Staða og viðhorf til öryggisstefnu og upplýsingaöryggis.
Könnun meðal íslenskra fyrirtækja á Íslandi

Maí 2011

Maríanna Magnúsdóttir

Ritgerð til

meistaraprófs (MSc) í rekstrarverkfræði

Staða og viðhorf til öryggisstefnu og upplýsingaöryggis. Könnun meðal íslenskra fyrirtækja á Íslandi

Maríanna Magnúsdóttir

Ritgerð til
meistaraprófs (MSc) í rekstrarverkfræði

Maí 2011

Staða og viðhorf til öryggisstefnu og upplýsingaöryggis. Könnun meðal íslenskra fyrirtækja á Íslandi.

Maríanna Magnúsdóttir

Ritgerð lögð fram við tækni- og verkfræðideild
Háskólans í Reykjavík til
meistaraprófs (MSc) í rekstrarverkfræði

Maí 2011

Leiðbeinandi

Ásrún Matthíasdóttir
Lektor, Háskólinn í Reykjavík

Prófdómari:

Kári Harðarson
Tölvunarfræðingur

Staða og viðhorf til öryggisstefnu og upplýsingaöryggis. Könnun meðal íslenskra fyrirtækja á Íslandi.

Maríanna Magnúsdóttir

Ritgerð lögð fram við tækni- og verkfræðideild
Háskólans í Reykjavík til
meistaraprófs (MSc) í rekstrarverkfræði

Maí 2011

Nemandi:

_____

Maríanna Magnúsdóttir

Leiðbeinandi:

_____

Ásrún Matthíasdóttir
Lektor, Háskólinn í Reykjavík

Prófdómari:

_____

Kári Harðarson
Tölvunarfræðingur

Undirritaðir hér með votta að þetta tiltekna meistaraverkefni sem ber titilinn **Staða og viðhorf til öryggisstefnu og upplýsingaöryggis: Könnun meðal íslenskra fyrirtækja á Íslandi,** unnið af **Maríönnu Magnúsdóttur** samræmist reglum og kröfum til meistaragráðu í rekstrarverkfræði við Tækni- og verkfræðideild Háskólans í Reykjavík.

Dagsetning: _____

Leiðbeinandi:

_____

Ásrún Matthíasdóttir
Lektor, Háskólinn í Reykjavík

Prófdómari:

_____

Kári Harðarson
Tölvunarfræðingur

.

Undirrituð veitir hér með Bókasafni Háskólans í Reykjavík heimild til að búa til eintak af þessu tiltekna meistaraverkefni sem ber titilinn **Staða og viðhorf til öryggisstefnu og upplýsingaöryggis: Könnun meðal íslenskra fyrirtækja á Íslandi** og lána eða selja slík eintök einungis í einka- , fræðilegum eða vísindalegum tilgangi.

Höfundur áskilur sér allan rétt á útgáfu þessa meistaraverkefnis á öðru formi en um er getið hér að ofan. Hvorki meistaraverkefnið né afrit af henni má nota til fjölföldunar án skriflegs leyfis höfundar.

Dagsetning: _____

Höfundur:

_____

Maríanna Magnúsdóttir

Meistarapróf í rekstrarverkfræði

Status and attitude towards security policies and information security. Survey amongst Icelandic organizations.

Maríanna Magnúsdóttir

May 2011

Abstract

Information is our most valuable asset in the modern society we live in and therefore a great reason to protect it. A security policy is meant to protect information assets from inner and outer threats of the environment anyhow they are intended, caused by failure or by accident. A survey amongst Icelandic organizations was performed to review status and attitude towards security policies and information security. Thirteen organizations participated in the survey and answered a questionnaire that was specially done for this cause. The results show that Icelandic organizations that process personal information or/and other perishables are conscious about information security and have a security policy documented. Majority of the participants that have already documented a security policy but are not certificated have chosen that they want to become certificated and plan to do so in near future. ISO/IEC 27001 is a national standard which declares all requirements for a Information security management system (ISMS). Presumptions for a security policy to work properly and bring desired success is the support from top officers and guarantors while executing the security policy. The best preventive of outsiders damaging information or destroying them is security awareness amongst employees.

Keywords – Security policy, Information security, Certification, ISO/IEC 27001, Information security management system (ISMS)

Staða og viðhorf til öryggisstefnu og upplýsingaöryggis. Könnun meðal íslenskra fyrirtækja á Íslandi.

Maríanna Magnúsdóttir

Maí 2011

Útdráttur

Upplýsingar eru verðmætustu eignir fyrirtækis í nútíma samfélagi og því góð ástæða til að huga vel að öryggi þeirra. Öryggisstefnu er ætlað að verja upplýsingaeignir fyrir innri og ytri ógnunum hvort sem að þær eru af ásetningi, vegna óhappa eða af slysni og stuðla að upplýsingaöryggi. Gerð var könnun meðal íslenskra fyrirtækja á Íslandi á stöðu og viðhorfi til öryggisstefnu og upplýsingaöryggis. Þrettán fyrirtæki tóku þátt og svöruðu spurningum af spurningalista sem gerður var sérstaklega fyrir þessa könnun. Niðurstöðurnar sýna fram á að íslensk fyrirtæki sem meðhöndla persónuupplýsingar og/eða aðrar viðkvæmar upplýsingar eru meðvituð um upplýsingaöryggi og marka öryggisstefnu. Meirihluti þeirra sem markað hafa öryggisstefnu og eru ekki nú þegar vottuð samkvæmt ISO/IEC 27001 hafa tekið þá ákvörðun að þeir vilji öðlast slíka vottun. ISO/IEC 27001 er alþjóðlegur staðall sem skilgreinir kröfur sem settar eru fyrir stjórnkerfi upplýsingaöryggis. Forsendur þess að öryggisstefna virki og beri tilætlaðan árangur er sýnilegur stuðningur yfirmanna og ábyrgðaraðila við framkvæmd stefnunnar. Besta forvörn fyrirtækis gegn utanaðkomandi aðilum sem kunna að valda tjóni eða eyðileggingu er öryggismeðvitund starfsfólks.

Lykilorð – Öryggisstefna, Upplýsingaöryggi, Vottun, ISO/IEC 27001, Stjórnkerfi

Efnisyfirlit

Myndaskrá

1 Inngangur

Þessi ritgerð er meistaraverkefni Maríönnu Magnúsdóttur í rekstrarverkfræði og var unnin á vorönn 2011 í Háskólanum í Reykjavík. Leiðbeinandi er Ásrún Matthíasdóttir lektor við Háskólann í Reykjavík. Tilgangur þessa verkefnis er að kanna stöðu og viðhorf til öryggisstefnu hvað varðar upplýsingaöryggi í íslenskum fyrirtækjum í dag. Spurningarnar sem leitast er við að svara eru:

- Munu einkarekin fyrirtæki sem ekki marka öryggisstefnu og framkvæma áhættumat lifa af í framtíðinni?
- Verður nauðsyn að öðlast vottun á sviði öryggis?
- Er framtíðin sú að öll fyrirtæki verði skyldug að vera með öryggisstefnu?
- Veitir öryggisstefna fyrirtækjum samkeppnisforskot?

Fyrst mun vera fjallað um aðalhugtök sem tengjast viðfangsefninu og eru hluti af grunnþekkingu til að öðlast skilning á öryggisstefnu, hvers vegna hún er mörkuð og innleidd. Síðan er fjallað um rannsóknina sem var gerð í tengslum við þetta meistaraverkefni og farið yfir niðurstöður hennar. Því næst koma umræður sem mynduðust í kjölfar rannsóknar. Þar á eftir eru tillögur lagðar fram og að lokum nefndir nokkrir punktar sem eru leiðbeinandi sem næstu skref í framhaldinu.

2 Hugtök og skilgreiningar

2.1 Hvað er öryggisstefna?

Upplýsingar eru verðmætustu eignir fyrirtækis í nútíma samfélagi og því góð ástæða til að huga vel að öryggi þeirra. Því verðmætari sem upplýsingarnar eru fyrir tiltekið fyrirtæki því meiri ástæða er til að huga að upplýsingaöryggi [1]. Upplýsingar geta verið á rafrænu formi, pappírs formi og/eða í formi eigna. Upplýsingar þurfa oft að fara í gegnum hendur á allnokkrum aðilum áður en þeim er að lokum eytt eða settar í framtíðargeymslu en ef þær komast í rangar hendur þá er voðinn vís. Þar kemur öryggisstefna til sögunnar. Öryggisstefnu er ætlað að verja upplýsingaeignir fyrir innri og ytri ógnunum hvort sem að þær eru af ásetningi, vegna óhappa eða af slysni [2]. Það er gert með því að marka tilgang, umfang, markmið og leiðir að markmiði og ábyrgð öryggisstefnunnar og innleiða síðan inn í fyrirtækið.

Samkvæmt lögum nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga ber öllum ábyrgðaraðilum eða vinnsluaðilum persónuupplýsinga skylda að útbúa og innleiða viðeigandi öryggisráðstafanir og hafa síðan eftirlit með framkvæmd þeirra. Í 11. grein laganna segir: „Ábyrgðaraðili skal skrá með hvaða hætti hann mótar öryggisstefnu, gerir áhættumat og ákveður öryggisráðstafanir“ [3]. Í reglum nr. 299/2001 um öryggi persónuupplýsinga eru nánari fyrirmæli um skyldur og hvernig ábyrgðaraðili skal haga málum sínum varðandi val á öryggisráðstöfunum útfrá mikilvægi og viðkvæmni upplýsinga. Í 3. grein segir að ábyrgðaraðili skuli setja sér skriflega öryggisstefnu og áhættumat [4]. Lagalega umhverfi öryggisstefnu er því nokkuð skýrt og innrammað viðfangsefni og er auðsótt í íslensku lagasafni.

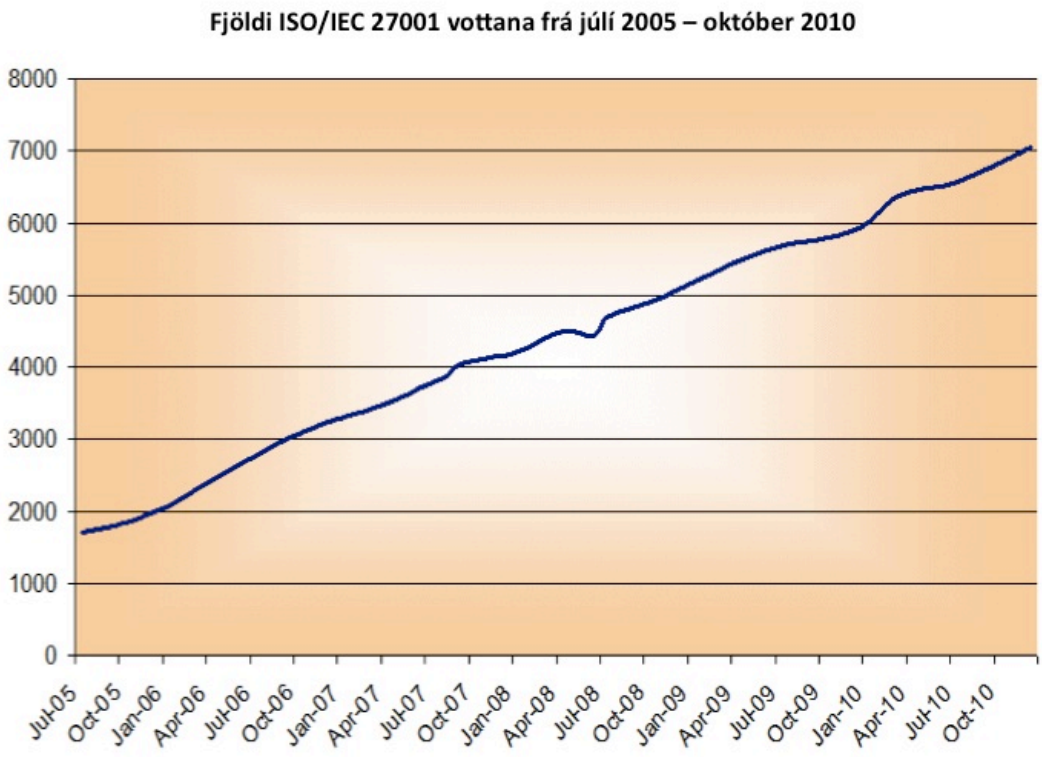
2.1.1 Vottun

Alþjóðlegi staðallinn ISO/IEC 27001 skilgreinir kröfur sem eru settar fyrir stjórnkerfi upplýsingaöryggis. Staðallinn hentar fyrirtækjum af öllum stærðargráðum því hægt er að heimfæra og aðlaga hann að hverju og einu fyrirtæki eftir því við hvað það er að fást og á hvaða sviði það starfar. Staðallinn er hannaður til að tryggja val á fullnægjandi stjórnkerfi sem sæmir stærð og umfangi hvers fyrirtækis. Staðallinn hentar þó sérstaklega vel þeim fyrirtækjum sem meðhöndla viðkvæmar upplýsingar og þurfa að vernda þær með einum eða öðrum hætti.

