonna turvalisus, arvutite ja võrgu ohjamine, süsteemi ligipääsu ohjamine, süsteemiarendus ja hooldus, organisatsiooni tegevuskavad (sealhulgas häire- ja kriisiolukorra puhul), vastavus seadusandluse ja lepingulistele nõuetele. Erinevus võrreldes standardiga ISO/IEC 13335 on suunatus

juhtkonnale – tehniliste küsimuste asemel keskendutakse juhtimisalastele küsimustele. Standard sisaldab ka riskide hindamise metoodikat. Kuna aga metoodika on väikeettevõtte seisukohast liiga keerukas ja põhjalik, jäetakse see käesolevas töös lähemalt käsitlemata. Standard ning selles sisalduv metoodika oli ka kaalumisel Eesti valitsusasutuste kohustusliku turbemetoodika väljatöötamisel aluseks võtta, kuid parema granulaarsuse ning lihtsamini rakendatava metoodika tõttu eelistati Saksa Infoturbeameti (BSI) metoodikat (Koppelmaa, 2004).

ISO/IEC 27000 standardite perekond on suunatud infoturbe juhtimisele ning hetkel aktiivselt arendatav. Hiljuti on ilmunud või lähiaastatel ilmumas mitmeid infoturbe eri tahke käsitlevaid standardeid.

2.4.2 Valdkonnas läbiviidud uuringud

Üks teemaga seonduv uuring on Virginia osariigis USA-s läbiviidud uuring „Infosüsteemide turbe probleemid ja lahendused väikefirmades" (Gupta, Hammond; 2003). Mastaabid on siin, tõsi küll, erinevad. Gupta ja Hammond defineerisid väike-keskmisteks ettevõteteks kõik, millel 10 kuni 499 töötajat. Suurem osa vastajatest olid siiski valimi alumises otsas ning võrreldavad käesolevas töös käsitletavate firmadega: 75%-l vastanutest oli personaalarvuteid firmas kuni 20 ning 81%-l oli töötajaid kuni 50.

Eelnevalt testitud ankeetküsitlus saadeti 1000 ettevõttesse, vastuste protsent oli 13,8. Madala vastuseprotsendi tõttu jääb mingil määral õhku küsimus, kas vastuseid ei laekunud pigem ettevõtetelt, millel IT turvalisus suhteliselt paremas seisus, ning vastamisest loobusid rohkem need, kelle jaoks oli teema problemaatiline.

Uuringust selgus, et kirjaliku turvapoliitika puudumine oli väga tihedalt seotud turvaintsidentide sagedusega. Teise tulemusena toodi välja, et ettevõtted usaldasid liigselt oma töötajaid. Kuigi kirjanduse põhjal on sisese ründe tõenäosus tunduvalt suurem kui välisel häkkerirünnakul, pidasid vastajad oma töötajatest tulenevat riski kõige väiksemaks. Paljudel väikefirmadel ei olnud vastamise hetkel märkimisväärse turvaintsidendi kogemust - see võis olla ka valdkonnale madala prioriteedi andmise

põhjuseks. Uuring tehti ajal, mil väga jõuliselt olid hakanud levima meiliviirused, ning 50,7% firmadest peeti viirusetõrjet kõige tähtsamaks arvutiturbe meetmeks. Uuringu tulemustena pakuti välja prioriteetsed valdkonnad, millele väikefirmades senisest rohkem tähelepanu pöörata: kasutajate koolitus, IT iga-aastane auditeerimine, firmasisesed juurdepääsukontrollid ning ettevaatus väliste konsultantide kasutamisel.

Spinellis, Kokolakis ja Gritzalis on läbi viinud teoreetilise uurimuse - hüpoteetilise väikefirma ning kodukontori IT riskide hindamise kasutades CRAMM riskide hindamise metoodikat (Spinellis, Kokolakis, Gritzalis; 1999). Käesoleva töö autor jääb antud uuringu suhtes kriitilisele seisukohale. Hüpoteetilised juhtumid olid esitatud liiga üldsõnaliselt - seega hinnangud riskidele olid suhteliselt meelevaldsed. Töö järelduseks oli, et väike- ja kodukontorite IT-riskid on nii kõrged, et neid polegi tüüpilise väikefirma võimuses vastuvõetavale tasemele tuua. CRAMM abil leiti hulgaliselt turvameetmeid, millele tähelepanu pöörata. Tähtsaimate turvameetmetena märgiti ära paroolihalduse tugevdamist, juurdepääsukontrolli tõhustamist, varundust ning turvapoliitika ning reeglite kirjapanekut.

Paljude firmade juhid arvavad ekslikult, et on end piisavalt IT riskide vastu kaitsnud. Computer Security Institute ja Föderaalse Juurdlusbüroo läbi viidud uuring tõsise turvaintsidendi üle elanud firmades näitas, et

- 98% kasutas viirusetõrjeprogramme
- 95%-l oli installeeritud tulemüür
- 90%-l oli kasutajanime- ja paroolipõhine juurdepääsukontroll
- 61% kasutas ründedetektorit (Intrusion Detection System)
- 42%-l firmadest oli infole juurdepääsuks vaja end digitaalselt autentida (Richardson, 2007).

Uus-Meremaa ettevõtetes läbiviidud riskide hindamise analüüs (Marsh, 2006) näitab, et kõikidest riskidest suurimaks peetakse väikestes ja keskmistes ettevõtetes personaliriski – s.t. oluliste töötajate üleminek konkurendi juurde või muusse sektorisse. Teise riskina on märgitud saamata jäänud tulu töötaja puudumise (haigestumise, vigastuse) tõttu.

Suuruselt kolmanda probleemina nähakse võimetust täita seaduses ettenähtud või lepingutega võetud kohustusi. Neljanda riskina nähakse andmete hävimist (tervikluse kadu) mis on otseselt infotehnoloogiaga seotud. Sageduselt viies risk on üldine liigsuur kahju õnnetustest, kuna puuduvad plaanid ja vahendid tegutsemiseks hädaolukorras (Tabel 1).

Mainimise sagedus	**Risk**
1.	Võtmetöötajate lahkumine (konkurendi juurde)
2.	Saamata jäänud tulu töötaja puudumise tõttu
3.	Võimetus täita regulatsioone ja lepingust tulenevaid kohustusi
4.	Andmete hävimine
5.	Kahju talitluspidevuse plaanide puudumisest

Tabel 1. Viis olulisimat riski väike-keskmistes ettevõtetes Uus-Meremaal (Marsh, 2006).

Igal aastal viib Computer Security Institute läbi IT riskihalduse alase uuringu USA firmade ja valitsusasutuste seas. 2007. aasta uuring on järjekorras juba kaheteistkümnes, välja saadeti 5000 küsimustikku ning vastuseid saadi 494 (Richardson, 2007). Uuringus on öeldud, et uuringu tulemuste põhjal ei saa teha järeldusi kogu riigi IT turbe olukorra kohta – esiteks on küsitletavad kuidagi CSI-ga seotud (liikmed, postiloendis, konverentsidel osalenud) – ning võib arvata, et IT turvalisuse probleemidest teadlikumad kui juhuslik IT spetsialist. Ning ka nende hulgas võib olla erinevus vastanute ja mittevastanute vahel. Uuringu tulemusi saab aga kasutada trendide leidmiseks, sest vastajate kogum on aastate jooksul suhteliselt vähe muutunud.

Üks huvipakkuv Richardsoni poolt ära märgitud fakt on, et kuigi kasutajateadlikkuse tõstmine on vaieldamatult kõikide turbe spetsialistide silmis üks tähtsamaid valdkondi, kulutavad peaaegu pooled vastanutest IT turbe eelarvest alla 1% kasutajateadlikkuse tõstmiseks (Richardson, 2007). Tabelis 2 on ära toodud kümme enamlevinumat turvaintsidenti, osakaal vastanutest näitab, mitmel protsendil vastanutest sellist tüüpi intsident vähemalt korra on aset leidnud.

Intsidendi tüüp	**Osakaal vastanutest**
Organisatsioonisisese kasutaja mitteõiguspärane võrgukasutus	59%
Viirusega nakatumine	52%
Sülearvuti või muu kantava seadme vargus	50%
Õngitsemine, kus vastaja organisatsiooni näidati saatjana	26%
IM programmi väärkasutus	25%
DoS rünne	25%
Autoriseerimata ligipääs andmetele	25%
Zombi-arvutid organisatsiooni võrgus	21%
Kliendiandmete vargus	17%
Juhtmeta kohtvõrgu väärkasutus	17%

Tabel 2. Kümme olulisemat turvaintsidendi tüüpi aastal 2007 (Richardson, 2007).

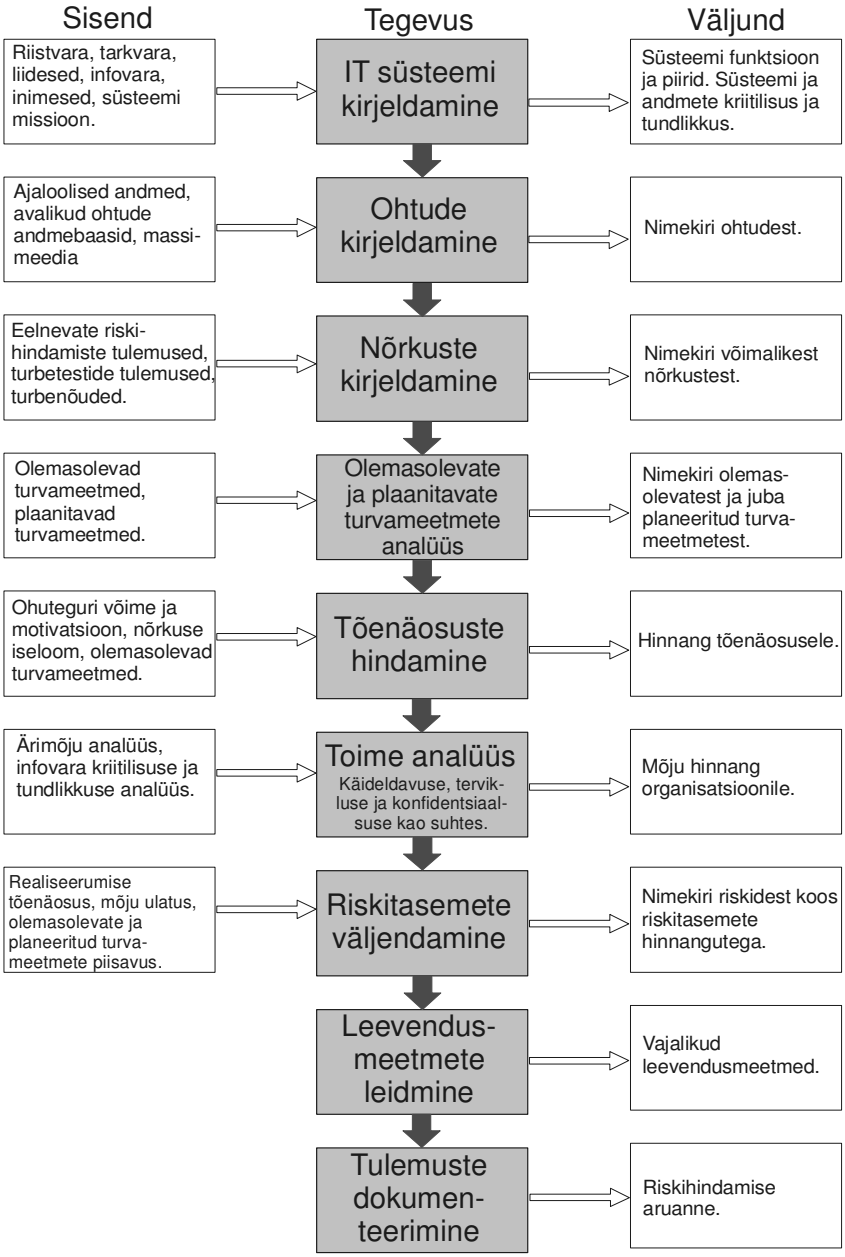
2.5 Riskihindamise metoodikad

Riskianalüüsi tüüpidena võiks eraldi rääkida kvalitatiivsest ja kvantitatiivsest analüüsist. Kuna kahjud ei ole alati materiaalsed, siis ei ole nad ka alati võrreldavates ühikutes väljatoodavad. Kvalitatiivse analüüsi puhul üritatakse leida kõigile turva-aspektidele ligikaudsed tasemehinnangud ning nende abil tuvastada riskantsemaid kohti süsteemis. Kvantitatiivse analüüsi puhul üritatakse kõiki aspekte kirjeldada samades ühikutes. Tavaliselt pole kvantitatiivse riskianalüüsi rakendamine IT valdkonnas õigustatud – töö hulk on suur ning väga keeruline on saada täpset ja täielikku statistilist informatsiooni (Landoll, 2006). Sellepärast jäetakse ka siin töös kvantitatiivsed meetodid vaatluse alt välja. Vaadeldakse üheksat riskide hindamise metoodikat, mis on kasutamiseks kõigile soovijatele ning ei ole valdkonnaspetsiifilised. Samuti on silmas peetud, et metoodika kirjelduses oleks öeldud, et see võiks sobida kasutamiseks äriettevõtetele, sealhulgas väikeettevõtetele.

