INSIDER THREAT IN IT

(de factor mens beschouwd)

Referaat postdoctorale opleiding EDP auditing
Erasmus Universiteit Rotterdam (EURAC)
Drs. A.J.A.M. Spee

Begeleiding
Drs. Ing. A. Nuijten RE

Versie 1.1
9 november 2003

Voorwoord

Het onderwerp 'insider threat in IT' draait om de kwaadwillige IT-medewerker die bij machte is om bedrijven te ruïneren, levens op het spel te zetten en gezien de voortgaande wereldwijde vervlechting van systemen problemen op wereldschaal te veroorzaken. Als systeemontwikkelaar, netwerkontwerper, performance- of beveiligingsspecialist heeft het me vroeger altijd verbaasd met hoeveel ongefundeerd vertrouwen ik carte blanche kreeg om met het elektronisch zenuwcentrum van een organisatie te doen wat ik wilde. 10 jaar later zie ik als auditor dat IT-medewerkers nog steeds een ongebreideld en ongefundeerd vertrouwen krijgen én dat het nog steeds heel gewoon is dat bijvoorbeeld systeembeheerders toegang hebben tot de inhoud van bestanden. Het verbaast mij dat deze verschijnselen bestaan, maar het verbaast me nog meer dat ze in brede kring, auditors incluis, worden geaccepteerd als onvermijdelijkheid. Ik zie in het onderwerp 'insider threat in IT' dan ook een onderwerp van onderbelicht belang. In reactie op mijn onderwerp wordt al snel gesproken van het belang van 'zachte factoren'. Die terminologie verbaast mij altijd: niet alleen behoren veel zogenaamde zachte factoren tot de harde realiteit, ze bepalen die realiteit zelfs in hoge mate. Wel is het zo dat ze vaak moeilijk hard te maken zijn in de zin van een bijdrage aan een deugdelijke grondslag van een oordeel.

Terwijl IT-auditors zich veelal bezig houden met risico's die door menselijk handelen ontstaan, wordt het menselijk handelen zelf zelden uitvoerig onder de loep genomen. Het lijkt me goed om daar nu de schijnwerper op te zetten.

Met dank aan Caroline Neys en Paul Samwel (Rabofacet Security Management) die aan het begin hebben meegedacht over het onderwerp (de eerste loodjes wegen vaak het zwaarst), Arno Nuijten (EURAC) voor de deskundige en zeer tijdige begeleiding, Olivier Nijland (Audit Rabobank Groep) voor zijn constructieve en positieve commentaar en Tanja de Ruijter, die naast een drukke baan en de zorg voor vier kinderen in 2003 vaak een parttime echtgenoot had.

"Auditors are not psychologists" (Bourassa)

Inhoud

Voorwoord 1
Inhoud 2
Samenvatting 3
1. Inleiding en leeswijzer 4
1.1 Inleiding 4
1.2 Leeswijzer 5
2. Vraagstelling 6
3. Afbakening en positionering van het onderwerp 7
3.1 Afbakening van het onderwerp 7
3.2 Positionering van het onderwerp 8
4. Aard en omvang van het probleem 10
5. Definities en classificatie 12
5.1 Definities van insider en insider threat 12
5.2 Classificaties 13
5.2.1 Classificatie naar motief van de insider 14
5.2.2 Classificatie naar functie van de insider 15
5.2.3 Classificatie naar operationele mogelijkheden van de insider 15
6. Theorieën en modellen 16
6.1 Overzicht 16
6.2 Psychodynamische benadering 17
6.2.1 Inleiding 17
6.2.2 Algemene kenmerken van de IT-er 17
6.2.3 Specifieke risicoverhogende persoonlijkheidskenmerken van de IT-er 17
6.2.4 Discussie 18
6.3 Statistische benadering 19
6.3.1 Inleiding 19
6.3.2 Behavioral Information Security 20
6.3.3 Discussie 21
6.4 Criminologische benadering 22
6.4.1 Inleiding 22
6.4.2 Three Dimensional Profiling 22
6.4.3 Discussie 23
6.5 Waarschijnlijkheidsbenaderingen 24
6.5.1 Overzicht 24
6.5.2 Heterogeen model van Schulz 24
6.5.3 Discussie 25
6.5.4 SKRAM-model en het Insider Threat Model for Adversary Simulation 25
6.5.5 Discussie 26
7. Normen 27
7.1 Inleiding 27
7.2 Normen 27
7.2.1 Normen: beleid en controle. 28
7.2.2 Normen: management 30
7.2.3 Normen: personeelsselectie 31
7.2.4 Normen: beheersing van risicogedrag 32
7.3 Normen uit dit referaat met COBIT vergeleken 34
7.3.1 Werkwijze 34
7.3.2 Resultaat van de vergelijking met normen uit COBIT 34
7.4 Meetbaarheid van normen 34
8. Conclusie 36
8.1 Voorkomen van opzettelijk schadelijk handelen door IT-personeel 36
8.2 Voorspellen van opzettelijk schadelijk handelen door IT-personeel 37
8.3 Epiloog 37
Geraadpleegde literatuur 39