Til að fá gæðastimpil þarf fyrirtækið að fá vottun þess að það sé að framfylgja ISO/IEC 27001. Það er til dæmis breska staðlastofnunin, The British Standards Institution (BSI), sem vottar fyrirtæki á Íslandi. BSI er stærsti vottunaraðili í heiminum með viðskiptavini á borð við Vodafone, Sony og fleiri. BSI er með útibú um allan heim til að taka út og votta fyrirtæki og stuðlar þannig að bættum rekstri og stjórnun fyrirtækja. Markmiðið með þessu eftirliti er að lágmarka áhættu í meðferð og vinnslu upplýsinga. Með það að leiðarljósi er einfalt að sannfæra viðskiptavini að upplýsingar þeirra séu verndaðar. Einnig býður BSI upp á kennslu og þjálfun á verklagi við notkun gæðakerfa, prófun á vörum og framleiðslu og kynnir alþjóðlegar vinnuaðferðir svo að íslensk fyrirtæki geti staðið jafn framarlega og fyrirtæki út í heimi hvað varðar uppsetningu stjórnkerfis [5].

Fyrirtæki sem taka ákvörðun um að marka öryggisstefnu ganga í gegnum undirbúningsferli þar sem þau stilla upp stjórnkerfi upplýsingaöryggis og innleiða það. Í kjölfarið standa fyrirtæki frammi fyrir þeirri ákvörðun hvort að þau eigi að stefna að því að fá vottun samkvæmt ISO/IEC 27001 eða hvort að þau ætli einungis að nýta sér ramma staðalsins sem leiðarvísi. Þegar fyrirtæki stilla upp stjórnkerfi upplýsingaöryggis og innleiða það halda þau öllu jöfnu þeim möguleika opnum að öðlast vottun seinna þar sem það yrði lítil viðbótarvinna við þá vinnu sem hefur þegar átt sér stað.

Mynd 1 sýnir hvernig þróunin hefur verið í fjölda fyrirtækja sem hafa öðlast vottun samkvæmt ISO/IEC 27001 eða sambærilega vottun frá júlí 2005 til október 2010. Sjá má línulega aukningu í hverjum ársfjórðungi með örlítilli undantekningu í júlí 2008 [6].



Mynd 1: Fjöldi ISO/IEC 27001 vottana frá júlí 2005 - október 2010

Sé litið á kosti og galla þess að ganga alla leið og öðlast vottun samkvæmt ISO/IEC 27001 má sjá að kostirnir eru langt um fleiri en gallarnir og mun veigameiri. Svana Björnsdóttir er forstjóri Stika sem er ráðgjafa- og hugbúnaðarfyrirtæki sem sérhæfir sig í gagnaöryggi, tölvuöryggi og öryggismálum upplýsingakerfa. Hún tók saman niðurstöður úr viðhorfskönnunum og það sem fram hefur komið í samskiptum Stika og viðskiptavina varðandi ávinning þess að öðlast vottun og birti í grein á vefsíðu 12. nóvember 2009 [7] en þar segir:

„Viðskiptavinir okkar telja ávinning vottunar vera:

- Aukin og bætt ímynd og orðspor
- Meiri viðskipti
- Betri áætlanagerð
- Betri stjórnun
- Betri ferli
- Meira gagnsæi varðandi allar viðskiptalegar aðgerðir
- Aukin starfsánægja meðal starfsmanna

- Fleiri ánægðir viðskiptavinir
- Aukin nýting tíma og auðlinda
- Aukin afkastageta
- Skýrari boðleiðir
- Auðveldari samskipti
- Auðveldari og betri breytingastjórnun
- Skilvirkari vinna varðandi almenna eftirlitsaðila
- Færri mistök
- Lægri aukagjöld varðandi tryggingar
- Betra lánstraust“ [7]

Einnig kom fram að „Gagnrýnendur viðurkenndrar vottunar benda á að vottun krefst mikils ógagnlegrar og tímafrekrar skjölunarvinnu“ [7]. Það er því auðsýnilegt að kostirnir vega upp gallana á örskömmum tíma og niðurstaðan sú að mörkun öryggisstefnu hefur jákvæðar afleiðingar sem hafa varanleg jákvæð áhrif á rekstur fyrirtækis.

Vottun er algerlega valkvæður möguleiki og þróunin stefnir í að fleiri og fleiri fyrirtæki geri kröfu um að önnur fyrirtæki séu vottuð til að viðskipti geti átt sér stað og þá sérstaklega þau fyrirtæki sem er umhugað um meðferð viðkvæmra upplýsinga. ISO/IEC 27001 vottun á stjórnkerfi upplýsingaöryggis er dýrmætt skref fyrir fyrirtæki. Hún er skýr yfirlýsing til viðskiptavina, birgja, samstarfsaðila og yfirvalda um að fyrirtækið sé með öruggt stjórnkerfi upplýsingaöryggis [8].

2.1.2 Vottunarferlið

Til að fyrirtæki öðlist vottun á sviði upplýsingaöryggis þarf það að ganga í gegnum ákveðið ferli. Þetta ferli má skipta upp í fjögur veigamikil skref.

- Fyrsta skrefið er undirbúningur. Þetta skref kann að hljóma eins og einfalt verkefni en er í raun stærsti og erfiðasti hlutinn í ferlinu. Það þarf að þróa og útfæra stjórnkerfi fyrir hvert fyrirtæki, prufukeyra það og innleiða inn í alla verkferla sem eru notaðir innan fyrirtækisins, sama hvort að þeir séu

framkvæmdir dagalega eða einu sinni á ári. Þjálfa þarf starfsfólkið í að tileinka sér þessi tilteknu vinnubrögð og meta árangur eftir ákveðinn tíma og gera endurbætur ef þörf er á þeim [9].

- Þegar fyrirtækið telur að það hafi náð tilsettum árangri fer það í annað skref sem er að sækja um vottun. Sótt er um vottun til aðila á borð við BSI á Íslandi.
- Eftir undirritun á umsóknarblaðinu er komið að skrefi þrjú en í því felst úttekt á fyrirtækinu. Sérfræðingur frá vottunaraðila mun þá framkvæma lokaúttekt. Sé eitthvað ábótavant mun þessi sami sérfræðingur fara yfir öll þau atriði sem þarfnast athugunar áður en staðfesting á vottun getur farið fram.
- Í fjórða og síðasta skrefinu er svo staðfesting á vottun gegn því að fyrirtækið uppfylli allar kröfur sem farið er fram á af vottunaraðila. Útgefið vottunarskjal er afhent fyrirtækinu. Í kjölfar vottunar koma eftirlitsaðilar með reglulegu millibili og taka út fyrirtækið með það að markmiði að kerfið standist enn kröfur staðalsins. Vottun gildir í flestum tilfellum í 3 ár og er síðan endurútgefin ef fyrirtækið stenst allar kröfur [10].

Líta má á vottunarferlið sem verkefni og að launum fái fyrirtæki vottunarskjal. Verkefnið á sér þó engan eiginlegan endi þar sem umhverfi fyrirtækja er stöðugt að breytast og því þurfa stöðugar umbætur að eiga sér stað.

2.2 Stjórnkerfi upplýsingaöryggis

Stjórnkerfi upplýsingaöryggis (e. ISMS – Information security management system) snýst um hvernig fyrirtæki og stofnanir koma sér upp skipulögðum vinnubrögðum við umgengni um mikilvægar upplýsingar. Markmiðið með því að innleiða stjórnkerfi upplýsingaöryggis er að ramma inn verklag við rekstur með betri skjölun, lágmarka áhættu og bæta öryggi almennt jafnt í rekstri sem þjónustu. Stjórnkerfi fyrirtækja byggja flest á sama grunni en eru síðan aðlöguð hverju og einu fyrirtæki eftir eðli starfsemi þess. Sameiginlegur grunnur byggir á að skipulagi sé komið á kerfið, haldið sé um skjöl og skrár, kerfið sé reglulega endurskoðað, auðsýndur rekjanleiki, ábyrgð og hlutverk séu skýr og að stöðugt sé unnið að endurbótum á kerfinu.

Vel skipulagt stjórnkerfi byggir á eftirfarandi atriðum:

- Aðstoðar fyrirtækið við að kortleggja veikleika í kerfum og ferlum
- Stuðlar að betri yfirsýn fyrir stjórnendur á rekstri upplýsingakerfa og öryggismála
- Upplýsir starfsmenn og eykur öryggismeðvitund
- Eykur skilvirkni í verkferlum og skjölun sem bætir rekstur og rekstraröryggi

[11]

Til uppbyggingar á stjórnkerfi upplýsingaöryggis er hægt að notast við tól sem nefnist PDCA módel [12] en skammstöfunin stendur fyrir ensku orðin ***p**lan, **d**o, **c**heck* og ***a**ct*. Sé þetta heimfært á íslenska tungu nefnast fasarnir fjórir: *Skipuleggja, Framkvæma, Gáta, Aðhafast*. Þetta tiltekna módel kemur úr heimi gæðamála og er nytsamlegt við að leysa og/eða sinna endurbótum á verkefnum.

Skipuleggja (e. Plan) – Skipuleggja þarf hvernig á hvaða máta og á hvaða formi skal setja upp stjórnkerfið, þ.e. markmið, verkferla og verklagsreglur.

Framkvæma (e. Do) – Innleiða þarf stjórnkerfið í alla verkferla fyrirtækisins og menningu þess. Hér skiptir leiðtogahæfni stjórnenda miklu máli til að starfsmenn fyrirtækisins tileinki sér verklag og aðferðir nýs stjórnkerfis með skilvirkum hætti.

Gáta (e. Check) – Eftir innleiðingu þarf að athuga hvort að hún hafi tekist sem skildi og hvort að hún skili tilskildum árangri. Í þessum fasa er stjórnkerfið því rýnt og niðurstöðum komið til stjórnenda.

Aðhafast (e. Act) – Eftir að niðurstöður hafa að verið rýndar þarf að setja í gang endurbótaverkefni. Eðlilegt er að það taki stjórnkerfið nokkurn tíma að komast í gott horf. Því er regluleg rýni og úrbætur á athugasemdum sem samræmast stefnu fyrirtækisins mjög veigamikill þáttur í ferlinu.

PDCA módelið hefur verið notað frá því árið 1950 af Japönum til að bæta gæði á vörum og þjónustu. Jens J. Dahlgaard, Kai Kristensen og Gopal K. Kanji skrifuðu grein um altæka gæðastjórnun (e. Total Quality management) og nefndu PDCA módelið sem gott verkfæri leiðtoga og stjórnenda við innleiðingu á gæðastjórnunarkerfi. Þeir sýndu einnig fram á að hægt væri að nota PDCA módelið við stöðugar umbætur (e. Continuous improvement) en módelið er hægt að aðlaga að hverju því verkefni sem það fæst hverju sinni [13].

2.3 Áhættumat

Áhættumat (e. Risk assessment) er framkvæmt reglulega innan fyrirtækja til að leggja mat á þær hættur og ógnanir sem steðja að upplýsingum fyrirtækja. Metið er hvaða áhrif það kann að hafa ef tiltekin hætta eða ógn á sér stað, hversu líklegt það er að það gerist og hversu viðkvæmur rekstur fyrirtækisins er fyrir henni. Dæmi um hættu eða ógn er að utanaðkomandi aðili komist í viðkvæm gögn, breyti þeim eða á annan hátt raskar öryggi þeirra. Með því að kortleggja hvaða hættur og ógnanir eru í innra og ytra umhverfi fyrirtækis er hægt að haga öryggismálum og öryggisferlum þannig að allar ákvarðanir séu byggðar á réttum forsendum út frá niðurstöðu áhættumats.

Áhættumat felur í sér að koma upp á yfirborðið öllum þeim atriðum sem kunna að hafa áhrif á öryggi þeirra kerfa sem fyrirtækið notar. Áhættumat nær yfir *upplýsingaeignir, öryggisáhættu, áhættuviðmið og afgangsáhættu*.

> **Upplýsingaeignir** (e. Information asset) teljast vera allar þær eignir sem koma við sögu við rekstur fyrirtækis hvort sem þær eru áþreifanlegar eða óáþreifanlegar.
>
> **Öryggisáhætta** (e. Security risk) er sú áhætta sem beinist að öryggi upplýsingaeigna og er aðallega metin útfrá fjórum atriðum: (1) hversu alvarlegar ógnanir eru sem steðja að eignum, (2) útfrá virði eigna, (3) hversu miklar líkur eru á að ógn verði að veruleika og (4) hversu viðkvæmar eignir eru fyrir tiltekinni ógn. Öryggisáhættu má lágmarka með því að gera viðeigandi ráðstafanir sem minnka líkur á að ógnanir verði að veruleika og/eða gera eignir minna viðkvæmar gegn ógnunum.
>
> **Áhættuviðmið** (e. Risk benchmarks) er sú áhætta sem stjórnendur telja ásættanlega í rekstri.
>
> **Afgangsáhætta** (e. Residual risk) er áhætta sem stjórnendur telja að ekki sé hægt að mæta þrátt fyrir að gera ráðstafanir gegn henni [14].