2.5.1 NIST - Risk Management Guide for Information Technology Systems

USA Rahvuslik Standardite ja Tehnoloogia Instituut (National Institute of Standards and Technology, edaspidi NIST) on välja töötanud IT süsteemide riskihalduse juhendi (Risk Management Guide for Information Technology Systems) valitsusasutuste tarbeks, mis töötlevad tundlikku informatsiooni (Stoneburner, Goguen, Feringa; 2001). Juhendi sissejuhatuses mainitakse, et selle täitmine pole kohustuslik – tegu pole standardiga. Samas võivad seda kasutada kõik, ka eraõiguslikud organisatsioonid. Dokumendiga tutvudes üllatab lugejat lihtne ja ladus stiil, mis peaks olema arusaadav ka mitte-IT töötajale.

Juhend koosneb viiest osast: peale sissejuhatust antakse esimeses osas teemast ülevaade, paigutatakse IT riskihaldus üldisesse organisatsiooni tervikusse ning määratakse riskihaldusega seotud rollid. Teine osa kirjeldab riskianalüüsi metoodikat läbi üheksa sammu. Kolmandas osas on kirjeldatud riskide vähendamise strateegiat, turvameetmeid, tasuvusanalüüsi, kontrollmeetmeid, jääkriski. Viimases osas käsitletakse riskihalduse integreerimist ettevõtte muude protsessidega ja selle muutmist iteratiivseks. Metoodika üheksa sammu on esitatud joonisel 3.



Joonis 3. NIST IT riskide hindamise üheksa etappi.

Järgnevalt on sammud ka detailselt lahti kirjutatud:

1) IT süsteemi kirjeldamine

Riskihindamise läbiviija kogub esimese sammuna IT infrastruktuuri ja süsteemide erinevate tahkude kohta infot:

- Riistvara – tööjaamad, serverid, võrguseadmed, võrgu topoloogia, füüsiline turve, keskkonnatingimused (näiteks temperatuur ja õhuniiskus serveriruumis).
- Tarkvara – versioonihaldus, hooldus, konfiguratsioonide dokumenteerimine.

- Võrgu liidestatus – ühendused sise- ja välisvõrgu vahel.
- Andmed ja informatsioon – mis andmeid süsteemis hoitakse, kuidas andmed liiguvad ja kes neid töötleb, olemasolevad turvameetmed andmete hoidmisel.
- Süsteemi kasutajad ja hooldajad – inimesed. Kellel millist süsteemi osa oma tööks on vaja kasutada? Kasutajakontode loomise ja kustutamise põhimõtted, erinevate kasutajagruppide õigused, õiguste andmise põhimõtted. IT turbepoliitika, dokumenteeritud ja dokumenteerimata reeglid ja käitumismallid.
- IT-süsteemi(de) funktsioonid ehk protsessid, mis toimuvad süsteemi kaasabil. Neisse integreeritud tehnilised turbemeetmed.
- Süsteemide ärikriitilisus – nende väärtus ja/või vajalikkus organisatsioonile, äripoole nõuded tervikluse, käideldavuse ja konfidentsiaalsuse osas.

Andmete kogumiseks on mitmeid võimalusi, tervikpildi saamiseks ei saa tavaliselt piirduda ühega neist.

- Ankeetküsitlus kasutajate, juhtkonna, IT süsteemi hooldajate seas.
- Vabas vormis intervjuud võtmeisikutega ning kohapealne vaatlus.
- Tarkvaralised vahendid võrguaadresside ja teenuste leidmiseks.
- Dokumentidega tutvumine. Tarkvara ja riistvara manuaalid ning organisatsioonisisene dokumentatsioon, kui seda eksisteerib.

2) Ohtude kirjeldamine

Ohtude määratluseks on vajalik leida ning omavahel vastavusse viia kolm komponenti: ohuallikad, potentsiaalsed nõrkused ning olemasolevad turvameetmed. Ohuallikas on defineeritud kui mis iganes sündmus või asjaolu, millel on potentsiaal IT süsteemile kahju tekitada.

3) Nõrkuste kirjeldamine

Nõrkuste leidmise protsess sisaldab uuringut avalikes turvaaukude andmebaasides, sissetungi testide läbiviimist, konfiguratsioonide analüüsi, dokumentatsiooni läbivaatamist. Paljud neist sammudest on läbitud käesoleva metoodika esimeses etapis.

Selles etapis soovitavad metoodika autorid koostada ka turvanõuete nimekirja kolmest aspektist lähtudes:

- Nõuded juhtimisele
- IT ülalhoiu nõuded
- Tehnilised lahendused

4) Olemasolevate ja plaanitavate turvameetmete analüüs

Riski hindamiseks on oluline arvesse võtta olemasolevaid ja ka planeeritud turbemeetmeid. Eraldi pööratakse tähelepanu infotehnilistele meetmetele (tark- ja riistvaralised) ning organisatoorsetele meetmetele (poliitikad, pääsuõigused, füüsiline turve). Selles etapis on hea kasutada eelmises punktis koostatud turvanõuete nimekirja ning ära märkida lahknevused.

5) Tõenäosuste hindamine

Ebasoodsa sündmuse tõenäosuse leidmine põhineb eelmises punktis leitud nõrkustel. Arvesse võetakse nõrkuse iseloom, ohu tüüp, motivatsioon ja potentsiaal ning olemasolevate turvameetmete efektiivsus. Tõenäosuse hinnangu võib anda skaalal madal-keskmine-kõrge.

6) Toime analüüs

Et leida negatiivne kogumõju sündmusest kus oht realiseerub kasutades ära nõrkust, on vajalik teada:

- süsteemi missiooni (süsteemi poolt läbiviidavad protsessid)
- süsteemi ning selles sisalduvate andmete ärikriitilisust
- süsteemi ja selles sisalduvate andmete tundlikkust.

Need hinnangud saadakse tavaliselt intervjuu teel andmete omanikult. Mõju võib väljendada samuti kvalitatiivsel skaalal madal-keskmine-kõrge.

7) Riskitaseme väljendamine.

Risk väljendatakse iga oht-nõrkus paari kohta, võttes arvesse:

- ohu realiseerumise tõenäosust
- mõju organisatsioonile, kui oht realiseerub

- olemasolevate ja planeeritud turvameetmete efektiivsust, kusjuures turvameede võib vähendada nii tõenäosust kui ka mõju.

Riskide väljendus on tõenäosuse ja mõju korrutis. Tihti väljendatakse seda kahemõõtmelise tabelina.

8) Leevendusmeetmete leidmine

Selles punktis leitakse kõikvõimalikud leevendusmeetmed, mis mõnda leitud riskidest alandada võivad.

9) Tulemuste dokumenteerimine

Kui riskihindamine on läbitud ning võimalikud leevendusmeetmed leitud, vormistatakse kõik ametlikuks dokumendiks.

Sellele järgneb seitsmeks sammuks jagatud riskide leevendamise protsess, milles leitakse kuluefektiivsed lahendused, toomaks kõik IT-riskid vastuvõetavale tasemele.

NIST'i IT süsteemide riskihalduse juhendit on käsitlenud oma magistritöös ka Anne Parts, kes oma töös demonstreeris selle kasutamist väga edukalt ühe Eesti keskmise suurusega kaubandusettevõtte IT-riskide hindamisel (Parts, 2003).

2.5.2 An Introduction to Computer Security: The NIST Handbook

NIST on lisaks eeltoodule veel ühe riskihalduse teemalise publikatsiooni avaldanud. "Sissejuhatus arvutiturbesse" (An Introduction to Computer Security: The NIST Handbook) on välja antud käsiraamatu kujul. Erinevalt eelpool vaadeldud väljaandest ei rõhutata siin suunitlust valitsusasutustele, vaid "kõigile, kellel arvutiturbega kokkupuude". Käsiraamat annab tervikliku vaate IT riskide haldusele: käsitletakse turvapoliitikat, rolle, planeerimist, riskide hindamist ning dokumenteerimist. Eraldi peatükk on ka ohtude identifitseerimisele pühendatud. Raamatu lõpus on ära toodud terviklik näide riskihindamisest kujuteldavas organisatsioonis. Riskide hindamise metoodika erineb ülalmainitud väljaandest olulisel määral. Riskihindamise struktuur koosneb kolmest jaotusest ning neis sisalduvatest sammudest:

1) Riskihindamise skoobi ja metodoloogia määramine: formaalne/informaalne, detailne/lihtsustatud, kõrge/madalatasemeline, kvalitatiivne/kvantitatiivne, kombinatsioon nendest.
2) Andmete kogumine ja analüüs
    a) Varadele väärtuse määramine.
    b) Tagajärgede hindamine. Mis juhtub, kui (info)vara hävib, saab avalikuks, on mittekasutatav (pikaajalised tagajärjed kogu organisatsioonile).
    c) Ohtude identifitseerimine (eksitus, pahatahtlik rünne, tuli, vesi, viirus jne) ja analüüs (toimumise tõenäosus ja varade kahjustamise potentsiaal). Erilist tähelepanu tuleb pöörata aspektidele, mis pole hästi dokumenteeritud!
    d) Hetkel olemasolevate leevendusmeetmete analüüs.
    e) Nõrkuste analüüs – süsteemid, kus puuduvad adekvaatsed leevendusmeetmed.
    f) Tõenäosuste hindamine. Arvesse tuleb võtta ohu olemasolu ning turvameetmete olemasolu ja efektiivsuse. Statistiline info on tihti ebapiisav, eriti inimfaktori osas.
3) Kvantitatiivne või kvalitatiivne riskide analüüs: millised riskid on vastuvõetavad, millised riski/leevendusmeetmete paarid on parima hinna/efektiivsuse suhtega (National Institute of Standards and Technology, 1997).

2.5.3 CobiT

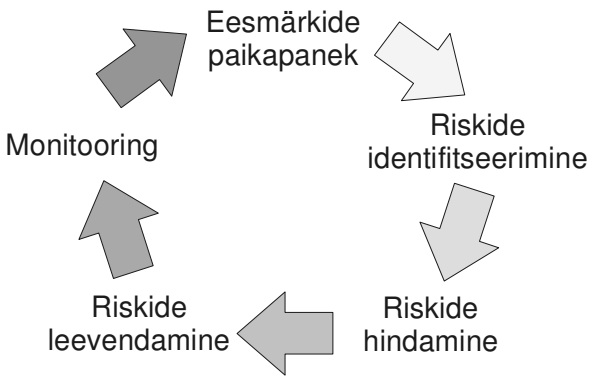
IT Governance Institute on alates 1996. aastast välja andnud ning pidevalt uuendanud dokumenti „Info- ja sellega seotud tehnoloogia kontrolli sihid" (CobiT - Control Objectives for Information and related Technology). See väljaanne on mõeldud täiendama COSO Sisekontrolli raamistikku (Internal Control—Integrated Framework). Üks viiest IT juhtimise fookuspunktist on ka riskihaldus. CobiT-i raamstruktuuri aluskontseptsioon on selles, et IT juhtimisele lähenetakse vaadeldes informatsiooni, mida vajatakse ärieesmärkide toetuseks (IT Governance Institute,

2007). COBIT-i raamstruktuuri on kasutanud Ivo Koppelmaa oma magistritöös (Koppelmaa, 2003), mille raames hindas ta ühe Eesti teenindusfirma IT juhtimise küpsustaset.

CobiT riskihaldus koosneb omakorda viiest sammust:

1) Eesmärkide paikapanek (IT eesmärkide kooskõla ärieesmärkidega lähtudes seitsmest kriteeriumist: efektiivsus, toimivus, konfidentsiaalsus, terviklus, kättesaadavus, vastavus regulatsioonidele, usaldusväärsus).
2) Riskide kindlaksmääramine, mis eelpool määratud eesmärkide saavutamist võivad mõjutada nii inimese, protsessi kui ka tehnoloogia vaatepunktidest (ohtude ja nõrkuste seostamine ning oht-nõrkus paaride seostamine võimalike negatiivsete mõjudega.)
3) Riskide hindamine (tõenäosus ja mõju ulatus nii turvameetmeteta kui ka hetke turvameetmeid arvestades – ehk leitakse hetke jääkrisk).
4) Riski leevendus (kui hetke jääkrisk on kõrgem kui vastuvõetav).
5) Monitooring, et kõik sammud toimiksid pidevalt ka kooskõlas (IT Governance Institute, 2007).

Skemaatiliselt on protsess näidatud joonisel 4.



Joonis 4. CobiT riskihalduse protsessi viis sammu.

2.5.4 I-ADD

Lihtsa ja laialdaselt rakendatava riskide hindamise metoodika I-ADD autorid, Swaminatha ja Elden demonstreerisid selle kasutamist oma raamatus traadita võrkude

turbe halduseks. Metoodika nimi tuleneb sammude inglisekeelsete nimetuste esitähtedest:

1) Identify – identifitseeri eesmärgid ja rollid
2) Analyze – analüüsi võimalikke ründestsenaariume ja nõrkusi (genereerimaks turbelahendusi ja riski leevendavaid meetmeid)
3) Define – defineeri turbestrateegia (raamistik kompromisside tegemiseks turbe/funktsionaalsuse/hinna/organisatsiooni eesmärkide suhtes).
4) Design – projekteeri turvalisus süsteemidesse ja protsessidesse sisse juba algusest (Swaminatha, Elden; 2002).