Samenvatting

Informatiesystemen en de onderliggende infrastructuur zijn kwetsbaar voor kwaadwillig gedrag van medewerkers die normaal gesproken als vertrouwd worden beschouwd. Er is omvangrijke informatie beschikbaar over schade die is toegebracht aan organisaties door eigen medewerkers die informatie aanpassen, verkopen, gijzelen of als ex-medewerker het netwerk en de systemen hacken. Uit onderzoek blijkt dat de aangerichte schade door (ex-)werknemers véél groter is dan de schade door externe hackers, hoewel de hoeveelheid aandacht voor de laatste het tegendeel doet vermoeden. Dit referaat gaat in op wat in de Engelstalige literatuur intussen een begrip is: 'the insider threat in IT'. De vraag die in dit referaat wordt gesteld is of kennis en begrip van dit gedrag kunnen bijdragen aan een betere beheersing van dit risico.

Tijdens het literatuuronderzoek bleek dat er veel over het onderwerp geschreven wordt, maar dat er nog vrij weinig onderzoek is gedaan. Het onderzoek dàt is gedaan biedt evenwel, in combinatie met enkele ontwikkelde relevante modellen en inzichten van deskundigen, voldoende houvast om reeds een antwoord te formuleren dat voor de IT-praktijk en voor de IT-auditpraktijk nuttig kan zijn en een uitgangspositie kan vormen voor verder onderzoek.

Een belangrijk deel van de 'malicious acts' van 'insiders' lijkt beïnvloedbaar te zijn door IT-management en derhalve ook in zekere mate beheersbaar te zijn. Er wordt vaak gedacht dat kwaadwilligen 'bij de poort' moeten worden tegen gehouden, m.a.w. door een zorgvuldige personeelsselectie toe te passen. Veel ongewenst gedrag blijkt echter tijdens het werkverband zijn ontstaansgrond te vinden. Het IT-management kan niet volstaan met het uitgangspunt dat werknemers vertrouwd kunnen worden, maar het zou inzicht moeten verkrijgen in het ontstaan van kwaadwillig gedrag en de stuurmogelijkheden daarop. Dat inzicht bevat geen kant en klare oplossing, zoals een duidelijk daderprofiel. Wel lijkt een bepaalde psychologische predispositie risicoverhogend te kunnen zijn. Het gaat daarbij om introversie in combinatie met andere factoren zoals bijvoorbeeld gebrekkige empathie of flexibele ethische opvattingen die in bepaalde omstandigheden eerder tot ongewenst gedrag kunnen leiden. Het lijkt erop dat het managen van IT-risico's ook inhoudt dat er contact onderhouden wordt met het wel en wee van medewerkers op kritische posities.

In dit referaat wordt de vraag beantwoord wat managers kunnen doen om kwaadwillig en schadelijk gedrag te voorkomen en te voorspellen. Voorkomen is in zekere mate mogelijk, voorspellen is veel moeilijker. Uit de (deel)oplossingen die hier zijn voorgesteld, worden normen afgeleid waarmee de auditor de kwaliteit van de beheersing van een aantal specifieke gedragsaspecten kan toetsen. Een confrontatie van die normen met de 'control objectives' van COBIT laat zien dat in COBIT nauwelijks aandacht wordt besteed aan het beheersing van ongewenst gedrag. Dit geeft voeding aan de gedachte dat daar in de toekomst meer energie naar uit moet gaan. Auditors zullen in de toekomst bij security management audits het gedragsaspect en de beheersing daarvan steeds minder kunnen negeren, hetgeen betekent dat het onderwerp in de opleiding tot IT-auditor ook een plaats verdient.

1. Inleiding en leeswijzer

1.1 Inleiding

In met name, maar niet uitsluitend, de Amerikaanse literatuur is de laatste tijd de aandacht gerezen voor wat wordt genoemd 'the insider threat' of 'the enemy within'. De gebeurtenissen op '11/9' zijn daar debet aan, maar reeds in 1998 zijn het Department of Defense en het adviesbureau Political Psychology Ltd. bezig met onderzoeken, het organiseren van congressen en samenstellen van werkgroepen die alle ten doel hebben om het gevaar van de 'malicious acting insider' in kaart te brengen en voorstellen te doen over de mitigatie van de bijbehorende risico's.