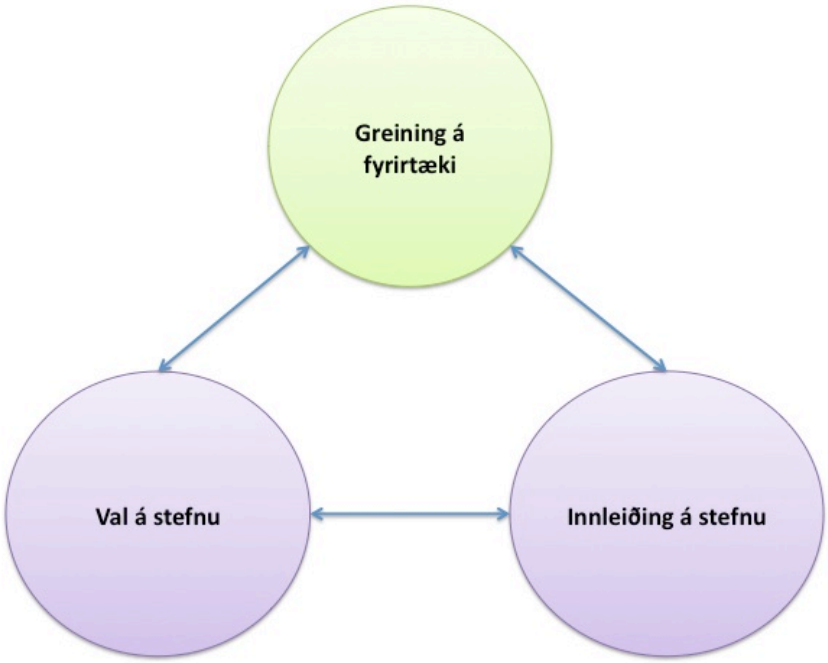
Glenn Koller er höfundur hagnýtrar handbókar um áhættumat og ákvarðanatöku. Hann viðurkennir að það tók hann mörg ár að átta sig á því að áhættumat væri

ákveðið ferli. Það krefst mikils undirbúnings að hanna áhættumódel sem nær að meta allar þær hættur og ógnir sem steðja að starfsemi fyrirtækis. Tæknileg atriði á borð við að velja hugbúnað og hanna áhættumódel eru smávægilegir þættir ferilsins samanborið við vistvæna, pólitíska, samskipta og menntunar þætti sem þarf að huga að við innleiðingu áhættumats í fyrirtæki. Koller vekur athygli á því að áhættumat skilar ekki hámarks ávinning sé það einungis notað í eitt verkefni eða af einu teymi heldur þarf að innleiða það í heildina til að fá sem mestan árangur. Líta skal á áhættumat og áhættumódel sem hjálpargagn sem stöðugt metur verkefni eða tækifæri með áherslu á samanburð og kanna stöðu í heild sinni. Hann varar við því að hanna of ítarlegt áhættumódel því þá eru líkur á að tapa heildaryfirsýn á fyrirtækinu. Einfeldni er fýsilegasti kosturinn við að hanna áhættumódel og styðjast skal við að hanna módelið svo að það nái til allra vídda fyrirtækisins svo að það geti spáð fyrir um alla mögulega atburði sem kunna að eiga sér stað [15].

2.4 Stefnumótun

Johnson og Scholes skilgreina **stefnumótun** (e. Strategy) í bókinni sinni Exploring Corporate Strategy sem leiðarvísi og umfang fyrirtækis til langs tíma sem veitir fyrirtækinu samkeppnisforskot með því að nýta þær auðlindir sem það hefur til umráða í krefjandi starfsumhverfi til að mæta þörfum markaðar og uppfylla væntingar hluthafa fyrirtækis [16]. Með öðrum orðum er stefnumótun notuð til að átta sig á hvert fyrirtækið ætlar sér og hvernig það ætlar að komast þangað. Hún felur í sér að fyrirtæki velja á hvaða markað þau ætla að einblína og hvernig þau ætla að eiga við og bregðast við samkeppnisaðilum. Stefnumótun sýnir fram á hvaða auðlindir fyrirtækið þarf að hafa til umráða til að geta haldið stefnu sinni (hæfni, eignir, fjármál, tengsl, tækni, aðstaða) og greinir ytra og innra umhverfi fyrirtækisins. Stefnumótun fyrirtækja er ávallt byggð upp með ávinning og hagsmuni hlutahafa að leiðarljósi [16].

Mynd 2 hér að neðan sýnir þrjá aðalþætti stefnumótunarferilsins en þeir eru **greining á fyrirtæki** (e. Strategic analysis), **val á stefnu** (e. Strategic choice) og **innleiðing á stefnu í fyrirtæki** (e. Strategy implementation).



Mynd 2: Þrír aðalþættir stefnumótunarferils [16]

Í greiningu á fyrirtæki eru innri og ytri þættir skoðaðir til þess að kortleggja hvar styrkleikar, veikleikar, ógnanir og tækifæri liggja og hvernig þessir þættir hafa áhrif á rekstur fyrirtækisins. Fjöldi tækja og tóla er hægt að nota til að aðstoðar við greiningu á fyrirtæki til dæmis SVÓT greiningu, PESTLE greiningu og markaðshlutun.

SVÓT greining (e. SWOT analysis) er veigamikill þáttur í stefnumótun þar sem hún aðstoðar við að kortleggja stöðu fyrirtækis í dag svo hægt sé að segja til um hvert eigi að stefna. Skammstöfunin SVÓT stendur fyrir **S**tyrkleikar, **V**eikleikar, **Ó**gnanir og **T**ækifæri. Einföld SVÓT greining felur í sér að skoða almenna umhverfið, nær umhverfið og innra umhverfið. Almenna umhverfið nefnist öðru nafni ytra umhverfi fyrirtækis og snýr að pólitískum, efnahagslegum, félagslegum, tæknilegum og lagalegum þáttum þess. Í nær umhverfi má finna aðila á borð við birgja, verkalýðsfélög, samkeppnisaðila og viðskiptavini. Í innra umhverfi er svo allt það sem snýr eingöngu að fyrirtækinu innanhúss, þ.e.a.s. skipulag fyrirtækis, markaðsmál, fjármál, starfsmannamál og verðmætasköpun.

Gagnlegt þykir að stilla upp einföldu líkani þannig að gerður er einn dálkur fyrir hvern þátt SVÓT (styrkleika, veikleika, ógnanir, tækifæri) greiningar og atriði skráð í

þá dálka eftir því sem við á. Til að fá betri mynd á raunstöðu er hægt að raða öllum atriðunum niður eftir mikilvægi og jafnvel gefa þeim einkunn þannig að mesti styrkleiki fyrirtækis væri til dæmis skráður efst í dálknum *Styrkleikar* [17].

PESTLE greining (e. PESTLE analysis) skoðar eingöngu ytra umhverfið eða almenna umhverfið en skammstöfunin miðast við ensku heitin **P**olitical, **E**conomical, **S**ocial, **T**echnological, **L**egal, **E**nvironmental eða á íslensku *pólitíska, efnahagslega, félagslega, tæknilega, lagalega og umhverfislega umhverfið* [17]. Þá eru skoðaðir þeir þættir eða þær breytur sem geta haft bein eða óbein áhrif á fyrirtækið og kannað hversu næmur rekstur fyrirtækis er fyrir þessum breytum. Suma þætti er ekki hægt að fyrirbyggja en í öðrum tilfellum eru gerðar áætlanir til að fyrirbyggja að ákveðin breyta muni hafa tilsett áhrif á fyrirtækið eða í það minnsta að draga úr áhrifunum sem hún kann að valda.

Stefna er valin í samræmi við væntingar hluthafa, hagsmuni þeirra og hvernig fyrirtækið ætlar að ná markmiðum sínum. Fyrirtæki getur til dæmis verið með þjónustustefnu með áherslu á lágt vöruverð og meðal gæði og getur þar af leiðandi náð markmiðum sínum í að verða með mestu markaðshlutdeild á sínu sviði. Innleiðing stefnu í fyrirtæki er oft erfiðasti hluti stefnumótunarferilsins og krefst þess að stjórnendur séu leiðtogar og byggi upp ákveðna menningu innan fyrirtækisins í takt við stefnu fyrirtækisins og hagsmuni hluthafa [16].

Það má því sjá að stefnumótun er veigamikið ferli þar sem fyrirtæki greinir stöðu sína í dag, hvert það vill komast og hvernig það ætlar að komast þangað. Ýmis tól er hægt að nota sér til aðstoðar við greininguna og val á stefnu en við innleiðingu hennar skiptir leiðtogahæfni og mannleg samskipti miklu máli svo að hún sé innleidd á réttan hátt og beri árangur.

2.5 Verkferlar og verklagsreglur

Uppbygging stefnu á borð við gæðastefnu eða öryggisstefnu er á þann veg að stefnan sjálf gefur heildarmyndina, hvert fyrirtækið stefnir og hvaða markmiðum það vill ná. Undirliggjandi er stjórnkerfi sem notað er til að koma fyrirtækinu á þann stað sem stefnan kveður á um og halda utan um *verklagsreglur* og *verkferla* [18].

Verklagsreglur (e. Procedure policy) eru skráðar og samþykktar aðferðir við að framkvæma skrefin í tilteknum atburði, starfsemi eða ferli. Verkferlar og verklagsreglur geta bæði verið á skriflegu og myndrænu formi og á hvers kyns gerðum miðla. Samkvæmt alþjóðlega staðlinum ISO/IEC 9001:2005 þá merkir skjalfest verklagsregla það að verklagsreglu hefur verið komið upp, hún skjalfest, innleidd og henni haldið við með reglulegri rýni [18].

Verkferlar (e. Work process) sýna fram á hvernig tiltekinn atburður er unninn skref fyrir skref. Samkvæmt íslenskri orðabók er verkferill skilgreindur sem „það hvernig verk er unnið eða hlutur framleiddur, greinargerð um hver vinnur hvað, hvenær og hvernig, við ákveðna framleiðslu“ [19] (Mörður Árnason, 2002, bls. 1730).

Samkvæmt þessum skilgreiningum má sjá að verklagsregla segir *hvað* skal gera og verkferlarnir koma í kjölfarið og segja *hvernig* skal framkvæma það. Ferlarnir og reglurnar í til dæmis öryggisstefnu eru byggðar upp með gæði og öryggi að leiðarljósi og að lokum sett saman í eina handbók sem er aðgengileg starfsfólki. Í grunninn eru fyrirtæki með svipuð ferli og reglur sem byggjast á ISO/IEC 9001 og/eða ISO/IEC 27001 og síðan bætast við sértæk verkferli og verklagsreglur hvers fyrirtækis.

2.6 Persónuupplýsingar

Allsstaðar í kringum okkur er verið að meðhöndla persónuupplýsingar fólks og fer magn þeirra ört vaxandi. Þessar upplýsingar eru misjafnlega viðkvæmar og því þarf að vera til rammi sem heldur utan um hvernig meðferð persónuupplýsinga skal háttað. Lög um persónuvernd og meðferð persónuupplýsinga nr. 77/2000 má finna í Lagasafni og/eða á heimasíðu Alþingis www.althingi.is. Þau tóku gildi 1. janúar 2001 og var síðast breytt 1. janúar 2011. Til að hafa eftirlit með framkvæmd þess sem lögin kveða á um er rekin stofnunin Persónuvernd. Reglur nr. 299/2001 um öryggi persónuupplýsinga og nr. 712/2008 um tilkynningarskylda og leyfisskylda vinnslu persónuupplýsinga sem finna má hjá Persónuvernd eru notaðar samhliða lögum um persónuvernd og meðferð persónuupplýsinga.

Hugtakið persónuupplýsingar er lítið afmarkandi þegar það kemur fram eitt og sér og segir ekki nákvæmlega til um hverskonar upplýsingar flokkast sem slíkar. Í 2. gr. laga nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga er hugtakið persónu-upplýsingar skilgreint sem: „Sérhverjar persónugreindar eða persónugreinanlegar upplýsingar um hinn skráða, þ.e. upplýsingar sem beint eða óbeint má rekja til tiltekins einstaklings, látins eða lifandi“ [3]. Það eru því margskonar upplýsingar um einstaklinga sem ber að verja gegn því að komast í hendur óprúttinna aðila sem geta valdið tjóni.

Í vinnuumhverfi fyrirtækis er að mörgu að hyggja til að vernda persónuupplýsingar. Lewis Schiff ráðgjafi ræddi þetta í grein sem var birt í mars 2011 [20]. Þar kemur fram nauðsyn þess að huga vel að öryggi persónuupplýsinga og taka inn í allar áhættur. Á svipstundu getur traust sem fyrirtæki hefur eytt miklum tíma í að byggja upp meðal viðskiptavina sinna brotnað. Ein lítil mistök geta orðið til þess að fleiri hundruð viðskiptavina efist um traust sitt gagnvart tilteknu fyrirtæki sem getur leitt til þess að það missir viðskipti.

Mistökum við að verja persónuupplýsingar má skipta upp í þrennt: *gagnabrot, gagnabirting og gagnatap*.