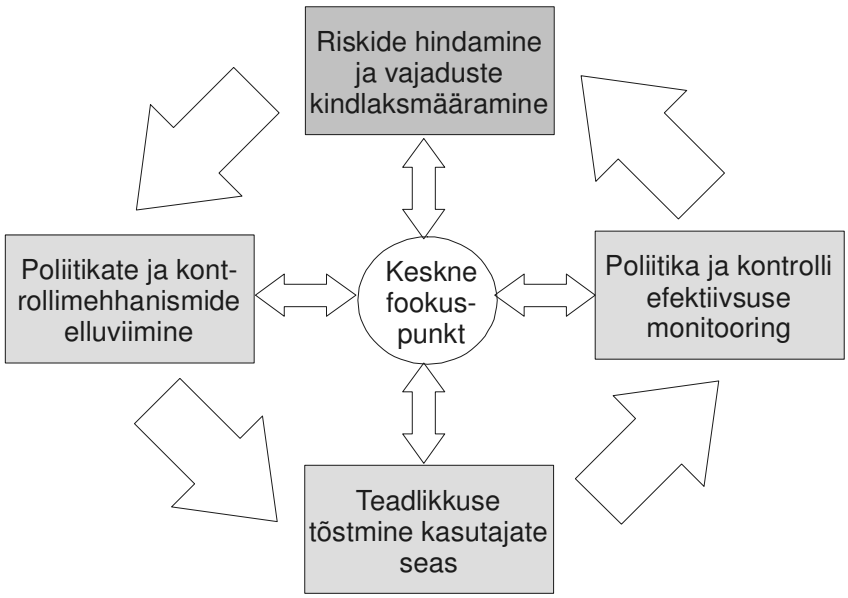
I-ADD riskianalüüsi protsess on iteratiivne ja rekursiivne – seda võib rakendada mistahes tasemel. See võimaldab antud lähenemist kasutades läbida ka projekti, mida muul juhul oleks oma keerukuse tõttu peaaegu võimatu edukalt sooritada (Swaminatha, Elden; 2002). Protsess on kirjeldatud suhteliselt üldsõnaliselt ning jätab riskide hindajale vabad käed konkreetsete meetodite kasutamisel. Seega sõltub tulemus suuremal määral läbiviijast, kui oleks täpsete juhistega metoodika kasutamisel. Riskide hindajal peavad IT turbe alal olema väga head teadmised, et genereerida võimalikult palju võimalikke ründestsenaariume.

2.5.5 GAO - Information Security Risk Assessment

USA kongressi juures tegutsev kontrolli- ja auditiorganisatsioon Government Accountability Office, endise nimega General Accounting Office (GAO), on 1999. aastal välja andnud IT riskihindamise juhendi, kus on analüüsitud nelja erineva erafirma riskide hindamise protsesse. Neid omavahel kõrvutades on välja pakutud eeskätt USA valitsusasutustes kasutamiseks, kuid on ka mujal rakendatav, suhteliselt detailne riskide hindamise metoodika. GAO käsitluses on riskihindamine üks riskijuhtimise protsessidest, teised IT riskijuhtimise protsessid on:

- Eesmärkide ja fookuspunkti paikapanek
- Poliitikate ja kontrollimehhanismide elluviimine
- Teadlikkuse tõstmine kasutajate seas
- Poliitika ja kontrolli efektiivsuse monitooring

Joonisel 5 on näidatud riskijuhtimise protsesside omavahelised seosed.



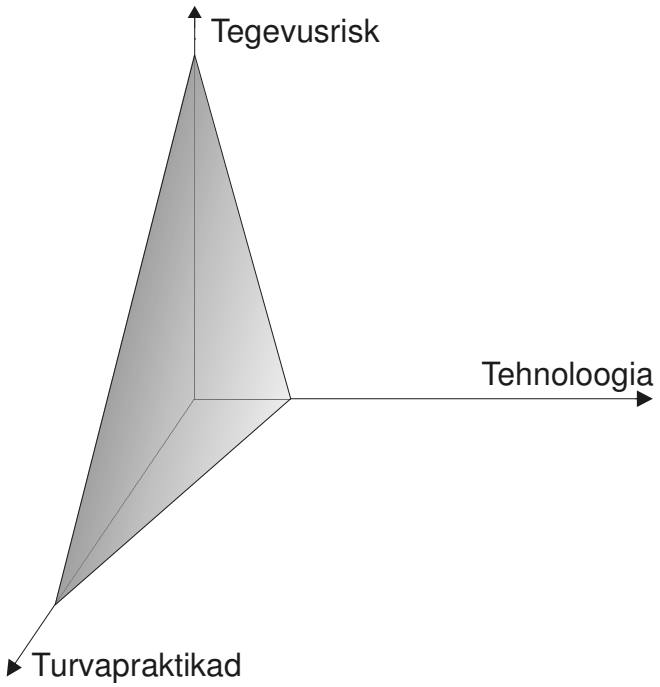
Joonis 5. IT riskijuhtimise protsesside omavahelised seosed (United States General Accounting Office, 2005).

Riskide hindamine koosneb kuuest etapist:

1) Ohtude kindlaksmääramine, mis võivad kriitilisi varasid või protsesse mõjutada.
2) Ohtude realiseerumise tõenäosuse hindamine (statistilise info põhjal ning eksperthinnanguid kasutades).
3) Varade väärtuse ja nõrkuste (ohtudele avatuse) määramine.
4) Kahju hindamine organisatsiooni jaoks kriitilisematele varadele (ning samuti kõige kaitsetumatele, ohtudele avatumate varadele), kui mõni esimeses punktis kindlaksmääratud risk peaks realiseeruma.
5) Kuluefektiivsete meetmete leidmine riskide leevendamiseks. Meetmed võivad olla nii organisatoorsed kui tehnilised.
6) Tulemuste dokumenteerimine ja plaanide paikapanek edasiseks.

2.5.6 OCTAVE-S

OCTAVE-S nimi väljendab ärikriitiliste varade, ohtude ja nõrkuste hindamist (Operationally Critical Threat, Asset and Vulnerability Evaluation) ning täht S lühendi lõpus viitab väiksusele – small. Metoodika on välja töötatud Carnegie-Mellon Software Engineering Institute poolt kasutades suurfirmadele mõeldud riskihindamise metoodika OCTAVE lähenemist, kohandades seda väiksematele organisatsioonidele (Alberts et al., 2005). Metoodika eessõnas on mainitud sobivust eelkõige 20-80 töötajaga organisatsioonidele. Tähelepanu on ka pööratud sellele, et sellise suurusega organisatsioonid ostavad IT-teenust tihti sisse ning organisatsioonis sees puudub ekspertteadmine süsteemide turbest. Sellises organisatsioonis võib riskihindamist läbi viiv meeskond vaatluse alla võtta tehnoloogiliste nõrkuste asemel protsessid, kuidas turvaliselt süsteeme käivitatakse, konfigureeritakse, ülal hoitakse ning asendatakse. OCTAVE-S lähenemise kaks põhilist alust on tegevusrisk ja turvapraktikad (Alberts et al., 2005). Tehnoloogia osa riskihalduses on meelega hoitud väike, viidates sellele ainult seoses turvapraktikatega (Joonis 6).



Joonis 6. OCTAVE-S fokusseeritus turvapraktikatele ja tegevusriskile (Alberts et al., 2005).

Käesoleva töö skoobist lähtudes on metoodika selgelt liiga detailne ning aeganõudev, kuid siinkohal on see vaatluse alla võetud just rõhuasetuse pärast mitte tehnoloogiale

(nagu mitmed teised selles peatükis vaadeldud metoodikad) vaid just protsessidele ning praktikatele.

Metodoloogia koosneb kolmest põhilisest faasist:

1) Koosta varadel põhinevad ohtude profiilid
2) Leia nõrkused infrastruktuuris
3) Loo turvastrateegia ja tegevusplaan

Esimeses faasis defineerib analüüsi läbiviija hindamiskriteeriumid. Analüüsija leiab organisatsiooni väärtuslikud varad ja hindab olemasolevaid turvapraktikaid. Kolme kuni viit ärikriitilist vara analüüsitakse sügavuti, vastavalt suhtelisele väärtusele organisatsiooni jaoks. Lõpuks defineeritakse nõutav turvatase ning ohtude profiil igale varale.

Teises faasis viiakse läbi arvutiinfrastruktuuri uuring fookusega küsimusele, kui ulatuslikult peab turvalisust silmas infrastruktuuri ülalhoiuga tegelev osapool ja ka teised osapooled. Nõrkusi otsitakse eelkõige protsessides ja praktikates, mitte tehnoloogias.

Kolmandas faasis leitakse kahe eelneva faasi tulemuste põhjal organisatsiooni varadele mõjuvad riskid ning otsustatakse edasine turvastrateegia ning konkreetsed plaanid riskide vähendamiseks (Alberts et al., 2005).

Iga faas sisaldab hulga tegevusi, mis on kõik detailselt kirjeldatud. Abimaterjalidena on antud kõikide täidetavate tabelite vormid.

2.5.7 Amanda Andress - Surviving Security

Amanda Andress on tuntud USA andmeturbe ekspert. Oma raamatus „Surviving Security – How to Integrate People, Process and Technology" pakub ta välja omapoolse variandi riskihindamisest. Protsess koosneb kuuest sammust, millest igaüks omakorda on jaotatud üheks kuni kolmeks tegevuseks.

1) Inventuur, defineerimine ja nõuded

a) Identifitseeri kriitilised äriprotsessid

b) Loo nimekiri varadest, mida need kriitilised protsessid kasutavad

c) Määra neile varadele väärtus või suhteline "tähtsus"

2) Haavatavuste ja ohtude hindamine

a) Kasuta automaatseid skaneerimisvahendeid turvaaukude leidmiseks

b) Vii nõrkuste analüüs lõpule käsitsianalüüsiga

c) Olemasolevate leevendusmeetmete hindamine

3) Leevendusmeetmete leidmine

Vii läbi ajurünnak võimalike leevendusmeetmete ning nendega seotud kulutuste kohta.

4) Analüüs, otsus ja dokumentatsioon

a) Analüüsi kõiki võimalikke leevendusvariante iga ohu jaoks

b) Otsusta, kas ja millist leevendusvarianti kasutada

c) Dokumenteeri hindamisprotsess ning tulemused.

5) Kommunikatsioon

Anna tulemustest teada kõigile asjassepuutuvatele osapooltele

6) Monitooring

Analüüsi pidevalt uusi ohtusid ning muuda vastavalt leevendusmeetmeid. Olulised muudatused organisatsioonis või IT infrastruktuuris eeldavad riskianalüüsi uut läbiviimist (Andress, 2004).

2.5.8 FRAP

Facilitated Risk Assessment Process (FRAP) ehk Lihtsustatud riskihindamise protsess on välja töötatud Thomas Peltieri poolt rõhuasetusega kuluefektiivsusel. See protsess sisaldab kaheosalist riskianalüüsi – informaalse eelanalüüsi käigus leitakse kõrge prioriteediga süsteemid ja infovarad ning neis valdkondades viiakse läbi detailne riskianalüüs. See võimaldab kontsentreerida aega ja ressursse sinna, kus neid kõige rohkem vaja on.

FRAP riskianalüüs koosneb kuuest sammust.

1) Esimese tegevusena viiakse läbi jäme IT riskianalüüs kogu organisatsiooni lõikes, et identifitseerida kõrge prioriteediga süsteemid, rakendused ja äriprotsessi segmendid, mis vajavad detailset riskianalüüsi.
2) Eelnevas punktis leitud alad võetakse ükshaaval ette ning ajurünnaku käigus leitakse võimalikud ohud, nõrkused ning negatiivsed mõjud.
3) Ärimõju analüüsi rakendades leitakse mõju äri põhiprotsessidele.
4) Riskid prioritiseeritakse.
5) Riskidele leitakse võimalikud leevendusmeetmed.
6) Rakendatavad leevendusmeetmed otsustab ärijuht. Vormistatakse tegevusplaan meetmete rakendamiseks (Peltier, 2003).

2.5.9 Steve Elky - Infosüsteemi riskihaldus

Steve Elky loodud riskide hindamise süsteem on väga lihtne ning jätab kõrvale mitmed sammud, mis eelpool vaadeldud metoodikates sisalduvad. See toob kaasa kitsendusi, kuid muudab metoodika väga atraktiivseks just väikefirmadele, kus pole võimalust palju aega ja ressursse riskide hindamisele kulutada. Näiteks puudub metoodikas eraldi punktina infovarade ja nende väärtuste leidmine. Eeldatakse, et see info on riskihindamise läbiviijal teada. Protsess koosneb kuuest etapist.

1) Loetle ohud süstemaatiliselt, ohuallika järgi.
2) Leia nõrkused süsteemides, protseduurides, poliitikates. Nii ohtude kui nõrkuste leidmiseks soovitatakse kasutada avalikke ohtude ja nõrkuste andmebaase.
3) Seosta ohud ja nõrkused. Tulemuseks peaks olema ohu-nõrkuse paarid iga infovara ja infrastruktuuri osa kohta. IT turbega seotud veebilehtedelt on võimalik leida standardseid ohu-nõrkuse paaride nimekirju. Nendesse tuleb aga ettevaatusega suhtuda, sest ohtusid tekib aja jooksul juurde ning avastatakse uusi nõrkusi.
4) Määra tõenäosused, et ohu-nõrkuse paari tagajärjel leiab aset soovimatu intsident. Elky pakub välja tõenäosuste skaala, kus tõenäosus sündmuse toimumisele ühe aasta jooksul 0...0,25 vastab tasemele "madal"; 0,26...0,75 tasemele "keskmine" ning 0,76...1 tasemele "kõrge" (Elky, 2006). Sellisel jaotusel on omad eelised – kõrgeks hinnatud tõenäosusi on vähe, mis võimaldab neile paremini keskenduda, ning vähem

on riske, mis madala tõenäosuse hinnangu tõttu jäetakse riskide leevenduse plaanist välja. Samas, kui vaid mõni üksik hinnang väljapoole keskmist taset jääb, on ilmselt otstarbekam kasutada lineaarset skaalat (madal 0...0,33; keskmine 0,34...0,66; kõrge 0,67...1). Tähtis on siiski peale sobiva skaala leidmist selle juurde jääda, et järgnevad riskihindamised oleksid omavahel võrreldavad.