De casuïstiek is indrukwekkend. De fenomenen van de 'mantel der liefde' of het intern afkopen van reputatieschade ten spijt, zijn er toch zeer veel gevallen bekend, en deels ook gepubliceerd, van opzettelijke schade die een organisatie is toegebracht door een insider. De waaier van gebeurtenissen is breed: verkopen van homemade software, versleutelen van een database van een ziekenhuis en veel geld én afzien van vervolging eisen in ruil voor de decryption key (met succes), ontvreemden van instructies om een kernbom te maken, inbouwen van een softwaretijdbom na dreiging met ontslag, het versturen van geheime klantgegevens vanuit een Luxemburgse bank naar Europese belastingorganen, spioneren voor een concurrent of voor het eigen bedrijf, etc. Studierapporten [POWE, KPMG] laten zien dat het aantal 'attacks' van binnenuit weliswaar veel kleiner is dan van buitenaf, maar dat de effectiviteit en de toegebrachte schade veel groter zijn, faillissementen niet uitgezonderd.

De casuïstiek laat zien dat er sprake is van een zeer serieus probleem. Het is ook een verwaarloosd probleem, vermoedelijk vooral doordat de gemakkelijkste weg voor een IT-manager erin bestaat de eigen mensen 'domweg' te vertrouwen. Wat moet de IT-manager ook met de amorfe notie dat er een rotte appel tussen zijn personeel kan zitten? Inderdaad is de vraag opportuun: wat zou hij dan moeten doen? En wat moet een IT auditor vinden van een IT manager die niet weet wat hij moet doen? De auditor weet het waarschijnlijk ook niet.

In onderstaand literatuuronderzoek wil ik de lezer een overzicht bieden van de belangrijkste inzichten die tot op heden zijn opgedaan met recentelijk onderzoek en naar aanleiding van denkwerk dat is verricht aangaande dit onderwerp. Verder wil ik de IT auditor zo mogelijk iets meegeven waarmee hij zijn auditwerk kan verrijken. Dat klinkt aanmatigend, maar het is mijn indruk dat IT auditors bij de beoordeling van beheersingsmaatregelen de 'human factor' vaak buiten beschouwing laten. Ook aan de kant van de auditee is de 'human factor' als te beheersen element vaak afwezig. Er wordt snel vanuit gegaan dat voor ieder probleem wel een toereikende technologische oplossing bestaat. Het lijkt er soms op dat ene technologische oplossing over de andere heen struikelt[1], maar er blijven gaten bestaan én er vallen nieuwe gaten in de beveiliging. Een technologisch perspectief levert in veel gevallen hooguit een deeloplossing op. Gudaitis heeft hierover een uitgesproken standpunt: "… the individual is the root of the problem, not the advancing technologies. If the problem is human-driven, the solution must include, in part, a human solution" [GUDA]. Een voorbeeld van het tekort schieten van een technologisch perspectief betreft de vrouw die in 1997 schade toebracht aan de Amerikaanse kustwacht door een applicatie te hacken (die ze mede zelf had gebouwd). Dat was waarschijnlijk niet te voorkomen geweest door meer AO/IC-maatregelen, maar wel door haar klachten over sexuele intimidatie serieus te nemen [GUDA]. Er is met inzicht in de human factor een en ander bij te dragen aan informatiebeveiliging en derhalve aan audits die daarop betrekking hebben. De aandacht kan gevestigd

[1] Neem bijvoorbeeld ontwikkelingen als IDS (Intrusion Detection System), behavior pattern recognition en automated code review. IDS is zeer lastig (blijvend) effectief te programmeren, voor behavior pattern recognition geldt dat in nog veel sterkere mate en automated code review is blind voor malicious code met 'veilige' instructies. Het is eigenlijk niet eens nodig om de beperkingen van moderne technologie te beschouwen als we beseffen dat ook zeer ouderwetse methoden als logische toegangsbeveiliging met access control lists e.d. of loginspectie nog steeds problematisch zijn en de onberekenbare mens niet in de greep kunnen krijgen.

worden op diverse operationele terreinen: werving en selectie van personeel, managementstijl van een IT-manager, selectie en opleiding van IT-managers, pre-employment screening en during-employment screening, zorgvuldige loopbaanplanning voor IT-ers, het implementeren van nieuwe ethische contouren, IT-ers opleiden om beter met signalen in de omgeving om te gaan, etc.

Dit referaat is geschreven door een auditor en hopelijk voor een of meer geïnteresseerde auditors. Daarom staat de beoordeling aan de hand van normen centraal en worden maatregelen genoemd om tot inzicht te komen, ter adstructie en om realistische normen te kunnen opstellen. Maatregelen staan dus niet centraal, maar de normatiek van de auditor staat centraal. In het voorlaatste hoofdstuk wordt een set normen voorgesteld dat kan worden gebruikt door de auditor. Tevens wordt bezien of er aanvullingen op COBIT [ISAC] mogelijk zijn en of er een aansluiting kan worden gevonden bij de notie van Nuijten en v.d. Pijl dat het gebruik van standaardmodellen of -normenkaders waarin met het menselijk gedragsapect geen rekening is gehouden, een te beperkte beschouwing kan opleveren [NUIJ].