Gagnabrot (e. Data breach) teljast vera brot á borð við þegar tölvuþrjótar öðlast aðgang að tölvukerfi fyrirtækis, halað er niður hugbúnaði sem er dulkóðaður vírus sem hannaður er til að ná haldi á gögnum og að starfsmenn eru plataðir til að gefa upp persónuupplýsingar til utanaðkomandi aðila.

Gagnabirting (e. Data exposure) getur óvart á sér stað þegar sendur er tölvupóstur á rangan aðila með viðkvæmum persónuupplýsingum, persónuupplýsingar eru settar á samfélagsvef eða heimasíðu og/eða tölvubilun eða mannleg mistök gefa upp viðkvæm gögn. Einnig eru gögn óvarin ef þau eru skilin eftir á glámbekk svo aðrir geti séð sem og gögn sem fleygt er í ruslafötu án þess að vera tætt eða eyðilögð.

Gagnatap (e. Data loss) verður þegar til dæmis fartölvum, borðtölvum, netþjónum, USB lyklum, geisladrifum og/eða snjallsímum er stolið eða glatað [20].

Einar Árnason ræddi í grein sinni Persónugreining í gagnagrunni á heilbrigðissviði [21] sem kom út árið 2001 hversu mikilvægt það er fyrir fámenna þjóð eins og Íslendinga að vernda persónuupplýsingar þar sem auðvelt er að rekja upplýsingar sökum smæðar t.d. með ættartrjám. Þrátt fyrir að dulkóðun hafi átt sér stað þá eru til svokallaðir lyklar sem nota má til að persónugreina einstaklinga í gagnagrunni. Með því að bera saman mynstur ættartrjáa úr ættargrunni með dulkóðuðum fastanúmerum og ættargrunni með kennitölum eða nöfnum er hægt að smíða lykil að grunninum og rekja þannig persónuupplýsingar. Einnig er hægt að persónugera einstaklinga af samhengi almennra upplýsinga. Einar nefndi einnig einfalt reikningsdæmi til að persónugreina einstaklinga. Meðalfjöldi fæðinga á ári á Íslandi væri rúmlega 4.200 (tala frá 2001). Daglega væru þá að meðaltali 11-12 fæðingar og fáir dagar með fleiri en 20 fæðingar. Einungis með þessa vitneskju og upplýsingar um fæðingardag og ár er búið að þrengja hringinn niður í 20 manns hið mesta. Með því að vita einnig kynið er hringurinn búinn að helmingast niður í 10 manns þar sem að meðaltali fæðast sex stúlkur eða drengir á dag og aldrei fleiri en tíu. Með því að bæta við hæð og búsetu eða augnlit er nánast öruggt að hægt er að bera kennsl á flesta eða alla einstaklingana sem eftir eru. Einar bendir á að þessar upplýsingar eru allar hægt að nálgast í vegabréfi einstaklinga og teljast sem almennar upplýsingar en ef einstaklingar bera með sér sértækar upplýsingar á borð við að vera með sjúkdóm eða augljós persónueinkenni þá er enn og auðveldara að persónugreina viðkomandi [21].

2.7 Skilgreining fyrirtækja

Hægt er að skilgreina fyrirtæki á marga vegu þ.e.a.s. eftir stærð, starfssviði og formi rekstrar. Á Íslandi tíðkast að flokka fyrirtæki sem einkarekin fyrirtæki eða fyrirtæki rekin af hinu opinbera. Hér verður einungis fjallað um einkarekin fyrirtæki þar sem þátttakendur í rannsókn (sjá kafla 3.1) eru öll einkarekin fyrirtæki. Skilgreiningar á borð við sprotafyrirtæki hafa rutt sér til rúms síðustu áratugi við aukna nýsköpun og þá sérstaklega eftir hrun í íslensku efnahagslífi 2008.

Á heimasíðu Samtaka iðnaðarins skilgreinir Ferdinand Hansen sprotafyrirtæki:

> „Sprotafyrirtæki eru venjulega sprottin upp úr rannsókna eða- þróunarverkefnum einstaklinga, þróunarhópa, háskóla, rannsóknarstofnana eða annarra fyrirtækja og byggjast á sérhæfðri þekkingu, tækni eða öðru nýnæmi. Gengið er út frá því viðmiði að árlegur þróunarkostnaður sprotafyrirtækja sé að jafnaði yfir 10% af veltu. Fyrirtæki hættir að teljast sprotafyrirtæki þegar það hefur verið skráð í kauphöll sem öflugt tæknifyrirtæki eða náð árlegri veltu sem nemur einum milljarði íslenskra króna“ [22].

Dr. Björn Þór Jónsson fjallar um í grein sinni í tímaritinu Tölvumál sem kom út í nóvember 2009 að hægt væri að skipta sprotafyrirtækjum í upplýsingatækniiðnaði í tvo flokka. Annan flokkinn skipa þau fyrirtæki sem hafa bætt þekkta tækni á einhvern hátt og hinn flokkinn skipa fyrirtæki sem eru að koma nýrri tækni á framfæri. Fyrirtæki sem hafa bætt þekkta tækni byggja að mestu á frumkvöðlum og tæknimenntuðum einstaklingum og nýta sér oftar en ekki opinbera sjóði eins og Tækniþróunarsjóð og Nýsköpunarsjóð til að aðstoða sig við fjármögnun fyrirtækisins. Fyrirtæki sem eru að koma nýrri tækni á framfæri geta þurft að leggja mikið á sig áður en þau verða hagnýt og fara að skila árangri en það tekur yfirleitt margra ára rannsóknar- og þróunarstarf [23].

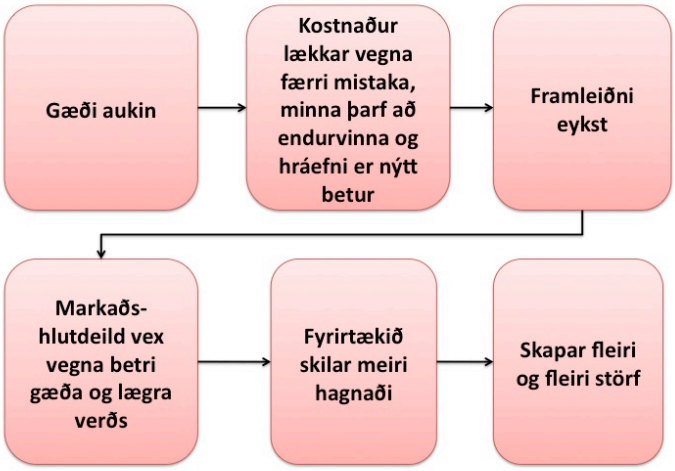
Þegar fyrirtæki hefur náð einum milljarði í ársveltu hefur það færst af vaxtastigi og yfir á þroskað stig á æviskeiði fyrirtækja og þar með ekki lengur skilgreint sem sprotafyrirtæki. Það getur hinsvegar valdið misskilningi að kalla slík fyrirtæki þroskuð fyrirtæki þar sem sprotafyrirtæki geta einnig verið mjög þroskuð. Hugtakið þroskað fyrirtæki kemur útfrá beinþýðingu úr ensku yfir á íslensku á *mature organization* en það væri nærri lagi að kalla þessi tilteknu fyrirtæki „fullmótuð fyrirtæki“ eða „mótuð fyrirtæki“.

2.8 Náið samband gæða- og öryggismála

Gæðastjórnun er þekkt fyrirbæri. Mögulegt er að fyrirtækjum þyki erfitt að fylgja þessum fræðum en tilgangurinn með gæðastjórnun er að vera einföld, leiðbeinandi og upplýsandi fyrir stjórnendur, starfsfólk, viðskiptavini og þannig að þessir aðilar þekki til hlítar ábyrgð, hlutverk, væntingar og kröfur hvers annars. Á heimasíðu Samtaka iðnaðarins skilgreinir Ferdinand Hansen hugtakið gæðastjórnun. „Gæðastjórnun á að kalla fram öguð vinnubrögð þar sem stjórnendur og starfsmenn horfa með fyrirhyggju

til lengri tíma í stað þess að eyða kröftum sínum í að vinna úr málum sem komin eru í óefni vegna lítils eða lélegs undirbúnings“ [24].

Gæðasérfræðingurinn William Edwards Deming fjallar í bók sinni Out of the Crisis um keðjuverkun sem á sér stað þegar innleidd er gæðastjórnun. Á Mynd 3 má sjá þessa keðjuverkun á myndrænu formi. Ef gæði eru aukin, lækkar kostnaður vegna færri mistaka. Vegna færri mistaka þarf ekki endurvinna hlutina jafn oft og hráefni nýtast mun betur. Við þetta eykst framleiðni og markaðshlutdeild sem skilar sér í meiri hagnaði [25].



Mynd 3: Keðjuverkun Demings [26]

Sé þessi keðjuverkun borin saman við það sem kom fram í kafla 2.1.1 þar sem fjallað var um vottun sést að ferlið er það sama þegar mörkuð er öryggisstefna, hún innleidd og öðlast vottun. Við aukið öryggi lækkar kostnaður vegna færri mistaka, afkastageta eykst og tími og auðlindir nýtast mun betur sem skilar sér í meiri viðskiptum. Það má því segja að gæði og öryggi vinni sambærilegt starf við innleiðingu þeirra.

Ferdinand Hansen bætir við á heimasíðu Samtaka iðnaðarins:

> „Margir halda að gæðastjórnun sé eingöngu fyrir stór fyrirtæki og sé alltof umfangsmikil til að henta litlum fyrirtækjum. Staðreyndin er hinsvegar sú að það er ekki réttlætanlegt að lítil fyrirtæki séu verr rekin en þau stóru og umfang gæðastjórnunar ætti alltaf að vera í beinu hlutfalli við stærð og rekstrarumfang fyrirtækisins. Gæðastjórnun er ekki heldur bundin við ákveðna tegund rekstrar og á við hvort heldur er um að ræða framleiðslu, þjónustu eða félagasamtök“ [24].

Það sama má segja um öryggisstefnur fyrirtækja. Þær henta í öllum þeim fyrirtækjum sem meðhöndla persónuupplýsingar og/eða viðkvæmar upplýsingar hvort sem þau eru stór eða smá. Árangur gæðastjórnunar og öryggisstefnu er áþekkur en bæði skila árangri í betri rekstrarafkomu og bættri samkeppnishæfni.

John S. Oakland lýsir í bók sinni Total Quality management sjö þrepa feril við innleiðingu gæðastjórnunar. Til að ná sem bestum árangri við innleiðingu gæðastjórnunar telur hann að stjórnendur þurfi að fylgja eftirfarandi ferli í réttri röð:

1. Sannfæra yfirstjórnendur fyrirtækis um ávinning gæðastjórnunar og fá þá í lið með sér.
2. Útbúa framtíðarsýn fyrirtækis
3. Skilgreina markmið
4. Greina fyrirtækið, skoða innri og ytri áhrifaþætti
5. Skrá öll ferli fyrirtækisins og ákveða hver ber ábyrgð á hverjum ferli
6. Sundurliða öll ferli í greinargóða verkþætti
7. Fylgjast með umbótaferlum og bregðast við þeim erfiðleikum sem kunna að koma upp við breytinguna.

[27]

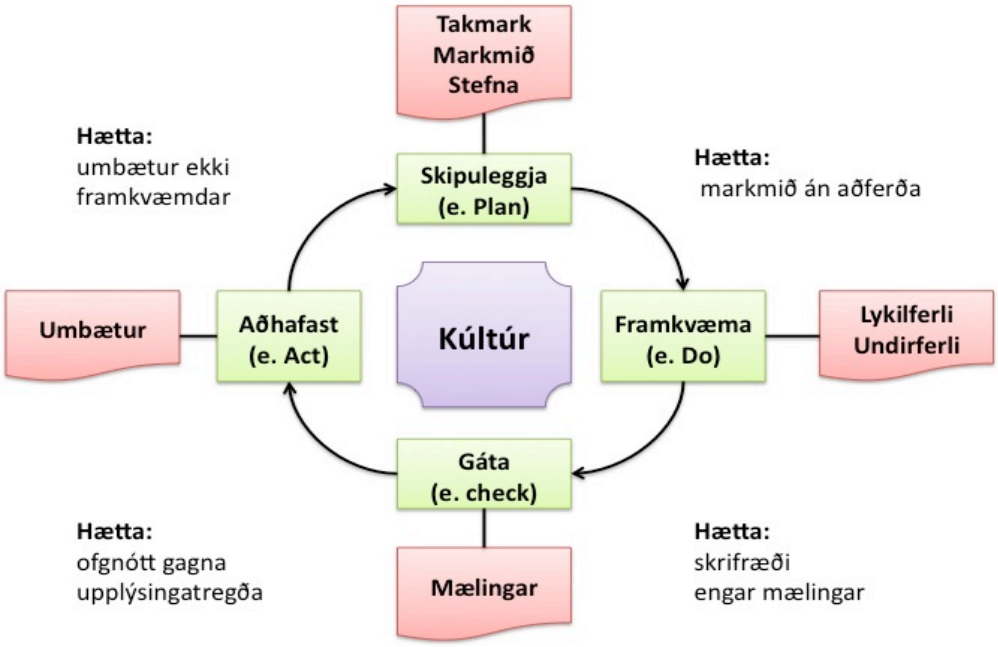
Hvernig gæðastjórnun er innleidd skiptir miklu máli.