5) Defineeri mõju organisatsioonile. Üheselt mõistetava raamistiku kindlustamiseks on üks võimalus mõju hinnata läbi kolme andmeturbe komponendi: tervikluse, käideldavuse ja konfidentsiaalsuse (Tabel 3).

	Terviklus	**Käideldavus**	**Konfidentsiaalsus**
Madal	Tervikluse kadu tekitab mõningast kahju.	Käideldavuse kadu tekitab mõningast kahju.	Konfidentsiaalsuse kadu tekitab mõningast kahju.
Keskmine	Tervikluse kadu tekitab olulist kahju.	Käideldavuse kadu tekitab olulist kahju.	Konfidentsiaalsuse kadu tekitab olulist kahju.
Kõrge	Tervikluse kadu tekitab ränka kahju.	Käideldavuse kadu tekitab ränka kahju.	Konfidentsiaalsuse kadu tekitab ränka kahju.

Tabel 3. Intsidendi mõju hindamine läbi kolme andmeturbe komponendi.

Eelnevas tabelis kasutatud mõisted “mõningane kahju”, “oluline kahju” ja “ränk kahju” saab iga organisatsioon enda jaoks ise defineerida. Tabelis 4 on näitena toodud Elky pakutud määratlused.

Mõju tüüp	**Mõju missiooni täitmisele**	**Rahaline kahju**	**Mõju inimelule**
Mõningane kahju	Vähetähtsa(te) funktsiooni(de) ajutine kadu	alla $5000	Kerged vigastused
Oluline kahju	Ühe või mitme vähetähtsa funktsiooni pikaajaline kadu	$5000 kuni $ 100 000	Keskmised vigastused, kuid mitte eluohtlikud
Ränk kahju	Ühe või enama põhifunktsiooni pikaajaline kadu	üle $100 000	Eluohtlikud vigastused või surm

Tabel 4. Kahju suuruse määramine lähtuvalt erinevatest aspektidest.

Tulpade arv ja sisu olenevad siin konkreetsest organisatsioonist. Ilmselt paljude väikeettevõtete jaoks on "Mõju inimelule" IT süsteemide seisukohast ebaoluline, kui just pole tegemist tervishoiuasutusega või elektrooniliselt juhitavaid tööstuslikke protsesse kasutava firmaga. Samas võib tulpasid vastavalt vajadusele juurde teha (näiteks mõju ettevõtte mainele).

6) Riskimaatriksi koostamine

Riskihindamise viimane etapp on paigutada riskid vastavalt oma mõjule ja realiseerumise tõenäosustele lihtsasse tabelisse (Tabel 5). Tulemuseks on nimekiri riskidest (ohu-nõrkuse paaridest) koos hinnanguga - kõrge, keskmine või madal.

		Mõju		
		Kõrge	**Keskmine**	**Madal**
Tõenäosus	**Kõrge**	**Kõrge**	**Kõrge**	**Keskmine**
	Keskmine	**Kõrge**	**Keskmine**	**Madal**
	Madal	**Keskmine**	**Madal**	**Madal**

Tabel 5. Riski hindamine tõenäosuse ja mõju alusel.

Erinevalt mitmetest eelpool käsitletud metoodikatest jätab Elky riskide hindamise definitsioonist välja olemasolevate turvameetmete analüüsi ning riskide leevendamiseks välja pakutavate meetmete leidmise. See võimaldab protsessi paljuski lihtsustada – hinnang nõrkusele antakse arvestades olemasolevaid turvameetmeid ning uue strateegia valik (uute turvameetmete väljavalimine vastavalt hinnale ja efektiivsusele) toimub juba vastavalt riskimaatriksile. See vähendab töö hulka, kuna kuluefektiivsete turvameetmete leidmiseks võetakse vaatluse alla esmajoones vaid kõrged riskid, ning seejärel keskmised. Selle lähenemise puudus on asjaolus, et näiteks kui mõnd keskmist riski on võimalik alandada ilma igasuguse rahalise kuluta, jääb see esialgu vaatluse alt välja, kuna tegeldakse kõrgete riskidega.

2.5.10 ISKE

Infosüsteemide kolmeastmeline etalonturbe süsteem (ISKE) töötati välja AS Cybernetica poolt Eesti Vabariigi Majandus- ja Kommunikatsiooniministeeriumi tellimusel. Metoodika põhineb Saksa Riikliku Infoturbeameti (BSI) etalonturbe süsteemil. Antud süsteem on väga detailne ning varustatud põhjaliku rakendusmetoodikaga. Metoodika on aegasäästev, sest puudub vajadus läbi viia riskianalüüs – see sisaldub juba metoodikas, tuginedes BSI pikaajalistele kogemustele Saksamaa riigiasutuste infoturbe alal. Samas, süsteem eeldab, et selle rakendajal on tüüpilised IT süsteemid, mida ähvardavad tüüpilised ohud ja nõrkused. BSI süsteemi on ISKE loomiseks aga edasi arendatud, tuues sisse kolm astet – lisaks keskmisele ka keskmisest väiksema või suurema turvavajadusega süsteemide tarbeks. 2007. aastal avaldatud versioon 3.0 on sisuliselt metoodika esimene praktikas rakendatav versioon. Siiski võib arvestada veel mitme aastaga, enne kui metoodika praktilise rakendamise käigus adekvaatselt Eesti riigiasutuse vajadustele vastama hakkab. Metoodika kriitikud on sellele ette heitnud vähest astmete arvu – rakendamine ei oleks keerulisem, kui astmeid oleks neli või viis, samas annab see suuremad võimalused turvanõuete diferentseerimiseks.

Metoodika koosneb viiest sammust:

1) Organisatsiooni infovaradest ning IT riistvarast ja infrastruktuurist nimekirja koostamine ning klassifitseerimine

2) Infovarade omanik määrab andmekogudele, rakendustele ja süsteemidele turvaklassid. Turvaklassid koosnevad neljast osaklassist – terviklus, konfidentsiaalsus, hilinemise kaalukus, aegkriitilise teabe käideldavus. Turvaklassist tuleneb nõutav turbeaste – madal, keskmine või kõrge.
3) Infovarade turbeaste kantakse üle ka riistvarale, infrastruktuurile ja ruumidele, mis nendega kokku puutuvad.
4) Igale varale leitakse vastavalt selle turbeastmele meetmete kataloogidest rakendamisele kuuluvad turvameetmed. Hinnatakse, millised meetmed on juba rakendatud või mille rakendamise vajadust pole, kuna risk on maandatud juba teiste vahenditega.
5) Rakendamist ootavate meetmete nimekirja põhjal koostatakse tööplaan vastavalt neile määratud prioriteetidele.

ISKE esimene versioon oli ühe metoodikana vaatluse all ka Anne Partsi magistritöös (Parts, 2003). Üks järeldusi antud töös oli, et kuigi ohud ja turvameetmed on väga paljuski riigiametil ja erafirmal sarnased, ei õnnestunud ISKE metoodikat erafirma tarbeks kasutada, kuna turvaklassid on riiklikul institutsioonil ja erafirmal väga erinevad.

3. Uuring

Käesolevas töös esitatakse küsimus - milline peaks olema IT riskide hindamise metoodika või raamistik, mis sobiks võimalikult paljudele Eesti väikefirmadele? Et sellisele küsimusele vastata, on kõigepealt vaja teada kriteeriume, mille järgi olemasolevate metoodikate sobivust hinnata, või siis uut metoodikat formuleerida. Kriteeriumide leidmiseks viidi käesoleva magistritöö raames läbi uuring firmajuhtide seas. Uuriti väikeettevõtete vajadusi seoses IT riskide hindamise ja haldamisega ning hinnati kitsendusi, mis riskide hindamise protsessis erinevates firmades ette võivad tulla.

3.1 Uuringu skoop

Kuna töö pealkirjas on sõna „väikeettevõtted", siis defineerime, mis see väikeettevõte on. Ettevõtted jaotatakse Eesti kontekstis tavaliselt töötajate arvu järgi järgmistesse gruppidesse (Siimon, 2001):

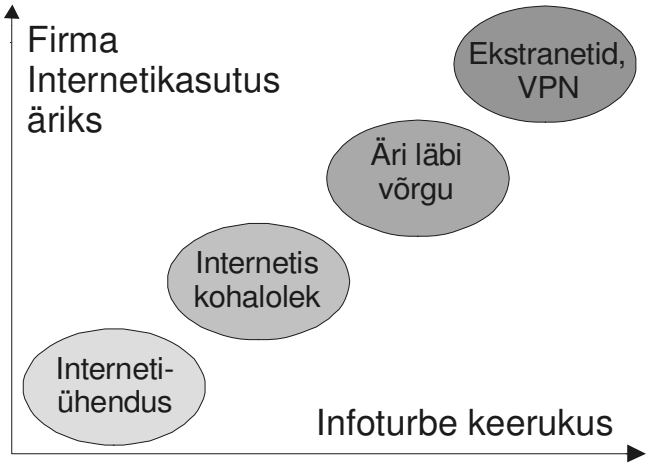
mikroettevõte	0 kuni 9 töötajat;
väikeettevõte	10 kuni 49 töötajat;
keskmine ettevõte	50 kuni 249 töötajat;
suurettevõte	250 ja enam töötajat.

Maksuameti andmetel oli 2000. a. Eestis 30 612 tegutsevat ettevõtet. Lähtuvalt siintoodud klassifikatsioonist 75% olid mikro-, 19% väike-, 3% keskmised, 1% suurettevõtted ja 2% määramata suurusega ettevõtted (EV Majandusministeerium, 2002).

Ettevõtted on regionaalselt ebaühtlaselt jaotunud: äriühingud Harju-, Pärnu- ja Tartumaal moodustavad peaaegu 75% kõigist äriühingutest. Märgatav on ka ettevõtluse kontsentratsioon linnadesse: kolmes suuremas linnas asub 60%, sealjuures Tallinnas ligikaudu pooled äriühingutest (EV Majandusministeerium, 2002).

Käesoleva töö skoobiks võeti ettevõtted, mis mahuvad töötajate arvu järgi kahte esimesse gruppi. Eelduseks võeti, et uuringusse võetaval firmal on rohkem kui üks

arvuti ning arvutid on omavahel ühendatud kohtvõrku. Lisaks eeldatakse, et vaatluse alla tulevad firmad kasutavad oma toodete ja teenuste tutvustamiseks ning informatsiooni levitamiseks Internetti. Roger Farnsworthi väljapakutud skaalal (Farnsworth, 1998) vastaks sellele internetikasutuse aste „Internetis kohalolek". (Joonis 6).



Joonis (6). Firma internetikasutuse ja infoturbe keerukuse seos. (Farnsworth, 1998)

3.1.1 Põhjendus sihtgrupi valikuks

Käesolevas töös on vaatluse all väikefirmad just IT vaatepunktist vaadatuna. Väikefirmade spetsiifilised probleemid selles vallas on :

- Firmas ei pruugi olla töötajat, kellele IT ülalhoid oleks põhiülesanne
- Organisatsiooni sees on tõenäoliselt piiratumad IT oskused
- Raske on igapäevaste tööde kõrvalt leida aega, et tegeleda strateegiliste küsimustega. See võib ka tähendada, et riskide haldusele ei jõuta piisavalt tähelepanu pöörata (Sophos, 2006).
- Alustavates väikeettevõtetes on tõenäoliselt ka juhtimisalane kompetents tihti madalam kui suuremates firmades.

Suurfirmadel on loomulikult rohkem kaotada, kui rahasummadest rääkida. Samas, väikefirmade tavapäraselt väiksem kasumimarginaal muudab riskihalduse jätkusuutlikkuse tagamiseks veelgi olulisemaks.

Väikeses ettevõttes töötavad juhid ja alluvad tihedamalt koos ning tahtliku sisese ründe võimalusi on vähem ning rünnet on ka lihtsam märgata. Samas on väiksemas firmas töötajatel tavaliselt laiemad volitused ning kohustused. Ülemused usaldavad alluvaid rohkem ning puuduvad kirjalikud reeglid arvutustehnika kasutuse kohta (Shinder, 2006).

Väikeettevõtted peavad üldiselt protsentuaalselt rohkem kulutama turvalisusele. Kui suurfirmades võib IT turbele kulutatav summa olla umbes 5% kogu IT eelarvest, siis väiksemates ettevõtetes on see keskmiselt 20% (CompTIA, 2007). Lihtne näide on kasvõi viirusetõrje litsentside ostmine: 5 litsentsi puhul on ühe litsentsi hind tunduvalt kõrgem kui näiteks 100 litsentsi korraga ostul.

Märkimisväärselt suur osa Eesti tööjõust on rakendatud väikeettevõtetes, millest tulenevalt on neil väga oluline roll uute töökohtade loojatena, aidates selle kaudu kaasa sotsiaalselt tasakaalustatud majandusarengu saavutamisele.