1.2 Leeswijzer

Tezamen met hoofdstuk 2 (Vraagstelling) vormen de hoofdstukken 6 t/m 8 de kern van dit referaat. Hoofdstuk 6 behandelt het literatuuronderzoek waarin deelantwoorden op de vraagstelling worden gegeven. Hoofdstuk 7 geeft de normen weer die afgeleid kunnen worden uit hoofdstuk 6. Hoofdstuk 8 geeft een zo volledig mogelijk antwoord op de belangrijkste en eerst vermelde vraagstelling en bevat de conclusie.

De hoofdstukken 3 t/m 5 bevatten het noodzakelijke plaveisel dat leidt naar de kern. De inhoud ervan spreekt voor zich en behandelt achtereenvolgens: bepaling en positionering van het onderwerp, probleemschets en definitie en classificatie van begrippen.

Omwille van de leesbaarheid wordt alleen de mannelijke persoonsvorm gebruikt.

2. Vraagstelling

In dit referaat zal een antwoord gezocht worden op de volgende vraag:

> *Kan een organisatie opzettelijk schadelijk handelen van IT-personeel voorkomen en voorspellen door gebruik te maken van kennis van dit gedrag en de totstandkoming ervan?*

Het resultaat wordt gepresenteerd in hoofdstuk 8.

Uit de antwoorden of deelantwoorden, zoals die gedurende het literatuuronderzoek naar voren komen, worden normen afgeleid die in hoofdstuk 7 zullen worden behandeld. In dat hoofdstuk worden de volgende vragen beantwoord:

> *Welke normen kunnen worden opgesteld die zouden kunnen worden gebruikt bij toetsing in welke mate een organisatie de risico's m.b.t. opzettelijk kwaadwillend gedrag van IT-personeel beheerst?*

> *Zijn deze normen terug te vinden in het toetsingskader van COBIT (3d ed.)?*

3. Afbakening en positionering van het onderwerp

3.1 Afbakening van het onderwerp

Het is lastig om een heldere en betekenisvolle afbakening te maken binnen het fenomeen risicobeheersing m.b.t. 'insider threats'. Vanuit de persoonlijke belangstelling is dat wel te doen, maar het is zaak om de omtrek zo te kiezen dat er een behoorlijke hoeveelheid relevante en interessante literatuur ter beschikking is.

In de voorhanden zijnde literatuur is er nauwelijks houvast te vinden voor een goede bepaling van de scope. Dat komt doordat definities vaak ontbreken en er meestal niet vanuit een welomschreven scope wordt geschreven. Onder de weinige auteurs die zich er wel druk over maken zijn Magklaras & Furnell, die een bepaalde taxonomie van cases voorstellen [MAGK], die begint bij een driedelige karakteristiek van 'misusers':

- naar rol in het systeem;
- naar reden van het misbruik;
- naar gevolgen voor het systeem.

Binnen de karakteristiek 'rol in het systeem' gebruiken zij de volgende driedeling:

- system users;
- advanced users;
- application users.

Bij nadere beschouwing valt die indeling precies samen met medewerkers in respectievelijk de verwerkingsorganisatie, de ontwikkelorganisatie en de gebruikersorganisatie zoals voorgesteld door Moonen [MOON] in het Handboek EDP Auditing, in de praktijk ook wel aangeduid als respectievelijk VTO (verwerkings- en transportorganisatie), SO (systeemontwikkelorganisatie) en GO (gebruikersorganisatie).

Binnen de karakteristiek 'reden van het misbruik' maken Magklaras & Furnell het onderscheid:

- intentional;
- accidental.

De afbakening sluit bij de bovenstaande indeling aan. We beperken ons tot de *intentional* insider threat, komende vanuit IT-medewerkers in de *verwerkingsorganisatie* en de *transportorganisatie*. Die beperking is zinvol omdat er een gemeenschappelijk kenmerk is: beide soorten insiders werken in de 'IT-keuken', zij het met verschillende potten en pannen. De medewerkers in de gebruikerorganisatie komen niet in die IT-keuken en de risico's behorend bij hun werk zijn even divers als de applicaties die ze gebruiken.

Voorts beperken we ons tot bestudering van de *menselijke factor*. Daarbinnen leggen we ons geen beperkingen op. Het pleidooi voor waarneembaarheid en meetbaarheid dat gemeengoed lijkt te zijn (zie bijvoorbeeld [AND1] of de pleidooien voor meetbaarheid op het ISACA/Eurocacs-congres 2003 in Amsterdam) snijdt veel mogelijkheden tot verwerving van kennis en inzicht af. Motieven van mensen zijn bijvoorbeeld meestal niet waarneembaar en in beperkte zin meetbaar te maken, maar ze zijn wel degelijk interessant en kunnen bijdragen aan risicobeheersing.

3.2 Positionering van het onderwerp

De vraagstelling blijkt de kern te zijn van een pas recent ontloken onderzoeksgebied[2], waarin op beperkte schaal onderzoek is verricht en aan theorievorming is gedaan, maar dat grotendeels nog bestaat uit het formuleren van wensen en hypothesen.