Mynd 4 sýnir hvernig þessi innleiðing gæðastjórnunar er í samræmi við PDCA módelið sem kynnt var í kafla 2.2. Þetta ferli styður við þá sem vilja innleiða gæðastjórnun og þeir sem kjósa að fara þessa leið við innleiðingu gæðastjórnunar eru ólíklegir til að tapa yfirsýn á hugmyndafræði gæðastjórnunar og verða þrælar skrifræðislegs gæðakerfis [26].

PDCA módelið er tól sem hægt er að nota við allskyns verkefni, aðstæður og innleiðingar eins og fram kom í kafla 2.2. Í einfölduðu máli má segja að hvert verkefni mun verða árangursríkara ef vel er að því staðið, gerð er áætlun en upphafið er góður undirbúningur og skipulag (P). Þá eru takmörk, markmið og stefna ákvörðuð. Eftir góðan undirbúning þarf að framkvæma tiltekna atburði og athafnir og beita skilgreindum aðferðum til að ná markmiðum samkvæmt áætlun (D). Því næst þarf að

athuga hvort að verkefnið hafi náð tilskildum árangri með mælingum (C). Að lokum þarf að rýna í niðurstöður og bregðast við með því að útbúa umbótaverkefni ef

niðurstöðurnar eru ekki í samræmi við væntingar (A) [13]. Við gerð umbótaverkefnis byrjar PDCA hringrásin upp á nýtt og er þar með í stöðugri notkun. Á Mynd 4 má sjá þær hættur sem kunna að vera í hverjum fasa PDCA módelsins sem geta valdið truflunum við notkun þess.



Mynd 4: Innleiðing gæðastjórnunar með PDCA módelinu [26]

Með gæðastjórnun sem grunn í rekstri fyrirtækis er auðvelt og lítil fyrirhöfn að bæta við öryggiskröfum hvað varðar upplýsingaöryggi samkvæmt ISO/IEC 27001. Hægt er að tala um gæðastjórnun eitt og sér en sjaldnast er talað einungis um öryggisstefnur, yfirleitt er þessu tvinnað saman og sett undir eina og sama hattinn sem gæða- og öryggismál.

3 Aðferð

Til að kanna stöðu og viðhorf í íslenskum fyrirtækjum á upplýsingaöryggi og mörkun öryggisstefnu var gerð spurningakönnun. Spurningarnar voru hannaðar með það að leiðarljósi að svara rannsóknarspurningum sem lagðar fram í upphafi. Spurningarnar sem leitast er við að svara eru:

- Munu einkarekin fyrirtæki sem ekki marka öryggisstefnu og framkvæma áhættumat lifa af í framtíðinni?
- Verður nauðsyn að öðlast vottun á sviði öryggis?
- Er framtíðin sú að öll fyrirtæki verði skyldug að vera með öryggisstefnu?
- Veitir öryggisstefna fyrirtækjum samkeppnisforskot?

3.1 Þátttakendur

Í úrtaki rannsóknarinnar eru þrettán íslensk fyrirtæki en þýðið eru öll einkarekin íslensk fyrirtæki sem meðhöndla persónuupplýsingar og/eða aðrar viðkvæmar upplýsingar sem ekki mega komast í hendur almennings. Haft var samband við 44 fyrirtæki með von um að fá að koma í viðtal en þrátt fyrir margar tilraunir og ítrekanir náðist aðeins samband við þrettán fyrirtæki. Svarhlutfallið er því 29,5%. Fyrirtækin sem voru þátttakendur í rannsókninni eru í stafrófsröð: Arionbanki, Betware, Blóðrannsóknarstofa í Glæsibæ, Borgun, Creditinfo, Eimskip, Init, Parlogis, SagaSystem, Skýrr, Valitor, Vátryggingafélag Íslands og Vodafone.

Allt eru þetta fyrirtæki sem starfa á ólíkum sviðum og meðhöndla persónuupplýsingar og/eða viðkvæmar upplýsingar sem ekki mega komast í hendur almennings.

3.2 Mælitæki

Spurningalistinn var hannaður af höfundi ritgerðarinnar og samanstóð af sjö aðalspurningum en heildarfjöldi spurninga var 27. Þriðja spurningin er umfangsmikil og eru tvennskonar sett af spurningum sem fylgja eftir því hvort svarað er játandi eða neitandi. Aðal munur á fjölda spurninga á hvert fyrirtæki felst í svari þeirra við aðalspurningu númer 3, "Er öryggisstefna til staðar hjá fyrirtækinu?". Sé henni svarað játandi þá er heildarfjöldi spurninga 19 en sé svarað neitandi þá er heildarfjöldi spurninga 14 talsins. Aðalspurningarnar sjö voru:

1. Á hvaða sviði starfar fyrirtækið?
2. Fyrirtækið flokkast sem: sprotafyrirtæki eða þroskuð fyrirtæki
3. Er öryggisstefna til staðar hjá fyrirtækinu?
4. Á fyrirtækið í samskiptum við erlend fyrirtæki?
5. Í hverskonar starfsemi telur þú að í framtíðinni þurfi að vera mörkuð öryggisstefna til að geta lifað og dafnað á markaði?
6. Í hverskonar starfsemi telur þú að ætti að vera skylda að marka öryggisstefnu?
7. Telur þú að það skapi samfélaginu traust að fyrirtæki marki öryggisstefnu?

Spurningalistann í heild sinni er hægt að skoða í Viðauka A þar sem nánari sundurliðun á spurningum er sýnd.

3.3 Framkvæmd

Viðtöl við fyrirtækin þrettán fóru fram dagana 4. – 18. mars 2011. Farið var í heimsóknir til hvers og eins fyrirtækis þar sem var bókaður fundur með ýmist framkvæmdastjóra, öryggis- og/eða gæðastjóra eða verkefnastjóra öryggismála. Viðtölin voru hálfopin þar sem fyrst var spurningalistanum svarað sem tók að meðaltali 15,1 mínútur og í kjölfarið mynduðust umræður og því var hvert viðtal að meðaltali 26,4 mín að lengd.

Spurningalistinn var upphaflega settur upp í Excel en var síðan yfirfærður í vefforritið www.freeonlinesurveys.com til nánari tölfræðilegrar og myndrænnar úrvinnslu. Teknir voru niður skriflegir punktar varðandi umræður sem mynduðust í hverju

viðtali fyrir sig og þeir hafðir samhliða svörum úr spurningalistanum fyrir hvert fyrirtæki.

4 Niðurstöður

Fyrirtækin þrettán sem tóku þátt í rannsókninni dreifðust ágætlega á mismunandi starfssvið. Þrjú þeirra eru á sviði hugbúnaðar, þrjú á sviði fjármála og tvö á sviði upplýsingatækni. Þau sem eftir eru skipa sess á sviði fjarskipta, flutnings og geymslu, heilbrigðis, heildsölu/smásölu og vátrygginga, eitt fyrirtæki á hverju sviði. Ljóst er að öll þeirra meðhöndla viðkvæmar upplýsingar. Í ljós kom að tólf af þrettán fyrirtækjum svöruðu játandi að það væri öryggisstefna til staðar hjá fyrirtækinu eða 92,3% og því aðeins einn þátttakandi sem markaði ekki öryggisstefnu. Tekið skal fram að þetta eina fyrirtæki sem hafði nú þegar ekki markað öryggisstefnu ætlar að gera það í nákominni framtíð og er mjög meðvitað um öryggi upplýsinga. Hér á eftir verður talað um svör fyrirtækis þegar átt er við svör starfsmanns þess sem tekið var viðtal við.

Niðurstöður úr rannsókn leiddu það í ljós að eitt fyrirtæki var bæði með meira en milljarð í ársveltu og skráð í Kauphöll Íslands. Níu fyrirtæki voru með meira en milljarð í ársveltu en ekki skráð í Kauphöll Íslands. Þrjú fyrirtæki flokkuðust sem sprotafyrirtæki og eitt fyrirtæki var blandað þ.e.a.s. með meira en milljarð í ársveltu og eyða meira 10% af ársveltu í rannsóknar- og þróunarstörf.

Fyrirtækin tólf sem höfðu markað öryggisstefnu svöruðu því öll játandi að þau teldu að fyrirtækið öðlaðist samkeppnisforskot með því að marka öryggisstefnu. Þau töldu að fyrirtæki öðluðust samkeppnisforskot vegna gæðastarfs, þjónustu, ímyndar, mikils eftirlits og agaðra vinnubragða við það eitt að marka öryggisstefnu. Hinsvegar kom í ljós að aðeins einu fyrirtæki taldi starfsmenn sínir fara mjög vel eftir öryggisstefnunni en átta af tólf fyrirtækjum töldu starfsmenn sínir fara nokkuð vel eftir öryggisstefnu sem sett er í þeirra fyrirtæki. Eitt fyrirtæki taldi starfsmenn sína fara nokkuð illa eftir settri öryggisstefnu og tvö fyrirtæki kusu að vera hlutlaus.

4.1 Vottun

Af þeim tólf fyrirtækjum sem marka öryggisstefnu voru aðeins þrjú sem voru vottuð samkvæmt ISO/IEC 27001 eða 25%. Þessi þrjú fyrirtæki voru einróma sammála um það að vottun veiti þeim samkeppnisforskot á önnur fyrirtæki sem starfa á sama sviði. Af þeim níu sem ekki eru vottuð samkvæmt ISO/IEC 27001 eru sex sem telja að fyrirtækið standist kröfur til að fá vottun eða 66,7% þeirra sem ekki eru vottuð. Ellefu af tólf fyrirtækjum sem marka öryggisstefnu endurskoða hana reglulega, í langflestum tilfellum árlega eða oftar (eftir þörfum). Í tíu af tólf tilfellum eru starfsmenn látnir vita með augljósum hætti (t.d. birt á innra neti eða sendur tölvupóstur) um þá breytingu sem var gerð á öryggisstefnu eftir endurskoðun.

4.2 Sýnileiki

Öryggisstefna er sýnileg í öllum þeim tólf fyrirtækjum sem hafa markað hana. Það er þó mismunandi hverjir fá að sjá hana. Í öllum tilvikum fá starfsmenn að sjá hana og er hún þá sýnileg til dæmis á innri vef eða í gæðahandbók fyrirtækis. Í 33,3% (4 af 12) tilfella fá viðskiptavinir að sjá öryggisstefnuna en þá einungis stefnuna sjálfa en ekki það sem býr að baki, það er að segja verkferla og verklagsreglur. Í 66,7% (8 af 12) tilfella eru aðrir en starfsmenn og viðskiptavinir sem sjá öryggisstefnuna en það eru aðilar á borð við eftirlitsaðila, samstarfsaðila, þjónustuaðila og endurskoðendur.

4.3 Innihald öryggisstefnu

Af þeim tólf fyrirtækjum sem marka öryggisstefnu þá eru ellefu fyrirtæki sem segja að öryggisstefna þeirra feli í sér stjórnkerfi upplýsingaöryggis s.s. hvernig upplýsingar eru geymdar, flokkaðar og eyddar, ábyrgð og hlutverk, áhættumat og lög og reglur. Tíu fyrirtæki segja að öryggisstefna þeirra innihaldi samfelldan rekstur og aðgangsstýringar. Verkferlar eru hluti af öryggisstefnu átta fyrirtækja og stefnumótun í sjö þeirra. Annað sem kom fram var að einnig væru neyðaráætlanir, umhverfisstefna, breytingastjórnun, rýni og eftirlit atriði sem væru innan öryggisstefnu í þremur fyrirtækjum.

4.4 Kröfur utanaðkomandi aðila

Öll þrettán fyrirtækin sem tóku þátt í rannsókninni eiga í samskiptum við erlend fyrirtæki. Sjö fyrirtækjanna sögðu að erlendu fyrirtækin gerðu kröfu um öryggisstefnu hjá þeim. Hin sex sögðu að það væri ekki gerð krafa um öryggistefnu en þó spurt um það og atriði tengdri henni. Í einu tilfelli var það öfugt, þ.e.a.s að íslenska fyrirtækið gerði kröfu á erlenda fyrirtækið um öryggisstefnu. Útfrá umræðum í viðtölunum kemur það í ljós að það fer vaxandi að fyrirtæki, sem eiga í samskiptum við önnur fyrirtæki hvort sem þau eru af íslenskum eða erlendum toga, athugi stöðu á öryggismálum áður en viðskipti eiga sér stað. Slíkt hefur orðið meira áberandi á undanförnum árum og þá sérstaklega hjá erlendum aðilum en vitað er að íslensk fyrirtæki eru á eftir fyrirtækjum á sama sviði erlendis hvað varðar öryggisstefnur og innleiðingu á stjórnkerfum upplýsingaöryggis.