3.1.2 Valim

Valimisse võetud 9 ettevõtet on oma tööstusharu tüüpilised esindajad, mis konkureerivad vabal turul teiste sarnase ülesehitusega ettevõtetega.

Kolmel ettevõttel on põhitegevusalaks tootmine, kahel jaemüük ning neljal teenuse osutamine. Suurima töötajate arvuga firmas töötas 22 inimest, väikseim ettevõte töötajate arvu poolest oli 4 töötajaga. Kuus ettevõtet tegutsevad Tallinnas ja Harjumaal, kolm mujal Eestis. Vaadeldud ettevõtete aastakäive on vahemikus 4 – 120 miljonit krooni.

3.2 Töös kasutatav metoodika

Käesoleva töö uurimuslikus osas otsitakse vastust uurimisküsimusele „Milline on Eesti väikeettevõttele sobivaim riskide hindamise metoodika?" Sellise küsimusepüstituse puhul pole uuringut alustades teada, millised on kriteeriumid, mille

alusel sobivust hinnatakse. Selle tõttu on antud uuringu läbiviimiseks hästi kasutatavad kvalitatiivsed uurimismeetodid. Autor valis uuringu läbiviimiseks põhistatud teooria meetodi, kuna sellel on konkreetsed, hästi järgitavad sammud andmete kogumisel ning töötlemisel.

Erialast teaduslikku kirjandust läbi töötades selgus, et teaduslikke uuringuid on organisatsioonide IT riskide vallas väga vähe. Kenneth Joseph Knappi töös ettevõtte juhtkonnapoolse mõju mudelist IT turbele on seda fakti ka korduvalt mainitud ning tõenäolise põhjusena välja toodud teema delikaatsusest tuleneva takistuse andmete hankimisel (Knapp, 2005). Ankeetküsitluse läbiviimisel on oht, et respondendid ei usalda uurijat piisavalt ning ei vasta mõnedele küsimustele või annavad väära informatsiooni. Knapp lahendas selle probleemi kaheosalise uuringuga: põhistatud teooria loomine 220 respondendi vastuste põhjal ning selle valiidsuse ja reliaabluse kontrolliks kvantitatiivne andmeanalüüs ankeetküsitlusega. Eelnimetatud probleemide vähendamiseks läbis küsitlus kaks korda ekspertide paneeli, mis andis hinnangud iga küsimuse sobivusele ning liiga sissetungivad küsimused eemaldati. Lisaks sellele korraldati pilootküsitlus ankeedi testimiseks. Küsitluses osalemise motiveerimiseks pakuti rahalist kompensatsiooni.

Käesoleva töö skoobist läheks võrreldava mahuga ankeetküsitluse läbiviimine välja ning piirdutakse kvalitatiivse analüüsiga. Uuringutulemuste kvaliteedi kindlustamiseks järgiti võimalikult täpselt põhistatud teooria meetodi kasutamise juhiseid. Edasine uurimistöö antud valdkonnas võib siinloodud hüpoteese teiste metoodiliste vahenditega kontrollida.

Metoodiliseks aluseks on Barney Glaseri ja Anselm Straussi poolt 1960ndate lõpus välja töötatud põhistatud teooria (grounded theory) meetod. Glaseri ja Straussi definitsioon põhistatud teooriast sisaldab:

- korraga toimuv andmete kogumine ja analüüs
- analüütiliste koodide ja kategooriate konstrueerimine andmetest, mitte eelnevalt püstitatud hüpoteesidest
- pidev võrdlus eelneva ja uue, kogutava andmestiku vahel

- teooria edasiarendamine iga andmekogumise ja analüüsi sammu ajal
- märkmete (memode) kirjutamine et kategooriaid täpsustada, nendevahelisi seoseid leida ning tekkivas teoorias nõrku kohti leida
- valimi koostamine eesmärgiga teooria luua (teoreetiline valim), mitte valimi representatiivsust üldkogumi suhtes esiplaanile tõstes
- kirjanduse ülevaate tegemine peale iseseisvat analüüsi (Charmaz, 2006).

Meetodi rakendamisel saadav teooria on hulk hoolikalt formuleeritud kontseptsioone, mis on hüpoteesideks integreeritud ümber keskse kategooria (Glaser, Holton; 2004). Klassikaline, "puhas" metoodika seisab objektivistlikel alustel – uurimuse läbiviija "avastab" teooria andmetest, minimeerides oma subjektiivsust ning maailmavaatelist prismat, läbi mille nähtust uurib (Seaman, 2008). Glaser toonitab olemasolevate teooriate kasutamisest hoidumist, sest lihtne on analüüsi rikkuda kontseptsioone väljast sisse tuues ning andmetele tähendust peale surudes (Glaser, 1978).

Strauss ja Corbin eemaldusid Glaseri positivismist, rääkides teooria konstrueerimisest, mitte avastamisest (Strauss, Corbin; 1990). See väike muutus rõhuasetuses võimaldab olemasolevat teooriat analüüsi kaasata, kuid ka nende lähenemises on väga tähtsal kohal meetodi ja protseduuride läbiviimise tehniline täpsus (Seaman, 2008).

Kathy Charmaz (Charmaz, 2006) on astunud veel ühe sammu kaugemale, võttes seisukoha, et uurija võib üldisi põhistatud teooria juhtnööre kasutada "koos kahekümne esimese sajandi metodoloogiliste eelduste ja tõekspidamistega" (Charmaz, 2006). Selle all peab ta silmas suhtelist vabadust kvalitatiivse andmeanalüüsi kasutamisel põhistatud teooria konstrueerimisel, nimetades põhistatud teooriat lähenemiseks, mitte jäigaks meetodiks. Charmazi väide on, et kuna keegi ei saa infot otse reaalsusest, vaid läbi tajude ning interpreteerimise, ei saa ka uurija olla täiesti objektiivne (Charmaz, 2006). Käesolevas töös on järgitud Straussi ja Corbini suunda meetodi kasutamisel.

Hästi tehtud põhistatud teoorial peaks olema võime uuritavat fenomeni seletada, lisaks peaks see olema:

- andmetega kooskõlas

- kasutatav
- kontseptuaalne
- ajas vastupidav
- modifitseeritav (Charmaz, 2006)

Põhistatud teooria meetod ei anna rangeid piire andmete kogumiseks. Kvalitatiivse uuringu tarbeks andmete kogumisel on üks sobivamaid meetodeid intervjuu (Dick, 2005). Sotsiaalteadustes kasutatakse tihti süvaintervjuud, kus intervjueeritaval palutakse lisaks faktidele ja tegevustele kirjeldada ka oma tundeid ning mõtteid, inimestevahelisi suhteid (Charmaz, 2006). Infotehnoloogia kontekstis pole süvaintervjuu mitmed aspektid relevantsed, kuid mõnevõrra siiski püüdis käesoleva töö autor jõuda sügavamale kui tavalise informatsioonilise intervjuu ulatus. Selleks julgustas autor intervjueeritavaid rääkima ka teemaga seonduvalt oma mõtetest, hinnangutest ja arusaamadest, mis seni tema tegevusena ei ole väljendunud.

Knapp (Knapp, 2005) kasutas oma töös põhistatud teooria andmekogumiseks väga lühikest ankeeti – respondentidel paluti uuritava fenomeni viis omadust tähtsuse järjekorda seada ning anti võimalus oma valikut lühidalt vabas vormis kommenteerida. Käesolevas töös kasutati poolstruktureeritud intervjuud. Intervjuu plaani aluseks kasutati Virginia ülikooli riskihindamise ankeedi ülesehitust. (University of Virginia, 2004) Ankeedi teemadele lisandus teema IT rollist ettevõtte protsesside võimaldajana ning mitmed konkreetsed küsimused firma üldandmete ja struktuuri kohta. Virginia ülikooli ankeet võeti aluseks tema põhjalikkuse pärast riskihindamise teemade käsitlemisel. Intervjuu struktuuri täiendati intervjueerimise käigus ka korduvalt.

Autor viis läbi 9 intervjuud erinevate väikefirmade tegevjuhtidega. Intervjuud viidi läbi ajavahemikus jaanuar – märts 2008 eelnevalt ettevõttesse helistades ning firmajuhiga kohtumises kokku leppides. Intervjuud olid nõrgalt struktureeritud, võimaldades intervjueeritaval lahti rääkida firma IT abil toimuvad protsessid, infovarad ning süsteemid. Intervjuu teemade plaan on antud Lisas 1.

Intervjuu ajal tegi autor märkmeid, kuid intervjuu ka salvestati hilisemaks märkmete kontrollimiseks. Glaser (Glaser, 1978) ja Dick (Dick, 2005) ei pea uurimise seisukohalt oluliseks täielike transkriptsioonide tegemist intervjuudest, seega neid ka käesolevas töös ei tehtud.

Valimi moodustamisel on silmas peetud teoreetilise valimi moodustamise põhimõtteid. Teoreetiline valimi moodustamine on suunatud teoorias esile kerkivate kontseptsioonide kontrollimiseks ja tugevdamiseks (Strauss, Corbin; 1990). Varasemad vastajad on valitud nii, et valimis sisalduks firmad erinevatest majandusharudest ning erineva IT-st sõltumise määraga, mis näitaks ära võimalikult hästi sarnasused ja erinevused erinevate töö skoopi jäävate organisatsioonide vahel. Hilisemate valimisse võetud respondentidega vesteldes pööras autor suuremat tähelepanu seni olulisematena esile tõusnud teemadele. Oli kategooriaid, mis said kinnitust, kuid mõne kategooria puhul saadi ka vastupidine tulemus. Väga erandlikke juhtumeid uuringusse ei võetud, kuna igas mõttes erandid nõuaksid ilmselt täiesti individuaalset mudelit. Kodeerimise käigus suurendati valimit (leiti uusi intervjueeritavaid) niikaua, kui ajaline ressurss võimaldas. 3-4 kategooria puhul hakkas tekkima siiski ka küllastumise efekt - ehk uued intervjuud kinnitasid mudelit ning midagi olulist sellele juurde ei andnud. Lisaks intervjuudele kasutati uurimisküsimusele teise vaatenurga saamiseks Eesti Statistikaameti kogutud kvantitatiivseid andmeid (Statistikaamet, 2007).

Intervjuude ajal ning hiljem intervjuu salvestust üle kuulates, kodeeriti tekst lauseti. Iga järgneva intervjuu märkmeid võrreldi alati kõigi eelnevatega, pidades silmas sarnasusi ning välja kujunema hakkavat teooriat. Avatud kodeerimise käigus leiti intervjuudest suurusjärgus 10-40 koodi, osa neist kattusid mitmel korral. Koodideks olid konkreetsed valdkonnad, tegevused, hinnangud, kirja panduna ühe-kahesõnalisena. Enamik koode seostus valdkondadega, millega vastaja ettevõttes võis olla probleeme, kuid kodeeriti ka valdkonnad, millega kõik oli vähemalt vastaja arvates korras.

Märtsis – aprillis 2008 rakendati osaliselt paralleelselt intervjueerimisega ning avatud kodeerimisega ka telgkodeerimist. Selleks on eelnevalt avatud kodeerimisega leitud

koodide kontseptualiseerimine - kirjapanek üldistavate kategooriatena ning omavaheliste seoste leidmine.

Straussi ja Corbini järgi on telgkodeerimisel tehtavad tegevused:

- kategooriate ja alamkategooriate hüpoteetiline ühendamine
- andmepõhine kontroll
- pidev kategooriate ja alamkategooriate omaduste otsimine
- fenomeni varieeruvuse uurimine (võrdlus) (Strauss, Corbin; 1990).

Kodeerimise lõppfaasis leiti selektiivse kodeerimise käigus tuumkategooriad ning nende alamkategooriad. Tuumkategooriateks on käesoleva uuringu kontekstis lähenemisnurgad või üldised rõhuasetused riskihalduses. Need võeti esmajoones aluseks sobiva riskihindamise metoodika valikul peatükis 3 vaadeldud metoodikatest.

Edasine metoodikate võrdlus põhines uuringus leitud alamkategooriatel. Kõrvutades leitud kategooriaid käesolevas töös eelpool vaadeldud riskihindamise metoodikatega, leiti, et kõige paremini vastab uuringus osalenud firmade vajadustele kombinatsioon mitmest metoodikast.

3.3 Uuringu tulemused

Telgkodeerimise käigus kategooriate ja alamkategooriate ühendamiseks pakuvad Strauss ja Corbin välja skeemi:

Põhjus -> fenomen -> kontekst -> spetsiifilised asjaolud -> tegutsemisstrateegia -> tagajärjed (Strauss, Corbin; 1990).

Skeem on suunatud siiski eelkõige sotsiaalteadustele ning käesolevas töös täpselt sellist skeemi kasutada polnud võimalik. Intervjuusid kodeerides ei leidnud autor koode, mis tähistaksid spetsiifilisi asjaolusid ning tagajärjed on käesoleva töö kontekstis pigem tegutsemisstrateegia puudumise tulemus. Käesoleva töö loogikast lähtudes tulenes enamiku kategooriate puhul kodeerimise skeem:

Lähtepunkt -> probleem -> lahendus -> tegutsemisstrateegia.