De 'Conference Proceedings' van een in 2000 gehouden conferentie over 'Research on mitigating the insider threat to information systems - #2' [AND1] bestond dan ook voor een belangrijk deel uit het formuleren van toekomstwensen:

- Een of meer modellen van de 'malicious insider' en kritische componenten daarin zoals:
  - menstypen;
  - gedrag;
  - kennis;
  - motivatie.
- Risicobepaling van de bedreigingen die van diverse 'malicious insiders' uitgaat.
- Richtlijnen en maatbare factoren.

Modellen zouden de volgende kritische componenten moeten bevatten:

- mensen (gedrag, kennis, motivatie);
- middelen (hardware, software, netwerken);
- omgeving (organisatiecultuur e.d.).

Modellen moeten de volgende elementen bevatten:

- waarneembaarheid en meetbaarheid;
- profielen van mensen, omgeving en middelen;
- gedragskarakteristieken;
- een aanduiding van de functie van het model ($F_{(aanduiding)}$).

Opvallend is het pleidooi voor de verzameling van meer data ter onderbouwing van het wetenschappelijk werk: "The group highlighted the need for a database of insider incidents that would be vital in creating and testing any such models." [AND1]. De wens om over meer gegevens te beschikken wordt in de literatuur diverse malen herhaald.

Het in georganiseerd verband denken over de risico's van insider threats staat in de kinderschoenen, dat blijkt ook uit de veel gelezen 'roep' om gemeenschappelijke definities en begrippenkaders, die immers aan het begin van de historie van een onderzoeksgebied thuis horen. Een van de weinigen die daar ook een praktische invulling aan geeft is Tuglular die een fijnmazig soort anamneseformulier heeft ontworpen, waarin per geval van 'computer misuse' kan worden gescoord op meer dan honderd kenmerken, waaronder ook kenmerken van de dader, profiel, rol, kwalificaties, psychologische staat, familieomstandigheden etc., alsmede o.a. kenmerken van de getroffen organisatie [TUGL]. Dit praktische voorstel staat nog vrijwel op zichzelf, het is dan ook een nieuw onderzoeksgebied.

Er lijken zich twee parallelle onderzoeksrichtingen te ontwikkelen. Enerzijds wetenschappelijk onderzoek, dat door de eisen die daaraan nu eenmaal gesteld moeten worden (objectiviteit, hoge validiteit, repliceerbaarheid, etc.) een eigen snelheid kent. Anderzijds zijn er onderzoeksactiviteiten waarin snel resultaat en directe bruikbaarheid zo belangrijk zijn dat aan wetenschappelijke eisen een lagere priori-

[2] Onderzoekers van de Syracuse University New York bevestigen de indruk dat gedragsonderzoek met betrekking tot informatiebeveiliging een vrijwel nieuw onderzoeksgebied is [STAN].

teit wordt toegekend. De dreiging van terrorisme heeft met name in Amerika waarschijnlijk deze pragmatische opvatting gestimuleerd.

De casuïstiek is, zoals reeds opgemerkt, omvangrijk. De hoeveelheid onderzoek is daarentegen nog gering en is vooral kwalitatief van aard, dat wil zeggen gebaseerd op interviews door professionele interviewers met daders. Kwantitatief onderzoek met meer dan beschrijvende waarde is nauwelijks voorhanden. Er is in de literatuur wél in ruime mate sprake van discussie, theorie-, model- en hypothesevorming. Op voorhand is dan ook niet te verwachten dat uit dit literatuuronderzoek een lange lijst met trefzekere maatregelen en onbetwijfelbare normstellingen tevoorschijn komt. Enkele deelantwoorden op de vraagstelling en enige suggesties voor normen is waarschijnlijk het best haalbare.

4. Aard en omvang van het probleem

Is er een probleem?

Er is de laatste 10 jaar veel aandacht aan hackers besteed en er is veel geschreven over hoe organisaties zich daartegen moeten wapenen. De boze buitenwereld mag zich altijd verheugen in veel aandacht en budget van het management, de insider krijgt beduidend minder aandacht, zo blijkt vaak tijdens IT audits. Mogelijk zijn het amorfe karakter van de outsider en zijn anonimiteit angstwekkender dan collega's met een gezicht en bekende menselijke trekjes. Thomsen [THOM] merkt op dat keurige en vertrouwde medewerkers die over de schreef gaan nu eenmaal minder nieuwswaarde hebben dan 13-jarige jochies die het Pentagon hacken. Meer nieuwswaarde betekent echter niet: meer risico.