4.5 Mörkun öryggisstefnu

Kannað var í hverskonar starfsemi væri talið að þyrfti að vera mörkuð öryggisstefna til að fyrirtæki gætu lifað og dafnað á markaði. Öll þrettán fyrirtækin töldu að fyrirtæki á sviði heilbrigðis og upplýsingatækni þyrftu að gera slíkt. Flest fyrirtæki eða 92,3% (12 af 13) merktu við fyrirtæki á sviði fjármála, fjarskipta og hugbúnaðar. Rúmlega tveir þriðju eða 9 af 13 fyrirtækjum töldu það eiga við vátryggingar og öryggisgæslu. Að lokum var það um helmingur eða 53,8% (7 af 13) sem merktu við fyrirtæki á sviði fasteigna, 46,1% (6 af 13) á sviði flutnings og geymslu og 30,8% (4 af 13) á sviði heildsölu/smásölu og útflutnings.

Kannað var í hverskonar starfsemi væri talið að þyrfti að vera skylda að marka öryggisstefnu. Niðurstöður voru afgerandi því öll fyrirtæki úrtaksins töldu fyrirtæki á sviði heilbrigðis og fjármála ættu að vera skyldug að marka öryggisstefnu. Rúmlega tveir þriðju (69,2 %, 9 af 13) töldu það eiga við á sviði fjarskipta. Tæpur helmingur (46,1%, 6 af 13) merkti við fyrirtæki á sviði vátrygginga og 38,5% (5 af 13) merktu við fyrirtæki á sviði upplýsingatækni og öryggisgæslu. Þriðjungur (30,8%, 4 af 13) taldi það eiga við fyrirtæki á sviði hugbúnaðar, 15,4% (2 af 13) á sviði fasteigna og

7,7% (1 af 13) á sviði flutnings og geymslu og útflutnings. Enginn taldi að fyrirtæki á sviði heildsölu/smásölu ætti að vera skylt að marka öryggisstefnu.

Mynd 5: Svör við spurningunni: Í hverskonar starfsemi ætti að vera skylda að marka öryggisstefnu?

4.6 Traust samfélags

Að lokum var kannað hvort að þátttakendur teldu að það skapi samfélaginu traust að fyrirtæki séu með öryggisstefnu. Hér gátu þátttakendur svarað með eigin orðum. Ýmis svör komu á yfirborðið en ellefu af þrettán svöruðu játandi. Þegar spurt var um ástæðuna töldu þessi 11 fyrirtæki að fólk vill vita að upplýsingar þeirra og annarra séu meðhöndlaðar rétt og að þær séu öruggar. Sýni fyrirtæki fram á að það verji upplýsingar sem það hefur að geyma og meðhöndli þær rétt þá skapi það traust samfélagsins á fyrirtækið.

Viðmælendur ræddu mikið um mikilvægi þess að vera vel upplýstir um hættur og ógnanir og stuðla að fyrirbyggjandi aðgerðum. Það að sýna fram á að fyrirtæki sé með öryggisstefnu auki því trúverðugleika fyrirtækis þar sem þessum atriðum er sinnt í stjórnkerfi sem lýtur að öryggisstefnu. Hinsvegar sé það í höndum utanaðkomandi aðila að treysta því síðan að fyrirtæki fari eftir öryggisstefnunni en hægt er að auka traustið enn og meira sé fyrirtækið vottað því það er staðfesting á farið sé eftir öllum kröfum sem snúa að öryggi upplýsinga.

5 Umræða

Rannsóknarspurningarnar sem settar voru fram í upphafi og leitast er við að svara í þessari ritgerð eru:

- Munu einkarekin fyrirtæki sem ekki marka öryggisstefnu og framkvæma áhættumat lifa af í framtíðinni?
- Verður nauðsyn að öðlast vottun á sviði öryggis?
- Er framtíðin sú að öll fyrirtæki verði skyldug að vera með öryggisstefnu?
- Veitir öryggisstefna fyrirtækjum samkeppnisforskot?

Leitað var svara við þessum spurningum með spurningakönnun. Taka þarf tillit til þess að svarhlutfall var ekki hátt. Niðurstöður geta gefið örlítið bjagaða mynd á raunstöðu og viðhorfi íslenskra fyrirtækja en áreiðanleiki myndi aukast ef svörun væri meiri. Engu að síður mun svörun þátttakenda vera notuð hér til þess að svara þessum spurningum.

Samkvæmt svörunum munu einkarekin fyrirtæki innan ákveðinna starfssviða lifa af í framtíðinni án þess að marka öryggisstefnu og framkvæma áhættumat. Svörin benda til þess að þau fyrirtæki sem eru á sviði heilbrigðis, upplýsingatækni, fjármála, fjarskipta og hugbúnaðar þurfa einna helst að marka öryggisstefnu til að lifa og dafna á markaði samanber það sem kom fram í kafla 4.5. Nauðsyn þess að öðlast vottun á sviði öryggis virðist vera að aukast með hverju árinu sem líður. Fleiri og fleiri fyrirtæki sjá hag í að marka öryggisstefnu og öðlast vottun þar sem það veitir þeim samkeppnisforskot og aukin viðskipti samanber kafla 4.1. Samkeppnisforskot kemur fram í gæðum fyrirtækis, þjónustu, ímyndar, mikils eftirlits og agaðra vinnubragða eins og fram kemur í upphafi kafla 4 og er augljós afleiðing þess að marka öryggisstefnu.

Svarendur telja að það séu helst þau fyrirtæki sem meðhöndla persónuupplýsingar og/eða aðrar viðkvæmar upplýsingar sem þurfa að marka öryggisstefnu og því ber framtíðin ekki með sér að öll fyrirtæki verði skyldug þess. Samanber kafla 4.5 þá eru það fyrirtæki sem eru á sviði heilbrigðis og fjármála sem ættu að vera skyldug til að marka öryggisstefnu en það eru nú þegar gerðar kröfur um að fyrirtæki á þessum sviðum búi yfir stjórnkerfi upplýsingaöryggis af utanaðkomandi aðilum.

Áhugavert er að sjá að allir þátttakendur virðast vera mjög sammála um það eigi að skylda fyrirtæki á sviði heilbrigðis til að marka öryggisstefnu ekki bara í þeim tilgangi að verja viðkvæmar upplýsingar heldur einnig til að geta lifað og dafnað á markaði. Einnig er áhugavert að sjá að niðurstöður leiði í ljós að allir þátttakendur líta svo á að fyrirtæki á sviði upplýsingatækni þurfi að marka öryggisstefnu til að lifa og dafna á markaði en einungis rúmur þriðjungur þeirra telur að það þurfi að skylda þau til þess. Það kemur ekki á óvart að niðurstöður gagnvart fyrirtækjum á sviði fjármála sýni að þeim eigi að vera skylt að marka öryggisstefnu en það sem er hinsvegar áhugavert er að einungis tæpur helmingur þátttakenda líta svo á að það eigi að skylda fyrirtæki á sviði vátrygginga að marka öryggisstefnu.

5.1 Staða öryggisstefna

Samkvæmt niðurstöðu rannsóknarinnar er staða varðandi öryggisstefnu fyrirtækja ágæt en lengi má gera gott enn betra. Íslensk fyrirtæki virðast vera orðin meðvitaðri um ógnir og hættur í innra og ytra umhverfi þess og að þau verði að hafa einhverskonar reglur og/eða kerfi til að vernda trúnaðar- og persónulýsingar.

Eftir umræður við þátttakendur er ljóst að mörg fyrirtæki standa frammi fyrir kröfum eftirlitsaðila um að innleiða verklag sem byggist á ISO/IEC 27001 staðlinum en það eru einna helsta fyrirtæki á sviði fjármála, heilbrigðis og vátrygginga. Svo virðist sem fyrirtæki, önnur en þau sem eru krafin um að marka öryggisstefnu, séu í æ fleiri tilvikum að innleiða stjórnkerfi upplýsingaöryggis þar sem stjórnendur sjá ávinning í því að stilla upp slíku stjórnkerfi í rekstri sínum. Fyrirtæki móta öryggisstefnu sína samkvæmt ISO/IEC 27001 án þess að endilega ætla sér að öðlast vottun. Þau sækjast í að vera með reglur og aðhald hvað varðar öryggi og vilja sýna fram á heilbrigt

stjórnkerfi. Almenningur virðist vera meira meðvitaður um auknar hættur á tjóni sökum upplýsingaleka þar sem rafrænt upplýsingaflæði hefur stóraukist á undanförnum árum. Það er því síaukin krafa um öryggisstefnu frá almenningi sem og öðrum fyrirtækjum.

5.2 Viðhorf til öryggisstefna

Að byggja upp stjórnkerfi upplýsingaöryggis þarf sinn meðgöngutíma og er því ómögulegt að gera það á einni nóttu. Það er ekki nóg að setja niður reglur og ferla og ætlast til að starfsfólk fyrirtækisins tileinki sér það á örskömmum tíma. Í tímaritinu Tölvumál 1. tbl. segir Gyða Halldórsdóttir að „Forsendur þess að öryggisstefna stofnana/fyrirtækja virki og beri tilætlaðan árangur er eindreginn og sýnilegur stuðningur yfirmanna og ábyrgðaraðila við framkvæmd stefnunnar“ [28]. Frá fyrsta degi þurfa æðstu stjórnendur að vera virkir þátttakendur í innleiðingu stjórnkerfis og bera ábyrgð á því að hún sé framkvæmd á markvissan hátt. Stjórnendur þurfa að vera meðvitaðir að innleiðing sem þessi beri mestan árangur sé hún innleidd „top-down“ þ.e.a.s. stjórnendur þurfa að vera fyrirmyndir og leiðtogar og fá fólkið með sér í breytingarnar. Séu stjórnendur ekki að fara út í innleiðingu af heilum hug þá er ekki hægt að ætlast til að undirmenn þeirra geri það [28].

Til eru ótal tæki og tól sem hægt er að nota til að bæta öryggi kerfa en besta forvörnin er vel upplýstur starfsmaður, góðir skýrir ferlar og heilbrigt stjórnkerfi. En hvernig er hægt að vita að starfsmaður sé vel upplýstur og meðvitaður um öryggi upplýsinga? Ebenezer Þ. Böðvarsson svarar þessari spurningu í tímaritinu Tölvumál 1 tbl. í grein sinni Öryggismeðvitund starfsfólks - virkjum mannlega eldvegginn:

> „Ýmsar skilgreiningar eru til á öryggismeðvitund en í stuttu máli má segja að starfsfólk hafi öryggismeðvitund þegar það þekkir hlutverk sitt við að tryggja rekstraröryggi vinnustaðarins, hegðar sér í samræmi við það og er fært um að taka upplýstar ákvarðanir við nýjar aðstæður. Í öðrum orðum: Það veit hvað verið er að vernda, hvers vegna og fyrir hverjum, þekkir reglur og ábyrgð og er fært um að greina ákveðnar hættur og bregðast rétt við“ [29].

Ef allir leggjast á eitt við að styrkja öryggismeðvitund innan fyrirtækis myndast ákveðin fyrirtækjamenning. Heppnist innleiðing á stjórnkerfi upplýsingaöryggis vel

þá verða starfsmenn farnir að vinna eftir settum verkferlum án þess að vera sérstaklega meðvitaðir um það en það er lýsandi fyrir breytingu á hugarfari sem hefur orðið að lífstíl eða réttara sagt vinnubrögðum og menningu innan fyrirtækis. Það má því segja að upplýsingaöryggi standi og falli að langmestu leyti með hollustu og vandaðri umgengni starfsmanna.

Samkvæmt niðurstöðum í upphafi kafla 4 sést að aðeins einu fyrirtæki taldi starfsmenn sínir fara mjög vel eftir öryggisstefnunni en átta af tólf fyrirtækjum töldu starfsmenn sínir fara nokkuð vel eftir öryggisstefnu sem sett er í þeirra fyrirtæki. Það má velta fyrir sér hvers vegna starfsmenn fara ekki alltaf mjög vel eftir settri öryggisstefnu. Er það vegna þess að þeir eru ekki nógu vel upplýstir eða er hægt að skrifa þetta á leiðtogahlutverk stjórnenda?

5.3 Er nauðsyn að marka öryggisstefnu?

Fram kom í viðtali við einn þátttakenda rannsóknarinnar að hans fyrirtæki þótti það vera óþarfa pappírs- og tímaeyðsla að skrá og skjalfesta öryggisstefnu, innleiða hana og fylgja henni eftir þar sem mikil meðvitund er innan fyrirtækisins um hættur og ógnir í innra og ytra umhverfi þess. Aðrir þátttakendur sem hinsvegar hafa gengið í gegnum þetta ferli telja það vera fjárfestingu en ekki bara eintómur kostnaður.

Þátttakendur í rannsókninni töluðu einnig um að sjá mætti bersýnilegan rekstrarávinning við innleiðingu öryggisstefnu hvað varðar skilvirkari vinnubrögð, lækkun á kostnaði í kjölfarið og færri mistökum. Starfsmönnum liði betur að geta flett upp á innra neti eða gæðahandbók og séð nákvæmlega hvernig á að vinna ákveðið verk. Starfmenn eru því vel upplýstir sem eyðir allri óvissu og tvíverknaði.