Näide telgkodeerimise läbiviimisest käesolevas töös on ära toodud Lisas 2. Järgnevalt on käsitletud analüüsi käigus esile tõusnud kuus telgkategooriat. Esimesed kolm neist on andmeturbe põhikomponendid. Nende mõisteteni kontseptualiseerimise käigus tagasi jõudmine oli ootuspärane. Uurimuse seisukohalt on oluline nende prioriteetsus nii omavahel kui ka teiste telgkategooriatega võrreldes.

Terviklus. Põhiline teema, mis kõigist vastustest läbi kumab, on mure andmetervikluse pärast. Mitmes firmas oli viimase 4 aasta jooksul ühel või teisel moel väärtuslikke andmeid kaotsi läinud – kõvaketta riknemise tagajärjel (respondendid 4 ja 6), tarkvaralise vea tõttu (resp. 1 ja 8), riistvara varguse tõttu (resp. 5). Kõigil nimetatud juhtudel puudus adekvaatne andmete varundus. Firmajuhid tunnistasid vajakajäämist, kuid ei osanud probleemi lahenduseks midagi ette võtta. Mõnel juhul varundusi aeg-ajalt tehti, kuid mitte regulaarselt - puudus konkreetne tööprotsess. Respondent 2 oli kõigist küsitletuist kindlam, et kaugvarundus failiserverist toimib, kuid ka tema möönis, et pole kontrolli, kas varundus toimub siiski kõigist vajalikest failidest. Samuti vajab lahendust probleem, et varunduse alt jäävad välja e-posti arhiivid ning failid, mida kasutajad hoiavad oma masinates.

Konfidentsiaalsus. Tähtsuselt teine, kuid siiski tunduvalt vähemoluline teema oli konfidentsiaalsus. Tulenevalt firmade erinevast spetsiifikast olid konfidentsiaalsuse kao põhimured erinevad: endise töötaja ligipääs andmetele (resp. 6); kassaarvutist toodete hinnainfo lugemine (resp. 4); varastatud riistvaraseadmest krüpteerimata tundliku info lugemine (resp. 2 ja 5) Mitte ükski firmajuhtidest ei olnud täheldanud edukaid suunatud ründeid nende firma vastu Internetist. Mitmed vastajad toonitasid, et konfidentsiaalse info neilt kättesaamiseks on tunduvalt lihtsamaid meetodeid kui arvutivõrgu ründamine.

Käideldavus. Jätkates andmeturbe põhiaspektide vaatlust, oli käideldavus neist kõige madalama tähtsusega. Vaadeldud firmadest on andmetöötlus aegkriitiline vaid resp. 7 firmas, mis töötleb suuremahulisi meediafaile. Antud firmas on olemas varuriistvara põhitööjaama väljalangemiseks olemas. Tööseisakuid IT mittetoimimise pärast oli

aset leidnud enamikus firmadest, kuid selle mõju firmale hindasid vastajad üldjuhul väikseks. Ainult resp. 9 raamatupidamisteenust pakkuvas ettevõttes aset leidnud tööseisak andmebaasiarvuti rikkimineku tagajärjel tõi intervjueeritava hinnangul kaasa märkimisväärset kahju.

Infovarad. Intervjueerimise käigus tuli tihti välja, et firmajuht ei olnud tuttav infovara mõistega ning erinevatele infokogumitele ei olnud antud erinevaid väärtusi. Seetõttu ei osatud ka turvameetmeid diferentseerida – millised andmed peaksid olema turvalisemas kohas, millised mitte. Väärtuslik info oli ka mitmel puhul paigutatud ebasüstemaatiliselt, erinevates arvutites, erinevatel ketastel jne. (resp. 1, 5, 8). Intervjuu käigus nõustusid kõik respondendid, et edukalt IT riske hallata, peavad infovarad olema identifitseeritud ning piiritletavad.

Tööviljakus. IT-st tugevalt sõltuvates firmades, kus tugiisikut ei ole, märgiti mitmel korral probleemina tööviljakuse langust seoses vale konfiguratsiooniga, kasutaja teadmatusega või aja kulutamisega, kui kasutaja proovib mõnd riistvara- või tarkvaraprobleemi ise lahendada. (resp. 1, 3, 5, 6) Olukorras, kus IT spetsialist jõuaks kohale paari tunni jooksul, tundub tihti mõttekam ise üritada lahendust leida. Siiski juhtub mõnikord ka nii, et töötaja näeb ise põhjendamatult kaua probleemi kallal vaeva ning ikka tuleb spetsialist kohale kutsuda. Kahju firmale on sellisest juhtumist väike, kuid tõenäosus selliseks juhtumiks on suur. Firmades, kus mõni töötaja on IT vallas teadlikum, on selline probleem tunduvalt väiksem. Paljud probleemid suudab selline tugiisik ise lahendada ning kui probleem käib talle üle jõu, oskab ta kiiremini otsuse vastu võtta väljastpoolt abi otsida.

Turvateadlikkus. Käsitledes arvutikasutajate teadlikkust erinevatest IT riskidest, jagasid intervjueeritavad oma kogemusi erinevate alluvatega, ning püüdsid ka ise üldistusi selle põhjal teha. Ühel meelel oldi selles, et pikaajalise töötaja puhul on oht väiksem, et ta firma infovarasid kogemata või meelega kahjustab, kui hiljuti tööle võetud töötajal. Paratamatult on uude kohta tööle asudes vaja midagi juurde või ümber õppida, ning selle käigus on oht ka vigu teha.

Probleeme mainisid firmajuhid ka seoses madalama haridustasemega töötajatega. Tänapäeva tööprotsess nõuab, et arvutit kasutab ka näiteks laojuhataja (resp. 1) või

mehaanik (resp. 3 ja 6), kuid esiteks tunnetatakse vastuseisu uute ülesannete õppimisele selliste töötajate poolt ning teiseks on tunduvalt kõrgem risk, et selliste kasutajate arvutid nakatuvad viiruste või nuhkvaraga.

Kolm intervjueeritavat seostasid arvutikasutajate käitumist ka nende vanusega. Respondendid 2 ja 4 pidasid kasutajatest tulenevat ohtu väikseks tänu kollektiivi noorusele – kuna noored inimesed on vastuvõtlikumad uuele tehnoloogiale, saavad paremini aru inglise keelest ning on üldiselt rohkem huvitatud IT valdkonna uudistest ja arengutest. Samas, respondent 7 pidas suurimaks ohu allikaks just noori töötajaid, kuna noored inimesed on riskialtimad, näiteks installeerides ise oma töökohaarvutitesse tundmatu päritoluga tarkvara. Samuti kasutavad noored Internetti tunduvalt enam isiklikuks suhtluseks ning nende poolt külastatavate saitide ring on laiem kui vanematel kolleegidel.

3.4 Metoodikate analüüs lähtuvalt uuringu tulemustest

Lähtuvalt uuringu tulemustest formuleeriti riskide hindamise metoodika kriteeriumid:

- Riskide hindamine peaks keskenduma protsessidele ja inimestele, mitte niivõrd tehnilistele vahenditele. Tehniline risk muutub ajas kiiresti – olgu näiteks operatsioonisüsteemide turvaaukude avastamine ja tarkvaratootja poolne lappimine. Tehnoloogia ostmine ning rakendamine poleks probleem kui juht teaks, mida täpselt vaja on.
- IT riskide hindamise fookuseks võtta ettevõtte infovarad. Kaugem eesmärk on muidugi firma väärtuse ning kasumlikkuse kaitsmine, kuid infovarade seos nendega on piisavalt püsiv ajas. Riistvara ja infrastruktuur kui abivahendid infovara töötlemiseks, ülekandmiseks ja hoidmiseks tuleb küll riskide hindamisse kaasata, kuid põhiliselt seoses neis sisalduva või töödeldava infovaraga. Erandiks on ainult riistvaraga seotud riskid – näiteks vääruslikke andmeid mittesisaldava sülearvuti vargus.
- Metoodika peaks iga infovara kolme andmeturbe aspekti eraldi vaatlema, kuna nende tähtsus võib olla väga erinev.
- Riskide hindamine peaks olema teostatav mitte-eriala inimese poolt. Mitu vastajat mainis, et IT riskihalduse jätmine IT tugiisiku hooleks ei ole olnud

õige samm, sest ka tugiisik ei hinnanud riske süstemaatiliselt ning leidis aset intsident, mida oleks saanud suhteliselt lihtsalt vältida.

- Riskide hindamine peaks olema ökonoomne, kiiresti läbiviidav – pika ja detailse analüüsi puhul on palju suurem tõenäosus, et ajapuuduse tõttu jääb riskide hindamine venima.

Kuna infovarasid ei ole paljud firmajuhid varadena käsitlenud ja neile väärtusi andnud, tuleks käesoleva töö autori arvates aluseks võtta metoodikad, mis alustavad sellest. Vastasel korral poleks ju riskide hindajal teada, mida tarvis kaitsta on. Küsimused, mida riskihindaja esimesena küsima peaks on:

- Milline infokogum/tarkvara/süsteem on eelduseks selles valdkonnas äri tegemiseks/võimaldab kasumit teenida/annab konkurentsieelise?
- Millised infovarad tõstavad efektiivsust, vähendavad kulusid või hoiavad kokku töötajate aega?

Koos infovarade määratlusega tuleks hinnata ka nende olulisust firmale (näiteks skaalal madal-keskmine-kõrge). Sellest oleneb hiljem otseselt turvameetmete valik, kuna kõigile süsteemidele maksimaalsete turvameetmete kohaldamine ei ole majanduslikult mõttekas. Need kaks sammu on eespool vaadeldud metoodikatest esimeste sammudena ära märgitud Andressi raamatus ja NIST *Käsiraamatus*. Viimase puhul on küll enne veel „Riskihindamise skoobi ja metodoloogia määramine", mis aga käesoleva töö raames ära tehakse. ISKE küll järgib sama loogikat, kuid siin on vajalik ka kogu riistvara ning infrastruktuuri nimekirja tegemine ning erinevate väärtuste andmine käib läbi standardsete turvaklasside, mis väikeettevõtte konteksti ei sobi. Teised vaadeldud metoodikad järgivad erinevaid loogikaid – alustades äriprotsesside kaardistamisest (FRAP), firma eesmärkide paikapanekust (CobiT ja I-ADD) või hoopis ohtude kindlaksmääramisest (GAO, Elky, NIST *Riskihindamise juhend*).

NIST Käsiraamat toob eraldi välja kolmanda sammuna tagajärgede hindamise – erineva raskusastmega stsenaariumide analüüsi tervikluse, käideldavuse ja konfidentsiaalsuse kao kohta. Käesolevale uuringule toetudes võib öelda, et sellised mõttelised stsenaariumid aitavad firmajuhte oluliselt infovarade väärtuste leidmisel.

Jätkates Andressi ja NIST Käsiraamatu riskide hindamise struktuuri analüüsi, on mõlema metoodika järgnevad sammud ohtude ja nõrkuste leidmine ning olemasolevate leevendusmeetmete analüüs. Erinevus on sammude järjestuses ja rõhuasetustes. Andress pakub välja kõigepealt nõrkuste otsimise. Arvutivõrgu, operatsioonisüsteemide ja rakendusprogrammide turvaaukude avastamiseks soovitatakse kasutada automaatseid skaneerimisvahendeid. Vaatluse ja dokumentidega tutvumise teel leitakse füüsilised, organisatsioonilised nõrkused ning puudulikud reeglistikud. Järgmine samm on olemasolevate leevendusmeetmete hindamine. Oht on Andressi käsitluses adekvaatse leevendusmeetmeta nõrkus, s.t. eeldatakse, et kui on olemas nõrkus, leidub sellele ka oht, mis selle nõrkuse ära kasutamisele on suunatud. Ohu suurus on sellises käsitluses määratletud vaid nõrkuse "suurusega" ning vara väärtusega. Inimfaktorist tuleneva, kuritahtliku ohu puhul jääb sel puhul ohu hinnangust välja motivatsioon, mida võetakse arvesse järelikult ohu realiseerumise tõenäosuse komponendina.

NIST Käsiraamat seevastu jätkab analüüsi ohtude leidmisega, mis võivad viia eelmises punktis kirjeldatud tagajärgedeni, kasutades ohu mõistet samamoodi kui käesolev töö (vt. ptk. 2.3). Seda tuleb teha süstemaatiliselt, iga infovara kohta. NIST Käsiraamat näeb ette selles sammus ka ohtude analüüsi – intsidendi toimumise tõenäosuse ja varade kahjustamise potentsiaali hindamise. Alles seejärel leitakse olemasolevad leevendusmeetmed ning hinnatakse nende efektiivsust ning tulemuseks saadakse nõrkused – süsteemid, kus puuduvad adekvaatsed leevendusmeetmed.

Viimaste sammude – riskianalüüsi – läbiviimine on vaadeldavates metoodikates lahendatud samuti erinevalt. Andress jätkab kõikvõimalike leevendusmeetmete leidmisega, nende kuluefektiivsuse analüüsi ning otsustusprotsessiga. NIST Käsiraamatu puhul on riskianalüüsi sammudeks tõenäosuste hindamine, võttes aluseks varem analüüsitud ohud ning avastatud nõrkused; ning võttes arvesse ka varade väärtusi, otsuste formuleerimine riskide aktsepteerimise või leevendamise vajaduse kohta. Leevendusmeetmete valiku protsess jäetakse läbiviija otsustada põhjendusega, et see oleneb suuresti organisatsioonikultuurist ja riskihindamise eesmärkidest.