Vooral in de Amerikaanse literatuur is de omvang van het probleem van de 'insider threat' goed zichtbaar gemaakt. In Nederland wordt er ook over geschreven. In de Monitor Internetbeveiliging, het eindrapport van een studie door KPMG in opdracht van het Ministerie van EZ, wordt de kwetsbaarheid van het bedrijfsleven in relatie tot Internet weergegeven [KPMG]. Daarin wordt opgemerkt dat 16% van de beveiligingsincidenten door insiders wordt veroorzaakt. Neys komt in een studie naar de invloed van regels op security awareness en gedrag tot de conclusie dat binnen de Rabobankorganisatie 6% van de overtredingen van beveiligingsregels door insiders "met boze opzet" gebeurt [NEYS]. In 2002 heeft het Computer Security Institute (CSI) in samenwerking met de FBI een 'Computer Crime and Security Survey' uitgevoerd [POWE], waarin van 1996 tot en met 2002 data worden gepresenteerd met betrekking tot beveiligingsincidenten. Het percentage attacks door een insider is weliswaar dalende, maar is niettemin substantieel: in 2000 gaf 71% van de respondenten (455 bedrijven en organisaties) aan dat ze last hadden gehad van insider attacks, in 2001 was dat percentage 49% en in 2002 38%. Verton [VER1] betoogt dat door steeds groter wordende kennis van medewerkers in combinatie met het gebruik van steeds geavanceerdere hulpmiddelen, de gevaarlijke insider is veranderd in iemand wiens activiteiten effectiever worden en moeilijker te detecteren. Met andere woorden, er wordt steeds minder gedetecteerd maar er gebeurt misschien steeds meer. Om een indicatie te geven van het gemiddelde jaarlijkse verlies door 'unauthorized insider access': in 1998 bedroeg dat bijna 3 miljoen dollar per bedrijf, ongeveer het tienvoudige van de gemiddelde jaarkosten door financiële fraude in 1998. Proctor, auteur van het Practical Intrusion Detection Handbook, zegt dat hoewel hackers een toenemende bron van ergernis zijn, 85% tot 90% van de verliezen door insiders worden veroorzaakt [COH1]. Het meest overtuigend is de opsomming door Gudaitis, die diverse statistieken bij elkaar heeft gezocht, zie voor referenties [GUDA]:

- 57% van de aanvallen en 66% van de netwerkaanvallen komt van binnenuit;
- de belangrijkste aanvaller is de 'disgruntled employee' ofwel de gefrustreerde medewerker;
- 80% van de respondenten noemde de gefrustreerde medewerker als bron van een incident;
- 82% van verlies door computercriminaliteit komt door gefrustreerde medewerkers, 2% van de concurrentie.

Lang niet alle cases komen aan het licht en bovendien is niet alles uit te drukken in financiële schade. Het verkopen van de bedrijfsapplicaties van Lucent Technologies aan een soortgelijk bedrijf in Beijing heeft het internationale handelsverkeer mogelijk op een niet vast te stellen manier beïnvloed. Dat geldt ook voor cases waarbij sales databases of geheime formules worden doorverkocht. In de case uit de inleiding waarin iemand een database met patiëntgegevens 'gijzelde' door encryptie was de gezondheid van mensen in gevaar, het is niet zinvol om aan zo'n case een geldbedrag te verbinden.

Een insider threat van een geheel andere en meer alarmerende soort is de terrorist. In de Volkskrant van 2 juli 2003 [BURG] meldt computerbeveiliginsexpert en oud-KGB-agent Sheymov dat zich onder gearresteerde verdachte terroristen steeds vaker computerprogrammeurs bevinden. Oud-directeur van de CIA Woolsey meldt in hetzelfde artikel dat het hogere middenkader van Al Qa'ida veel computertechnici bevat. Verton [VER2] is bezorgd over gaande geruchten dat Al Qa'ida mollen bij Microsoft

heeft werken die Trojan Horses in Windows XP introduceren. Microsoft ontkent het gerucht, maar het gerucht is moeilijk te ontzenuwen omdat lidmaatschap van een terroristische organisatie geen formele registratie vereist.

Er is dus een probleem.

5. Definities en classificatie

5.1 Definities van insider en insider threat

Het is opvallend met welk gemak de begrippen 'insider' en 'insider threat' worden gebruikt zonder definitie te geven. Het is niet zonder belang om dat te doen, immers organisaties bestaan niet (meer) zwart-wit uit insiders en outsiders. Er zijn consultants, er zijn gedetacheerde programmeurs, er zijn dienstverlenende technici van buiten, er is de online support van de pakketleverancier die bereid is om te allen tijde in het systeem mee te kijken, er is steeds meer outsourcing, etc. Vanuit het oogpunt van controletechnische functiescheiding is het begrip insider bovendien te weinig verfijnd omdat er intern relatieve insiders en outsiders moeten zijn op het niveau van afdelingen, op het niveau van functies binnen applicaties, etc. Het is derhalve van belang om van een definitie uit te gaan, ten behoeve van gemeenschappelijk begrip in de praktijk en ten behoeve van de wetenschap om onderzoek repliceerbaar en opvolgbaar te maken.