Niðurstaðan er því að það er nauðsynlegt hverjum þeim sem meðhöndlar persónuupplýsingar að marka öryggisstefnu til að standa lagalegar kröfur um persónuvernd og meðferð persónuupplýsinga.

5.4 Vottun eða ekki vottun?

Ferlið við að öðlast vottun sem er lýst í kafla 2.1.2 er umfangsmikið, kostnaðarsamt og tímafrekt. Samkvæmt niðurstöðum úr rannsókninni telja þau fyrirtæki sem hafa nú þegar öðlast vottun það vera algjörlega þess virði og líta á það sem fjárfestingu að hafa gengið í gegnum ferlið en ekki kostnað. Sex af níu fyrirtækjum sem eru ekki vottuð en hafa markað öryggisstefnu stefna að því að öðlast vottun eða 66,7% þátttakenda. Það má því draga þá ályktun að framtíðin beri það með sér að fleiri fyrirtæki sækist í að öðlast vottun á sviði upplýsingaöryggis.

6 Tillögur

Hér að neðan má sjá nokkrar tillögur sem komnar eru af vinnu þessa verkefnis og niðurstöðum rannsóknar.

6.1 Uppbygging stjórnkerfis

Öryggisstefna ætti að vera hluti af stefnumótun hvers fyrirtækis sem meðhöndlar persónuupplýsingar og/eða aðrar viðkvæmar upplýsingar en gert er ráð fyrir slíku í lögum nr 77/2000 um persónuvernd og meðhöndlun persónuupplýsinga eins og fjallað var um í kafla 2.6. Það að vera með öryggisstefnu undirstrikar að fyrirtæki sé að fara eftir settum lögum og reglum varðandi meðferð upplýsinga og eykur trúverðugleika og áreiðanleika.

Öryggisstefnur fyrirtækja eru í grunninn alveg nákvæmlega eins en síðan bætast við sértæk atriði sem einkenna rekstur hvers fyrirtækis eftir starfssviði þess. Búa þarf til leiðbeiningahandbók og/eða skapalón að öryggisstefnu til að auðvelda rekstrareigendum að stilla upp öryggisstjórnkerfi í sitt fyrirtæki. Margir kjósa að horfa framhjá mörkun öryggisstefnu sökum þess hversu mikið flækjustigið er og því er tilvalið að létta undir verkum þar sem kostur er. Slík tól við mörkun öryggisstefnu myndu verða til þess að fleiri fyrirtæki myndu sjá sér fært að setja verkefnið í framkvæmd og eftir því sem fleiri bætast í hópinn því meira öryggi verður í rekstrarlegu umhverfi íslensks samfélags.

Flækjustig verkferla og verklagsreglna getur verið mikið og því er ákjósanlegast að setja upp öryggisstefnu á eins greinargóðan hátt og mögulegt er. Myndræn uppsetning er fýsilegur kostur þar sem hún er auðlesnari og skiljanlegri uppsetning heldur en

eintómir textar og málsgreinar. Til eru forrit á borð við Microsoft Visio, iGrafx og fleiri sambærileg sem hægt er að nota við að teikna upp verkferla. Hægt er þá að sjá verkferli í sinni einföldustu mynd en einungis með því að smella á tiltekinn hluta verkferils birtist nánari lýsing á honum. Hægt er að setja inn ábyrgðaraðila fyrir hvern þátt ferils og ferilsins í heild sem einfaldar þá líka þeirri manneskju sem ber þessa ábyrgð að sjá til hvers er ætlast af honum.

Þar sem ferlið við að stilla upp stjórnkerfi upplýsingaöryggis er tímafrekt og nokkuð kostnaðarsamt þá mælir höfundur með því að fyrirtæki setji sig í samband við ráðgjafafyrirtæki um upplýsingaöryggi eða hafa samband við vottunaraðila á borð við BSI (sjá kafla 2.1.1) og fá aðstoð við uppsetningu og innleiðingu stjórnkerfis. Einnig á máltækið „Betur sjá augu en auga“ vel við í þessu samhengi þar sem starfsmenn geta orðnir vanir sínu starfsumhverfi og ná ekki að koma auga á hluti sem annars eru mikilvægir.

6.2 Innleiðing stjórnkerfis

Þegar ákveðið hefur verið að fara í það verkefni að marka öryggisstefnu, innleiða hana og fylgja henni eftir er það undirbúningsferlið sem er umfangsmesti liðurinn. Kortleggja þarf marga ferla, bæta þá og breyta og skilgreina ábyrgðaraðila og eftirlitsaðila. Leið sem er líkleg til árangurs gæti verið í eftirtalinni röð:

1. Ákvörðun tekin um innleiðingu staðalsins
2. Ábyrgð stjórnenda skilgreind og verkefnisstjóri tilnefndur
3. Öryggisstefna útfærð (fyrsta útgáfa)
4. Umfang stjórnkerfisins skilgreint
5. Áhættugreining
6. Ákveðið með hvað hætti skuli meðhöndla áhættu
7. Velja ráðstafanir úr staðlinum til að lágmarka áhættu
8. Innleiða ráðstafanir / nýtt verklag
9. Útbúa stöðumatsskýrslu / yfirlit yfir hvaða kröfur stjórnkerfið uppfyllir
10. Ákvörðun um vottun

[11]

Ef fyrirtæki á annað borð er tilbúið að leggja vinnu og fjármagn í að marka öryggisstefnu mælir höfundur með því að gæðastjórnun sé innleidd á sama tíma. Gæðastjórnun er grunnur reksturs til að afkasta eftir bestu getu með sem minnstum kostnaði og skila sem mestum hagnaði. Þegar gæðastjórnun er til staðar þá er mun auðveldara og minni fyrirhöfn að bæta við öryggiskröfum hvað varðar upplýsingaöryggi samkvæmt ISO/IEC 27001 samanber kafla 2.8 þar sem fjallað var um náið samband gæða- og öryggismála.

6.3 Vottun og viðhorf

Sé ætlunin að marka öryggisstefnu, innleiða hana og öðlast vottun þá þarf breytingastjórnun innan fyrirtækisins að vera virk. Ekki er nóg að ein deild eða eitt teymi innan fyrirtækisins vinni þetta mikla verk og segi síðan samstarfsfélögum sínum að þetta sé nýja skipulagið og þeim beri að gera eins og þeir segi. Hugarfarsbreyting og þátttaka stjórnenda eru lykilforsendur þess að vel takist til. Kynna þarf vel fyrir stjórnendum ávinning þess og kosti að marka öryggisstefnu og fá þá til að vera hluti af teyminu sem vinnur að þessu verkefni. Auðvitað eru einhverjir sem líta á allar breytingar sem ógnun á þeirra þægindahring en þá reynir á stjórnendur að vera leiðtogar og fá fólkið með sér í að líta á breytingar sem tækifæri (sjá kafla 5.2). Gangi ekki vel að koma á hugarfarsbreytingu gæti ástæðan ef til vill verið sú að starfsmenn og stjórnendur eru ekki nógu vel upplýstir um málefnið og því skilningur fyrir breytingu enginn. Útbúa ætti kynningarefni fyrir alla rekstrareigendur sem meðhöndla persónuupplýsingar og/eða aðrar viðkvæmar upplýsingar og auka vitund þeirra á málefninu. Halda ætti námskeið fyrir stjórnendur um hvernig þeirra þáttur í verkefninu er og mikilvægi þess að þeir séu virkir þátttakendur svo að verkefnið skili tilteknum árangri. Fyrirtækjamenning myndast þegar allir starfsmenn eru virkir þátttakendur í ákveðnu verklagi og gera það ómeðvitað. Því fyrr sem allir ákveða að tileinka sér nýtt verklag því fyrr vinnst það ómeðvitað á þann hátt og hefur myndað ákveðna menningu innan fyrirtækis.

6.4 Gæðastimplar

Fyrirtæki sem eru ekki vottuð í dag en eru með öryggisstefnu hafa engan gæðastimpil til að sýna viðskiptavinum og samstarfsaðilum sem sönnun þess að þeir séu með stjórnkerfi fyrir upplýsingaöryggi og verndi upplýsingar sínar. Hugmynd væri að hafa nokkrar gerðir af vottun eða gæðastimplum svo að þau fyrirtæki sem kjósa að hafa öryggisstefnu en ekki innleiða ISO/IEC 27001 að fullu hafi eitthvað til að sýna fram á að það sé hugað að upplýsingaöryggi í rekstri þeirra. Hægt væri að hafa mismunandi stig á gæðastimplum (t.d. A,B,C) eftir því hvers eðlis áhættur og/eða ógnanir steðja að tilteknu fyrirtæki og hversu miklar persónuupplýsingar og/eða aðrar viðkvæmar upplýsingar það hefur að geyma. Með þessu móti væri meira eftirlit með rekstri íslenskra fyrirtækja hvað varðar upplýsingaöryggi og tryggir viðskiptavinum og öðrum þeim sem eiga viðskipti við tiltekið fyrirtæki að það sé eitthvað á bakvið öryggisstefnu fyrirtækisins sem er annars auðvelt að hafa á yfirborðinu án þess að hún byggi á einhverjum grunni.

7 Næstu skref

Könnunin sem fjallað er um hér að framan veitti að hluta til svör við þeim spurningum sem lagt var upp með. Megin niðurstöður eru að kynna þarf öryggisstefnu, tilgang hennar og ávinning betur fyrir stjórnendum fyrirtækja til að upplýsa íslenska rekstraraðila um nauðsyn þess að vernda persónuupplýsingar og/eða aðrar viðkvæmar upplýsingar fyrir utanaðkomandi aðilum sem kunna að valda þeim skaða eða tjóni. Til að ná til flestra er hægt að stofna kynningarteymi sem myndi fara í einhverskonar herferð og kynna öryggisstefnur. Þetta kynningateymi gæti verið með ráðstefnu, hádegisfyrirlestra í fyrirtækjum, útbúið bæklinga og svona mætti lengi telja.

Það væri einnig verðugt að skoða hvort og þá hvernig vottaðar öryggisstefnur hafa áhrif á útflutning frá Íslandi. Sé litið á lista yfir þau fyrirtæki sem eru vottuð í heiminum þá sést að Japan er með langflestu vottuðu fyrirtækin eða 3790 af 7136 (53,1%) [9]. Er það vegna stærðar eða vegna þess að í Japan eru fjölmörg framleiðslufyrirtæki? Myndi fyrirtæki á Íslandi versla við framleiðslufyrirtæki í Japan ef það væri ekki vottað og/eða sýndi fram á gæði við meðferð viðkvæmra upplýsinga? Af hverju ættu fyrirtæki erlendis að versla við íslensk fyrirtæki sem ekki sýna fram á gæði í sínum öryggismálum?

Við vinnslu ritgerðarinnar komu einnig upp spurningar sem ekki fengust svör við að þessu sinni en eru þess í stað efni í aðra rannsókn tengda þessari. Spurningar sem vert er að kanna frekar svör við eru m.a.:

- Fara starfsmenn betur eða verr eftir öryggisstefnu eftir því hvort hún er vottuð eða ekki?
- Marka fyrirtæki öryggisstefnu einungis vegna þess að það er gerð krafa um það frá aðilum sem þeir eiga viðskipti við eða eftirlitsaðilum?
- Á að þurfa að setja skyldu um mörkun öryggisstefnu eða er það sjálfsagt mál?

- Hver/Hverjir sjá um að marka öryggisstefnu fyrirtækis? Eingöngu starfsfólk innanhúss eða eru fengnir ráðgjafar til aðstoðar?
- Hvenær er ákjósanlegast að marka öryggisstefnu? Á hvaða tímapunkti á æviskeiði fyrirtækja?

Takmarkanir þessa rannsóknar er hversu fáir svöruðu beiðni um viðtal og þar af leiðandi fáir þátttakendur í rannsókninni. Fleiri þátttakendur myndu auka marktækni á niðurstöðum og gefa skýrari mynd um raunverulega stöðu og viðhorf til öryggisstefnu og upplýsingaöryggis meðal íslenskra fyrirtækja á Íslandi í dag. Við gerð næstu rannsóknar væri því vert að íhuga að fá fyrirtæki sem sérhæfir sig í gerð kannanna til dæmis Capacent í lið með sér til að fá betri svörun og ná dýpri túlkun á niðurstöðum.

Einnig væri áhugavert að horfa meira til hlutlægra gagna heldur en huglægra. Formið á viðtölunum í þessari rannsókn býður uppá að svörin séu fremur huglæg þar sem þau byggjast á persónulegum skoðunum þátttakenda. Fróðlegt væri að skoða betur vinnu-umhverfi í fyrirtækjum, rýna í fyrirliggjandi gögn, verkferla og verklagsreglur, fylgjast með vinnubrögðum starfsmanna og jafnvel fylgjast með störfum úttektarmanna svo dæmi séu tekin. Hlutlæg gögn sem aflað væri á vettvangi gætu gefið ítarlegri mynd af stöðu mála.