Käesoleva töö üks kriteeriume oli ökonoomsus. Selles valguses tasub vaadelda ka Steve Elky riskide hindamise protsessi, mille koostamisel on silmas peetud kiiret ja lihtsat läbiviimise protsessi ning sobivust väikestele organisatsioonidele. Alustatakse ohtude ja nõrkuste loetelude koostamisest. Ohtude ja nõrkuste leidmiseks soovitatakse kasutada avalikke andmebaase. Järgnevalt seostatakse ohud ja nõrkused omavahel, luues oht-nõrkus paarid. Selliste paaride põhjal hinnatakse ebasoovitava sündmuse toimumise tõenäosused ning seejärel hinnatakse mõju organisatsioonile läbi kolme andmeturbe komponendi.

Ükski vaadeldud metoodika muutmata kujul käesoleva uuringu tulemusel formuleeritud kriteeriumidele ei vasta. Küll aga on võimalik nende osi kombineerides välja töötada sobivam lahendus.

3.5 Kohandatud metoodika

Võttes aluseks uuringu tulemusena formuleeritud IT riskide hindamise kriteeriumid ning olemasolevate riskihindamise metoodikate analüüsi, pakub autor välja kohandatud metoodika, milles on kombineeritud NIST Käsiraamatu ja Elky metoodikate osi.

Käesoleva töö autor ei pea vajalikuks eraldi nõrkusi ning seejärel olemasolevaid turvameetmeid hinnata. Kui mõni turvameede on saanud organisatsioonis normiks ning toimib efektiivselt, ei ole mingit põhjust teda vastavast nõrkusest eraldada (näiteks: koridorist ligipääs serveriruumile – serveriruumi lukustamine). Kui turvameede osutub ebapiisavaks ning see tuleb uue turvameetme kasutuselevõtul eemaldada, saab vastava analüüsi teha peale riskide hindamist, täiendavate turvameetmete valiku protsessis.

Väikeettevõtte piiratud ressursside tõttu pole mõtet koostada nimekirja kõikvõimalikest turvameetmetest, olenemata hinnast. Kuna firma juht on niigi kogu riskihindamise protsessi juures, võib ka meetmete leidmine ja nende vahel valimine toimuda korraga. Meetmete leidmisel on oluline püstitada küsimus vaatenurgast: kuidas on võimalik riski leevendada eelkõige organisatoorsete vahenditega -

tööprotsesse muutes, töötajate kohustusi ja vastutust määratledes? Võimaluse korral tuleks sellesse sammu kaasata asjassepuutuvad töötajad, kellel võib olla ka endal ideid lahenduse leidmiseks. Kui sel teel kõigile osapooltele aktsepteeritavat lahendust ei leita, analüüsitakse võimalikke tehnoloogilisi lahendusi riskide leevendamiseks.

Käesolevas töös formuleeritav riskide hindamise metoodika koosneb seitsmest sammust:

1) **Infovarade identifitseerimine**. Koos identifitseerimisega hinnatakse infovarade väärtusi suhtelisel skaalal, näiteks madal-keskmine-kõrge. Suurema täpsuse saavutamiseks saab astmeid ka rohkem defineerida.
2) Võimalike ebasoovitavate **tagajärgede hindamine** (eraldi tervikluse, käideldavuse ning konfidentsiaalsuse osaline ning täielik kadu infovarade lõikes).
3) Lähtudes eelpool leitud riskihindamise seisukohalt olulistest tagajärgedest, **nimekirja koostamine ohtudest**, mis võivad nimetatud tagajärgedeni viia. Lähtepunktiks saab võtta mõne vabalt kättesaadava ohtude nimekirja, näiteks CACI, Inc. ohtude taksonoomia veebilehel *http://www.caci.com/business/ia/threats.html,* eemaldades sellest ebavajalikud ning lisades organisatsioonispetsiifilised.
4) Organisatsioonis eksisteerivate **nõrkuste leidmine**. Tehnoloogiliste nõrkuste leidmiseks on sobivad avalikud nõrkuste andmebaasid, näiteks Common Vulnerabilities and Exposures (*http://cve.mitre.org/*). Organisatsiooniliste ning inimestega seotud nõrkuste hindamiseks on käesoleval hetkel hea materjal Riigi Infosüsteemide Arenduskeskuse poolt eesti keelde tõlgitud *Infoturbe juhend. Lühiülevaade olulisematest infoturbe alastest turvameetmetest* (Riigi Infosüsteemide Arenduskeskus, 2004). Materjal on algselt saksakeelsena Saksa Infoturbeameti (BSI) poolt välja antud ning põhineb BSI etalonturbe juhendil.
5) **Ohtude ja nõrkuste seostamine** omavahel. Tulemuseks on nimekiri oht-nõrkus paaridest. Iga oht-nõrkus paari puhul hinnatakse kohe ka selle realiseerumise tõenäosust suhtelisel skaalal madal-keskmine-kõrge. (näiteks Elky pakutud skaala, ptk. 2.5.9).
6) **Riskide hindamine** tõenäosuse ja teises sammus leitud tagajärgede alusel, kasutades Steve Elky riskide hindamise tabelit. (Tabel 5, ptk. 2.5.9)

7) Täiendavate **turvameetmete leidmine ja valik**. Liikudes kõrgetelt riskidelt madalamate suunas, leitakse võimalikud leevendusmeetmed ning otsustatakse nende rakendamine. Selles etapis toimub ühtlasi kommunikatsioon – kõigi töötajate teavitamine infovarade väärtusest, nõrkustest ning ohtudest. Kui võimalik, võiks turvameetmete valiku protsessi kaasata asjassepuutuvad töötajad. Lisakohustus töötajatele võetakse tõenäoliselt paremini vastu, kui see on ühise arutelu käigus vastu võetud. Samas selgub ka kohe arutelu käigus, millised turvameetmed tekitavad töötajates vastuseisu ning on tõenäoline, et nad ei hakka seda kasutama. John Wylder toonitab oma raamatus (Wylder, 2004) vajadust iga-aastases arenguvestluses käsitleda ka arvutiturvalisuse teemat, et kasutajad mõistaksid, et nad ise on osa lahendusest ja vastutavad ka neile usaldatud info eest. Ilmselt leidub väikeettevõtteid, kus ei peeta arenguvestlusi – sel juhul on hea võimalus teemat käsitleda riskide hindamise lõppfaasis. Erinevate tehniliste meetmete maksumuse ja efektiivsuse prognoosimisel võib kasutada väliste spetsialistide abi.

Kokkuvõte

Käesoleva töö eesmärk oli välja selgitada, millistele kriteeriumidele peab vastama väikeettevõtte jaoks sobiv IT riskide hindamise metoodika. Selleks vaadeldi üheksat riskihindamise metoodikat ning viidi läbi uuring väikeettevõtete juhtide seas.

Uuringu andmete kogumine toimus intervjueerimise teel ning andmeanalüüsiks kasutati põhistatud teooria meetodit. Uuringu tulemusena leiti viis kriteeriumit, mille alusel valida IT riskide hindamise metoodikat väikeettevõttele.

- Riskide hindamine peaks keskenduma protsessidele ja inimestele, mitte niivõrd tehnilistele vahenditele. Inimesed (töötajad) on alati olnud infoturbe nõrgim lüli ning väikeettevõtetes ei pöörata protsesside korrektsele läbimisele tihti piisavalt tähelepanu.
- IT riskide hindamise fookuseks tuleks võtta infovarad. Väikeettevõtete juhid ei osanud erinevatele andmetele erinevaid väärtusi anda ning paljuski selle tõttu olid vaadeldud ettevõtetes olulised infovarad ebapiisavalt turvatud.
- Infovarade kolme andmeturbe aspekti tuleks vaadelda eraldi, kuna nende olulisus võib olla väga erinev.
- Riskide hindamine peaks olema teostatav ka mitte-erialaspetsialisti poolt.
- Riskide hindamine peaks olema võimalikult ökonoomne ja kiiresti läbiviidav.

Lähtuvalt nendest kriteeriumidest olemasolevaid metoodikaid analüüsides selgus, et optimaalse tulemuse annab kahe metoodika erinevatest sammudest kombineeritud uus metoodika. Metoodika seitse etappi on:

- Infovarade identifitseerimine ja neile väärtuste andmine
- Võimalike intsidentide tagajärgede hindamine infovarade lõikes
- Ohtude nimekirja koostamine, mis eelpool loetletud tagajärgedeni võivad viia
- Nõrkuste leidmine, arvestades olemasolevaid turvameetmeid
- Ohtude ja nõrkuste omavaheline seostamine koos tõenäosuse hindamisega
- Riskide hindamine tõenäosuste ja tagajärgede kaalukuse alusel
- Täiendavate turvameetmete leidmine ja valik.

Töö eesmärk sai üldjoontes täidetud, kuid metoodika reaalseks rakendamiseks firmajuhtide poolt oleks autori hinnangul vaja metoodika sammud rohkem lahti kirjutada ning võibolla ka erinevate tegevuste läbiviimisest näiteid tuua.

Edasine töö antud valdkonnas olekski formuleeritud metoodika sammude täpsem määratlus ning metoodika reaalne testimine ettevõtte riskide hindamisel. Uurimist väärib ka küsimus, kas väikeettevõtetele oleks võimalik välja töötada ISKE-ga sarnane etalonturbe süsteem, s.t. kas on võimalik väga erinevate tegevusalade ja tööprotsessidega ettevõtteid rahuldav turvaklasside ja turvameetmete süsteem.

Kasutatud kirjandus

Alberts, Christopher; Dorofee, Audrey; Stevens, James; Woody, Carol. (2005). OCTAVE-S Implementation Guide, Version 1.0. Carnegie Mellon University, Software Engineering Institute. URL http://www.cert.org/octave-s/download/ (28.04.2008)

Andress, Amanda. (2004). Surviving Security: How to Integrate People, Process and Technology. Auerbach Publications.

Better Business Bureau. (2006). Security & Privacy: Made Simpler. URL http://us.bbb.org/WWWRoot/storage/16/documents/SecurityPrivacyMadeSimpler.pdf (28.04.2008)

Black, Rex. (2002). Investing in Software Testing: The Risks to System Quality. URL http://www.stickyminds.com/getfile.asp?ot=XML&id=3564&fn=XDD3564filelistfilename1%2Epdf (28.04.2008)

Braunstein, Adam. (2003). The Importance of Mitigating IT Risk. CIO Magazine. URL http://www2.cio.com/analyst/report1867.html (28.04.2008)

Carr, Nicholas G. (2003). IT Doesn't Matter. URL http://www.roughtype.com/archives/2007/01/it_doesnt_matte.php (28.04.2008)

Charmaz, Kathy. (2006). Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis. SAGE Publications.

Committee of Sponsoring Organizations of the Treadway Commission, the. (2004). Enterprise Risk Management: Integrated Framework. Executive Summary. URL http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf (28.04.2008)

CompTIA. (2007). Information Security: A CompTIA Analysis of IT Security and the Workforce. URL http://www.comptia.org/sections/research/reports/200704-ITSecurity.aspx (28.04.2008)

Dick, Bob. (2005). Grounded Theory: A Thumbnail Sketch. URL http://www.scu.edu.au/schools/gcm/ar/arp/grounded.html (28.04.2008)

Elky, Steve. (2006). An Introduction to Information System Risk Management. URL http://www.sans.org/reading_room/whitepapers/auditing/1204.php (28.04.2008)

EV Majandusministeerium. (2002). Ettevõtlik Eesti: Eesti väike- ja keskmise suurusega ettevõtete arendamisele suunatud riiklik poliitika 2002 - 2006. URL http://www.mkm.ee/failid/Ettevotlik_Eesti.doc (28.04.2008)

Farnsworth, Roger. (1998). Introduction to Information Security. White Paper. Cisco Systems, Inc. URL http://whitepapers.silicon.com/publisher/39025422/cisco.htm?o=325&pp=25 (10.09.2007)

Federal Aviation Administration. (2005). FAA System Safety Handbook. URL http://www.faa.gov/library/manuals/aviation/risk_management/ss_handbook/ (28.04.2008)

Glaser, Barney. (1978). Theoretical Sensitivity: Advances in the Methodology of Grounded Theory. Sociology Press.

Glaser, Barney; Holton, Judith. (2004). Remodeling Grounded Theory. Forum: Qualitative Social Research, Vol. 5 No. 2, 2004. URL http://www.qualitative-research.net/fqs-texte/2-04/2-04glaser-e.htm#g31 (28.04.2008)

Goodwin, Steve. (2000). Software Risk Management Makes Good Business Sense. URL http://www.stickyminds.com/s.asp?F=S2663_ART_2 (28.04.2008)

Gregg, Michael; Kim, David. (2005). Inside Network Security Assessment: Guarding Your IT Infrastructure. SAMS Publishing.

Gupta, Atul; Hammond, Rex. (2003). Information Systems Security Issues and Desicions for Small Businesses: An Empirical Examination. Information Management & Computer Security, Vol. 13 No. 4, 2005, lk. 297-310.

Hall, Payson. (2003). Knowing the Odds. URL http://www.asma-sqa-nsw.org.au/newsletters/webJul03.pdf (28.04.2008)

Hanson, Vello; Buldas, Ahto; Martens, Tarvi; Lipmaa, Helger; Ansper, Arne; Tulit, Viljar. (1997). Infosüsteemide turve I: Turvarisk. Cybernetica AS.