Cohen [COH2] doet als een van de weinige auteurs een poging tot een volwaardige definitie: *"Employees, board members and other internal team members who have legitimate access to information and/or information technology. Insiders typically have special knowledge of internal controls that are unavailable to outsiders, and they have some amount of access. In some cases, they perform only authorized actions as far as the information systems have been told. They are typically trusted and those in control often trust them to the point where placing internal controls against their attacks are considered offensive".*

Interessant is dat het begrip 'trusted' wordt gebruikt als belangrijk attribuut van de insider. Hundley & Anderson [HUND] vragen zich in een artikel over vijandige outsiders in cyberspace (dat ze vergelijken met het Wilde Westen waar wetteloosheid heerste en ieder zichzelf moest bewapenen) af wat de zin is van het begrip 'trusted insider' bij grote organisaties. Binnen bedrijven als Microsoft met 100.000 werknemers of andere giganten als SUN of Cisco verliest zo'n begrip "force and focus" [AND2]. Het attribuut 'trusted' lijkt inderdaad niet erg bruikbaar, ook binnen kleine organisaties is het een attribuut dat niet goed hard te maken is.

Tuglular benadrukt het overtreden van de gebruikersrichtlijnen (policies) [TUGL]:

"Insider computer misuse may be defined as an act, directed at or committed with a computer system, violating the insider computer use policies defined by the organisation that own the computer system"

De relatie met interne regelgeving is 1:1, hetgeen dus hoge eisen stelt aan de regelgeving.

Anderson benadert de kwestie analytisch en stelt vast dat de term 'insider threat' op zichzelf een veel te brede connotatie heeft om bruikbaar te zijn [AND2]. Hij stelt voor om eerst de omgeving te definiëren waarbinnen de insider acteert (physical access, logical access or perimeter, technical environment, law enforcement environment) en vervolgens de insider te definiëren naar de volgende beschrijvende parameters:

- soort gebruik: normaal, abnormaal (fouten zonder opzet) en kwaadwillend (fouten met opzet);
- mate van vaardigheid: novice of gevorderd;
- kennis van de omgeving;
- rechten (fysiek en logisch);
- mate van affiliatie met de organisatie;
- soort actor (mens, programma, middleware, etc.).

De notie dat het opstellen van een definitie nodig is én geen eenvoudige zaak is, is de belangrijkste bijdrage, een definitie wordt niet gegeven.

Er zijn nog wel enkele definities van insider attacks te vinden, maar die voegen helaas weinig toe aan een nauwkeuriger bepaling van wat onder een insider moet worden verstaan. Het veel gebruikte begrip 'attack' wordt ook globaal gedefinieerd, bijvoorbeeld als "intentional misuse of computer systems" [SCHU]. Alleen Anderson besteedt gedetailleerd aandacht aan de definitiekwestie in een verslag van een 3-daagse conferentie over 'insider misuse' van kritische defensie-informatiesystemen [AND2], maar na een uiteenzetting van verschillende perspectieven beperkt hij zich uiteindelijk tot het stellen van vragen en komt niet tot een definitie. Moet je de grens trekken bij de logische omtrek van een organisatie (firewalls, toegangssoftware e.d.) of moet je de grens juridisch trekken: is de insider iemand met een arbeidsrechtelijke relatie met de informatie-eigenaar? De definitie van het DoD (Department of Defense in de VS) werd in genoemde conferentie gebruikt als werkdefinitie:

"Anyone who is or has been authorized access to a DoD information system whether a military member, a DoD civilian employee, or employee of another Federal agency or the private sector".

Erg werkbaar voor algemene doeleinden is deze definitie niet. Tijdens de conferentie werden nog de volgende definities gegeven.

"Insider: any authorized user who performs unauthorized actions."
"Insider threat: any authorized user who performs unauthorized actions that result in loss of control of computational assets."

De 'insider' valt hier samen met de 'malicious insider'. Dat kan gemakkelijk tot verwarring leiden, bovendien zijn deze definities te algemeen.

Als een goede algemeen bruikbare definitie niet voorhanden is, moet deze geformuleerd worden. Hoewel het begrip 'trust' [COH2] een moeilijk werkbaar begrip lijkt te zijn, kan toch niet worden genegeerd dat het cruciale verschil met de outsider ligt in vertrouwen en andere gedragsverwachtingen dan van de outsider. Bij de insider bestaan andere gedragsverwachtingen door een sollicitatieproces, door het eventueel tekenen van een gedragscode, door persoonlijke contacten, door deelname aan een aanwezige of veronderstelde gemeenschappelijke bedrijfscultuur en doordat hij parallelle belangen heeft met zijn werkgever. Dat leidt tot de volgende werkdefinitie binnen het kader van deze tekst:

Een insider is een legale werknemer[3] die toegang heeft tot delen van de technische en logische infrastructuur en van wie verwacht wordt dat hij zich aan de geschreven en algemeen aanvaarde ongeschreven regels van de organisatie houdt. Er is sprake van een insider threat als de insider die regels bewust overtreedt en daarmee de organisatie met opzet schaadt.