8 Lokaorð

Öryggisstefna er einskonar viðurkenning á öruggum starfsháttum sem eyðir allri tortryggni í garð viðskiptavina og samstarfsaðila. Hún bendir til gæða í rekstri og sýnir ábyrgð. Það kann að vera að fólki finnist það vera óþarfi að marka öryggisstefnu en miðað við þekkingu mannsins í dag þá eru tölvur sigranlegar, kerfi götótt og ástæða til að verja allar persónuupplýsingar og/eða aðrar viðkvæmar upplýsingar eftir bestu getu fyrir óprúttnum utanaðkomandi aðilum. Það að sýna fram á að fyrirtæki marki öryggisstefnu eykur trúverðugleika þess þar sem það sýnir fram á að öryggisatriðum er sinnt í stjórnkerfi upplýsingaöryggis. Það er hinsvegar í höndum utanaðkomandi aðila á borð við viðskiptavini og samstarfsaðila að treysta því að fyrirtæki fari eftir settri öryggisstefnu en hægt er að auka traustið enn meira sé fyrirtækið vottað samkvæmt ISO/IEC 27001 því það er staðfesting þess að farið er eftir öllum kröfum sem snúa að öryggi upplýsinga.

Besta forvörn fyrir fyrirtæki gegn tjóni og/eða eyðileggingu upplýsinga er öryggismeðvitund starfsmanna þess. Vel upplýstur starfsmaður getur komið í veg fyrir tjón með því að bregðast rétt við ákveðnum aðstæðum. Það má því segja að upplýsingaöryggi standi og falli að langmestu leyti með hollustu og vandaðri umgengni starfsmanna. Að undanskildum þeim fyrirtækjum sem settar eru kröfur um að marka öryggisstefnu er það algjörlega valkvætt að marka slíka stefnu. Hvort sem fyrirtæki eru stór eða smá þá eru líkur á því að það koma upp þær aðstæður þar sem þau lenda í samkeppni við fyrirtæki sem hafa markað öryggisstefnu og innleitt hana og samkvæmt niðurstöðum þá eru þau líklegri til að hafa vinninginn. Valið er frjálst, enda er ekki skylda að lifa samkeppnina af.

Heimildaskrá

[1] A. Eshlaghy, A. Pourebrahimi, and B. Nobari, "Presenting a Model for Ranking Organizations Based on the Level of the Information Security Maturity," *Computer and Information Science*, vol. 4, no. 1, p. 72, Jan. 2011.

[2] "Stiki - Öryggisstefna." [Online]. Available: http://stiki.is/index.php/is/um-stika/oryggisstefna. [Accessed: 18-Apr-2011].

[3] "2000 nr. 77 23. maí/ Lög um persónuvernd og meðferð persónuupplýsinga." [Online]. Available: http://www.althingi.is/lagas/139a/2000077.html. [Accessed: 18-Apr-2011].

[4] "Reglur nr. 299/2001 um öryggi persónuupplýsinga | Reglur og reglugerðir | Lög og reglur | Persónuvernd. Þínar upplýsingar, þitt einkalíf." [Online]. Available: http://www.personuvernd.is/log-og-reglur/reglur-og-reglugerdir/nr/35. [Accessed: 18-Apr-2011].

[5] "ISO/IEC 27001 Information Security." [Online]. Available: http://www.bsigroup.com/en/Assessment-and-certification-services/management-systems/Standards-and-Schemes/ISO-IEC-27001/. [Accessed: 18-Apr-2011].

[6] "ISO/IEC 27001 certification standard." [Online]. Available: http://www.iso27001security.com/html/27001.html. [Accessed: 18-Apr-2011].

[7] "Benefits of ISO certification." [Online]. Available: http://www.riskmanagementstudio.com/index.php/en/knowledge-center-articles/166-benefits-of-certifications. [Accessed: 18-Apr-2011].

[8] A. Calder and S. Watkins, *IT governance: a manager's guide to data security and ISO 27001/ISO 27002*. Kogan Page Publishers, 2008.

[9] "Neue Seite 1." [Online]. Available: http://www.iso27001certificates.com/. [Accessed: 18-Apr-2011].

[10] "Leiðin að vottun stjórnkerfa." [Online]. Available: http://www.bsiaislandi.is/index.php/leiein-ae-vottun-stjornkerfa.html. [Accessed: 18-Apr-2011].

[11] Ólafur Róbert Rafnsson, "Stjórnkerfi Upplýsingaöryggis: Hvernig göngum við um mikilvægar upplýsingar?" .

[12] Staðlaráð Íslands, *ÍST ISO/IEC 27001:2005*, 2nd ed. .

[13] J. J. Dahlgaard, K. Kristensen, and G. K. Kanji, "Total quality management and education.," *Total Quality Management*, vol. 6, no. 5, pp. 445-455, Dec. 1995.

[14] "Stiki - Áhættumat." [Online]. Available: http://stiki.is/index.php/is/radgjof-og-tjonusta/upplysingaoryggi/ahaettumat. [Accessed: 18-Apr-2011].

[15] Glenn Koller, *Risk assessment and decision making in business and industry : a practical guide*, 2nd ed. Taylor and Francis Group, 2005.

[16] P. G. Johnson and P. K. Scholes, *Exploring Corporate Strategy: Text and Cases*, 7th ed. Financial Times/ Prentice Hall, 2006.

[17] Páll Kr. Pálsson, *Handbók athafnamannsins : stefna, stjórnun og starfsmenn : lyklar að árangri í rekstri*. Reykjavík: Oddi hf., 2006.

[18] Staðlaráð Íslands, *ISO 9000 Kjarnastaðlarnir - hljóma betur saman*, 1st ed. Reykjavík: Staðlaráð Íslands, 2005.

[19] Mörður Árnason, *Íslensk orðabók*, 3rd ed., vol. bindi M-Ö. Edda, 2002.

[20] Lewis Schiff, "Protect Affluent Clients' Data - and Privacy," *Investment Advisor*, Mar. 2011.

[21] E. Árnason, "Persónugreining í gagnagrunni á heilbrigðissviði."

[22] Ferdinand Hansen, "Sprotafyrirtæki | Starfsgreinar | Samtök iðnaðarins - íslenskur iðnaður." [Online]. Available: http://www.si.is/starfsgreinahopar/sprotafyrirtaeki/. [Accessed: 18-Apr-2011].

[23] Dr. Björn Þór Jónsson, "Reynslusaga: Um tilurð sprotafyrirtækis," *Tölvumál*, vol. 1, pp. 18-19.

[24] Ferdinand Hansen, "Hvað er gæðastjórnun | Gæðastjórnun | Gæðastjórnun og rekstur | Málaflokkar | Samtök iðnaðarins - íslenskur iðnaður." [Online]. Available: http://www.si.is/malaflokkar/gaedastjornun-og-rekstur/gaedastjornun/. [Accessed: 18-Apr-2011].

[25] W. E. Deming, *Out of the crisis*. MIT Press, 2000.

[26] "Greinasafn: Gæðastjórnun, eðli hennar og tilgangur." [Online]. Available: http://www.landbunadur.is/landbunadur/wgsamvef.nsf/0/6a32324cfe7a302200256c300009f675?OpenDocument. [Accessed: 07-May-2011].

[27] J. S. Oakland, *Total quality management : the route to improving performance*. Oxford ; Boston: Butterworth-Heinemann, 1993.

[28] Gyða Halldórsdóttir, "Öryggi trúnaðarupplýsinga: Þekking, viðhorf og fræðsla," *Tölvumál*, vol. 1, p. 28.

[29] Ebenezer Þ. Böðvarsson, "Öryggismeðvitund starfsfólks - virkjum mannlega eldvegginn," *Tölvumál*, vol. 1, p. 4.

Viðauki A

Spurningalisti fyrir fyrirtæki

1. Á hvaða sviði starfar fyrirtækið?

- ❑ Tryggingastofnun
- ❑ Upplýsingatækni
- ❑ Hugbúnaðarfyrirtæki
- ❑ Banki
- ❑ Heilbrigðissvið
- ❑ Fjármálafyrirtæki
- ❑ Annað, hvað?

2. Fyrirtækið flokkast sem:

- ❑ 2.1 **Þroskað fyrirtæki** (fyrirtæki með meira en milljarð króna í ársveltu og er skráð í Kauphöll Íslands)
- ❑ 2.2 **Sprotafyrirtæki** (fyrirtæki sem leggur amk 10% af veltu í rannsóknar- og þróunarstarf og er með ársveltu allt að milljarði króna)
- ❑ 2.3 **Annað**, hvað?

3. Er öryggisstefna til staðar hjá fyrirtækinu?

3.1 Já

- **3.1.1 Telur þú að fyrirtækið öðlist samkeppnisforskot með því að marka öryggisstefnu?**
  - Já
    - Að hvaða leyti?
  - Nei
    - Hvers vegna ekki?

- **3.1.2 Hversu vel telur þú að starfsmenn fyrirtækisins fari eftir öryggisstefnunni?**
  - Mjög vel
  - Nokkuð vel
  - Hlutlaus
  - Nokkuð illa
  - Mjög illa

- **3.1.3 Er fyrirtækið vottað skv. ISO 27001?**
  - **Já**
    - **3.1.3.1 Telur þú að vottun veiti samkeppnisforskot?**
      - Já
        - Að hvaða leyti?
      - Nei
        - Hvers vegna ekki?
  - **Nei**
    - **3.1.3.2 Stendur til að fá vottun?**
      - Já
      - Nei
        - Hvers vegna ekki?

- **3.1.4 Er öryggisstefna fyrirtækisins endurskoðuð reglulega?**
  - Já
    - 3.1.4.1 Með hversu löngu millibili?
      - Hvenær var það gert síðast?
    - 3.1.4.2 Eru starfsmenn látnir vita um allar breytingar sem á henni eru gerðar?
  - Nei

- **3.1.5 Hvað felur öryggisstefna fyrirtækisins í sér?**
  - ❑ Stjórnkerfi upplýsingaöryggis (hvernig geymd, flokkuð, eytt)
  - ❑ Ábyrgð og hlutverk
  - ❑ Verkferlar
  - ❑ Áhættumat
  - ❑ Samfelldur rekstur
  - ❑ Lög og reglur
  - ❑ Aðgangsstýringar
  - ❑ Stefnumótun
  - ❑ Annað, hvað?

- **3.1.6 Er öryggisstefna fyrirtækisins sýnileg?**
  - Já
    - 3.1.6.1 Hverjir sjá öryggisstefnuna?
      - Viðskiptavinir
        - Hvar?
      - Starfsmenna
        - Hvar?
      - Aðrir, hverjir?
  - Nei

- **3.1.7 Er öryggisstefna fyrirtækisins kynnt öllum starfsmönnum?**
  - Já
  - Nei

3.2 Nei

- **3.2.1 Stendur til að marka öryggisstefnu?**
  - Já
  - Nei
    - Hvers vegna ekki?

- **3.2.2 Hvers vegna hefur ekki verið mörkuð öryggisstefna?**

- **3.2.3 Telur þú að mörkun öryggisstefnu myndi auka samkeppnisforskot fyrirtækisins?**
  - Já
    - Að hvaða leyti?
  - Nei
    - Hvers vegna ekki?

- **3.2.4 Eru til reglur um meðferð upplýsinga/gagna innan fyrirtækisins?**
  - Já
    - Á hvaða formi eru þær settar fram?
  - Nei

- **3.2.5 Er gert áhættumat?**
  - Já
    - Hvað er gert við gögnin sem koma út úr áhættumatinu?

- Nei
  - 3.2.5.1 Er fyrirtækið meðvitað um þær áhættur sem er í umhverfi þess?
    - Já
    - Nei

4. Á fyrirtækið í samskiptum við erlend fyrirtæki?

- 4.1 Já
  - 4.1.1 Gerir það fyrirtæki kröfu um öryggisstefnu hjá ykkur?
    - Já
    - Nei
- 4.2 Nei

5. Má merkja við fleiri en einn reit: Í hverskonar starfsemi telur þú að í framtíðinni þurfi að vera mörkuð öryggisstefna til að geta lifað og dafnað á markaði?

- ❑ Fasteignir
- ❑ Fjármál
- ❑ Fjarskipti
- ❑ Flutningur og geymsla
- ❑ Heilbrigðissvið
- ❑ Heildsala/Smásala
- ❑ Hugbúnaður
- ❑ Upplýsingatækni
- ❑ Útflutningur
- ❑ Vátryggingar
- ❑ Öryggisgæsla
- ❑ Annað, hvað?

6. Má merkja við fleiri en einn reit: Í hverskonar starfsemi telur þú að ætti að vera skylda að marka öryggisstefnu?

- ❑ Fasteignir
- ❑ Fjármál
- ❑ Fjarskipti
- ❑ Flutningur og geymsla
- ❑ Heilbrigðissvið
- ❑ Heildsala/Smásala
- ❑ Hugbúnaður
- ❑ Upplýsingatækni
- ❑ Útflutningur
- ❑ Vátryggingar
- ❑ Öryggisgæsla
- ❑ Annað, hvað?

7. Telur þú að það skapi samfélaginu traust að fyrirtæki séu með öryggisstefnu?

- Já
  - Hvers vegna?
- Nei
  - Hvers vegna ekki?