ISO/IEC. (2004). International Standard ISO/IEC 13335-1: Information Technology - Security Techniques - Management of Information and Communications Technology Security. First Edition 2004-11-15

IT Governance Institute. (2007). CobiT 4.1. URL http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders/COBIT6/Obtain_COBIT/Obtain_COBIT.htm (28.04.2008)

Kivimaa, Jüri. (2007). Missugune peaks olema hea infoturbe standard? URL http://www.focusit.ee/doc.php?25431 (28.04.2008)

Knapp, Kenneth J. (2005). A Mediation Model of Managerial Effectiveness in Information Security: From Grounded Theory to Empirical Test. URL http://handle.dtic.mil/100.2/ADA440189 (28.04.2008)

Koppelmaa, Ivo. (2003). Infotehnoloogia riskide juhtimine AS-is Express Post. Magistriprojekt ärijuhtimise magistri kutsekraadi taotlemiseks. Tartu Ülikool.

Koppelmaa, Ivo. (2004). Kehtestati infosüsteemide turvameetmete süsteem. URL http://www.riso.ee/et/pub/2004it/docs/2.2.html (28.04.2008)

Landoll, Douglas J. (2006). The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments. Auerbach Publications.

Marsh Plc. (2006). Attitudes to Risk Management: A New Zealand Perspective. URL http://www.marsh.co.nz/docs/NZ%20Survey%20of%20Risk%202006.pdf (28.04.2008)

Munipalli, Yamini. (2005). Measuring the Risk Factor. URL http://www.stickyminds.com/s.asp?F=S9379_ART_2 (28.04.2008)

National Institute of Standards and Technology. (1997). An Introduction to Computer Security: The NIST Handbook. Special Publication 800-12. URL http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf (28.04.2008)

Parts, Anne. (2003). IT riskianalüüs Elektroskandia AS näitel. Magistritöö. Tallinna Ülikool. URL http://www.cs.tlu.ee/osakond/opilaste_tood/magistri_tood/2003_sugis/Anne_Parts/Anne_Parts_Mag_Too_Lubatud.pdf (28.04.2008)

Passori, Al. (2004). Selecting the Risk Assessment Method of Choice: White Paper.

Peltier, Thomas. (2003). Understanding Facilitated Risk Analysis Process (FRAP) and Security Policies for Organizations. URL http://www.security.org.sg/webdocs/news/event21/TomPeltier_FRAP.ppt (28.04.2008)

Richardson, Robert. (2007). CSI Survey 2007: The 12th Annual Computer Crime and Security Survey. URL http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf (28.04.2008)

Riigi Infosüsteemide Arenduskeskus. (2004). Infoturbe juhend: Lühiülevaade olulisematest infoturbe alastest turvameetmetest. URL http://www.bsi.de/gshb/intl/ee/infoturbe_soovituste_juhend_v1.pdf (28.04.2008)

Seaman, Jayson. (2008). Adopting a Grounded Theory Approach to Cultural-Historical Research: Conflicting Methodologies or Complementary Methods? International Journal of Qualitative Methods, Vol. 7 No.1, 2008 URL http://ejournals.library.ualberta.ca/index.php/IJQM/article/view/1616/1145 (28.04.2008)

Shinder, Deb. (2006). Strategies for Preventing Internal Security Breaches in a Growing Business. URL http://articles.techrepublic.com.com/5100-10878_11-6123377.html (28.04.2008)

Siimon, Aino. (2001). Ettevõtte suuruse määratlemine majanduspoliitilise harmoniseerimise kontekstis. Tartu Ülikool. URL http://www-1.mtk.ut.ee/varska/2001/Str_ettevotluspol/Siimon.pdf (28.04.2008)

Snedaker, Susan. (2006). IT Security Project Management: Handbook. Syngress Publishing.

Sophos Plc. (2006). Protecting Small and Growing Businesses: A Sophos Positioning Paper. URL http://www.sophos.com/security/whitepapers/Sophos-Small-Business-wpus (28.04.2008)

Spinellis, D., Kokolakis, S., Gritzalis, S. (1999). Security Requirements, Risks and Recommendations for Small Enterprise and Home Office Environments. Information Management & Computer Security, Vol. 7 No. 3, 1999, lk. 121-128.

Statistikaamet. (2007). IT08: Turvameetmeid kasutavad ettevõtted turvameetme järgi. URL http://pub.stat.ee/px-web.2001/Database/Majandus/05Infotehnoloogia/02Infotehnoloogia_ettevettes/02Infotehnoloogia_ettevettes.asp (28.04.2008)

Stoneburner, Gary; Goguen, Alice; Feringa, Alexis. (2001). Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology. URL http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (28.04.2880)

Strauss, Anselm; Corbin, Juliet. (1990). Basics of Qualitative Research: Grounded Theory Procedures and Techniques. SAGE Publications.

Swaminatha, Tara M.; Elden, Charles R. (2002). Wireless Security and Privacy: Best Practices and Design Techniques. Addison Wesley.

Tipton, Hal; Krause, Micki (toimetajad). (2000). Information Security Management Handbook. 4th ed. CRC Press.

Tulloch, Mitch. (2003). Microsoft Encyclopedia of Security. Microsoft Press.

Turner, Kimberley; Keetelaar, Deanne. (2005). Risk Management Guide for Small Business. URL http://www.smallbiz.nsw.gov.au/NR/rdonlyres/57688513-FCF3-4AF4-AC76-B2B640974C10/0/RiskManagementfullcopy.pdf (28.04.2008)

United States General Accounting Office. (1999). Information Security Risk Assessment - Practices of Leading Organizations: A Supplement to GAO's May 1998 Executive Guide on Information Security Management. URL http://www.gao.gov/special.pubs/ai00033.pdf (28.04.2008)

University of Virginia. (2004). Information Technology Security Risk Management (ITS-RM) Program. URL http://www.itc.virginia.edu/security/riskmanagement/docs/ITS-RM_v2-0_packet.doc (28.04.2008)

Wylder, John. (2004). Strategic Information Security. Auerbach Publications.

IT Risk Assessment Methodology for Small Enterprises

Statistical data show, that as IT usage continues to spread in businesses, the percentage of IT budget spent on security rises as well. While in 2005, security spending was 15% of IT budget on average, in 2006 it had risen to 20% (CompTIA, 2007). As the importance of IT security rises, it becomes more and more important to develop and use cost-effective risk management methods to keep IT risks at the desired level.

This thesis addresses IT risk assessment, which is one of the most important components of risk management. There are several different risk assessment methodologies for big organizations. One can also find many articles and guides on PC security for individual users at homes. But no methodology was found by the author that is specifically designed for small companies (10 to 50 employees). This thesis is trying to fill in this gap. The aim is to give reliable criteria for selecting a methodology for a small company, and using the criteria, propose a methodology that fits them best.

The thesis begins with a brief overview of enterprise risk management, and positioning IT risk management within that. After that, IT risk management and risk assessment terminology is discussed on the basis of International Standard ISO/IEC 13335-1.

Nine risk assessment methodologies were chosen from literature, which were considered by their authors also suitable for small enterprises. These are presented along with overview of recent research literature in IT risk management field. The research portion of this thesis tries to find answers to the question, what are the possibilities and limitations of typical small firms regarding IT risk assessments. For that, nine interviews were made with managers of small companies. The interviews were coded using the Grounded Theory method. Five criteria were formulated, that should be taken into account when choosing a risk assessment methodology.

The five criteria are:

- The emphasis of a risk assessment should be on processes and people (and less on technology).
- The focus of risk assessment should be on information assets. The correct identification and valuation of information assets is vital to a cost-efficient IT risk management.
- The three aspects of information security - data integrity, accessibility and confidentiality - should be considered separately because they can have very different values to a company.
- It should be possible to perform the risk assessment by a person who is not computer specialist.
- The risk assessment process should be as economic and fast as possible

The nine methodologies were evaluated based on these criteria and a conclusion was made, that an optimal methodology for a small company would be combined from the steps of two existing methodologies.

The seven steps of the proposed methodology are:

- Identifying and evaluating information assets.
- Evaluating possible consequences for the company when data integrity, accessibility or confidentiality of an information asset is compromised.
- Identifying threats that can lead to aforementioned consequences.
- Finding weaknesses in systems, organization, processes and people, considering current security measures in place.
- Pairing threats and weaknesses, and assessing the probability of the threat exercising the vulnerability.
- Assessing risks based on probability and consequences.
- Identifying and selecting additional security measures, starting from high-risk areas.

To be of real value to small businesses, this rather conceptual framework of the methodology should be further specified and tested in business environment. One idea might be to develop security classes for small companies similar to those in ISKE.

Lisad

Lisa 1. Intervjuu teemade plaan

A. Firma iseloomustus

Millega firma tegeleb?

Mitu töötajat on firmas?

Aasta müügikäive (suurusjärk).

Aasta IT eelarve (suurusjärk).

Hinnang sõltuvuse määrale infotehnoloogiast.

vähesel määral: arvuti abil toimuvad vaid põhitegevust toetavad protsessid (e-suhtlus, raamatupidamine, maksete teostamine). IT mittetoimimine (kuni 4 tööpäeva) põhjustab üldjuhul vaid ebamugavust ja väga vähe lisakulu.

keskmisel määral: infotehnoloogial on toetav roll, kuid põhitegevuse jätkamine ilma selleta on mõnevõrra raskendatud. Kogu IT väljalangemine kuni kaheks päevaks tekitab probleeme, kuid need on muul viisil lahendatavad ning rahaline kahju ei ole üldjuhul märkimisväärne.

suurel määral: infotehnoloogia toimimine on firma põhitegevuse eelduseks - kui IT ei toimi, seiskub ka töö. Kahjud või saamata jäävad tulud on firma seisukohast märkimisväärsed, kui töökoht on rivist väljas üle ühe tööpäeva või kesksüsteem/server pool tööpäeva.

täielikult: firma vajab elektroonilisi kanaleid ning süsteeme oma kauba/teenuse pakkumiseks - iga katkestus süsteemis võib tähendada lahkunud kliente ja saamata jäävat tulu. Üle 15 minutiline katkestus keskses süsteemis või töökoha rivist välja langemine kaheks tunniks tekitab olulist kahju.

Mitu arvutitöökohta on firmas?

Serverid, nende funktsioonid.

Kes hoiab IT-d korras?

- üks isik firma sees/väljas
- igaüks ise oma arvuti
- vastavalt olukorrale otsitakse abi
- lepinguga teenusepakkuja

Kas vastutus on selge? Teenustase, trahvid?

Kui tähtsaks peab firmajuht adekvaatset IT riskihaldust firma seisukohalt?

- üldse mitte
- pigem mitte
- mõnevõrra
- tähtis
- väga tähtis

B. Kontode ja paroolide haldus

Operatsioonisüsteemi paroolid.

Rakendustarkvara paroolid.

E-posti paroolid.

Lahkuvate ja lisanduvate töötajate kasutajakontod.

Juurdepääsuõiguste haldamine.

C. Viirusetõrje

Kas on kõigis arvutites?

Kuidas kontrollitakse, kas toimib, uuendused jne.

Kas on aset leidnud nakatumisi? Kirjeldus, kahju suurus.

Muu "pahavara".

Kes õpetab kasutajaid õigesti käitlema meilimanuseid, faile võõralt mälupulgalt, makrodega dokumente jne).

D. Andmete varundus ja taaste

Kas toimuvad regulaarsed varundused? Millest?

Kas on proovitud taastada varundatud faili?

Kes vastutab varunduse eest?

Intsidendid seoses varundusega (varunduse puudumine, ebapiisavus).

E. Tundliku informatsiooni kaitse

Infovarad – andmekogumid, tarkvara, intellektuaalomand.

Kas on teada kus (kettal) füüsiliselt infovara asub?

Kas andmetel on konkreetne omanik?

Kuidas (kas) piiratakse juurdepääsu?

Kaugjuurdepääs ja traadita võrk – kas krüpteeritud? Kas on teada, mis krüptoalgoritm, kas on piisav?

F. Operatsioonisüsteemid

Operatsioonisüsteemide turvauuendused – kas toimuvad? Automaatselt või käsitsi?
Ketaste ja kaustade väljajagamine kasutajate arvutitest.
Failiõigused serverites konfigureeritud?
Kasutajad oma arvutites administraatori õigustes?

G. Rakendustarkvara

Rakendustarkvara uuendused ja turvapaigad.
Kes installeerib kasutajate rakendustarkvara?
Kasutajate juurdepääs kesksetele rakendustele vastavalt tööülesannetele?

H. Kasutajate turvateadlikkus

Uute töötajate IT-alane instrueerimine.
Turvareeglite meelde tuletamine aeg-ajalt.
Interneti kasutamine isiklikuks otstarbeks.

I. Protseduurid

Kas võrk, rakendused, serverid, konfiguratsioonid on piisavalt dokumenteeritud et uus IT inimene suudab selle suurema vaevata üle võtta?
Milline on tegevuskava, kui senise IT spetsialistiga midagi juhtub?
Millised on ohud mõne töötajaga töösuhte lõppemisel?
Kas (kuidas) oleks võimalik ettevõttelt raha, informatsiooni vms. välja petta?

J. Füüsiline turve

Kas arvutustehnikast on täielik nimekiri? Ülevaade peas?
Serverid – millised on turvameetmed?
Juurdepääs arvutitele väljast tulijal?
Akende ja uste lukustamine.
Sülearvuti kasutajate vastutus (mitte jätta valveta).

Lisa 2. Telgkodeerimine