Het onderwerp van deze tekst beperkt zich derhalve tot de 'malicious insider' die bewust en met kwade opzet handelt binnen het IT-domein, de tijdelijke medewerker, de ingehuurde medewerker en de medewerker bij een outsource-dienstverlener inbegrepen.

5.2 Classificaties

De werkelijkheid is te complex om vanuit één perspectief te kunnen begrijpen. Een zinvolle manier om de werkelijkheid te benaderen is vanuit verschillende perspectieven op de insider. In de literatuur zijn enkele classificaties (een iets concretere aanduiding dan perspectief) voorgesteld, die hieronder worden gepresenteerd en kort toegelicht.

[3] Sollicitanten worden ook in beschouwing genomen. Hoewel een insider threat vaak gedurende een dienstverband blijkt te ontstaan, kan die natuurlijk ook 'binnengehaald' worden. Een definitie van een sollicitant is bijvoorbeeld: "iemand die naar een baan dingt" [KRUY].

Behalve dat een classificatie kan helpen om de werkelijkheid in een zekere omvang te kunnen bestuderen of 'behappen', heeft de ene classificatie misschien meer verklarende waarde dan de andere. Misschien verklaart (en voorspelt) een indeling als gebruiker/ontwikkelaar/beheerder veel meer dan een indeling naar motieven (hebzucht/wraak/verhoging hackerstatus/etc.). Helaas is er tot 2003, voor zover bekend, geen onderzoek gedaan dat hier iets zinnigs op kan zeggen. Wel is het zo dat toekomstige onderzoekers bij het kiezen van steekproefgroepen een bewuste keuze moeten maken uit één classificatie om de kans op verklarende waarde vergroten.

De classificaties laten zich verdelen naar:

- motief van de insider;
- functie van de insider;
- operationele mogelijkheden van de insider.

5.2.1 Classificatie naar motief van de insider

Albert & Dorofee komen tot de volgende classificatie [ALBE]:

1. Disgruntled employees - people within the organisation who deliberately abuse or misuse computer systems and their information.
2. Attackers - people who attack computer systems for challence, status or thrill.
3. Terrorist - people who attack computer systems to cause fear for political gain.
4. Vandals - people who attack computer systems to cause damage.
5. Criminals - people who attack computer systems for personal financial gain.
6. Spies - people who attack computer systems for political gain.

Shaw, Post & Ruby hebben een intensieve studie gedaan naar de psyche van de kwaadwillende insider (zie het volgende hoofdstuk). Ze presenteren naar aanleiding daarvan een classificatie op grond van motivatie [SHA1, SHA2, MILL]:

1. Hackers. Hoewel een hacker geen insider is, zijn er veel gevallen bekend van ex-werknemers die na hun onvrijwillige vertrek het netwerk van de ex-werkgever hebben gehackt. Verder kan een hacker een insider worden als hij gewoon in dienst treedt bij een organisatie. Hackers en dan met name de hackers die aan een hackersgroep zijn verbonden, zijn vaak sterk gericht op het opzoeken van grenzen, ook de grenzen van autoriteiten en kunnen sterk gemotiveerd worden door de goedkeuring door en status binnen de eigen hackersgemeenschap. Hackers richten binnen een normale werkomgeving meestal geen schade aan, maar doen dat wel als ze een 'disgruntled employee' (ontevreden werknemer) zijn geworden.
2. Machiavellianen. Mensen die hun functie gebruiken om een ander doel (eigen positie, aanzien, carrière) te bereiken dan de doelen van de organisatie waarvoor men werkt. Er zijn gevallen bekend van werknemers die met opzet crisissituaties veroorzaken die alleen zij kunnen oplossen, waardoor hun aanzien stijgt. Er zijn andere gevallen bekend waarin consultants tijdbommen of conditionele bommen (programmatuur met een desastreus effect, die in werking treedt op een bepaald moment of onder een bepaalde voorwaarde) plaatsten om betaling af te dwingen respectievelijk om wraak te nemen als er geen betaling plaats vindt.
3. Bijzondere Mensen. Mensen die zichzelf boven de regels verheven achten. Een subset is de 'proprietor': de man die zich zo vereenzelvigt met de systemen, dat hij meent dat het zijn eigendom is. Hoewel hij in het algemeen waardevolle bijdragen levert, kan hij snel ontgoocheld raken als zijn gevoel bijzonder te zijn ondermijnd wordt, bijvoorbeeld als de bijzonder beloningen (extra grote auto, loftuitingen, business class vliegen, uitverkoren worden voor bijzondere taken, etc.) uitblijven, kan deze persoon snel ontgoocheld raken en zeer ongewenst gedrag gaan vertonen in de zin van een 'insider threat'.

4. De Snelle Wraaknemer. Werknemers die bij een teleurstelling snel en hard toeslaan. Opvallend daarbij is dat de teleurstelling eerder subjectief dan objectief is, dat wil zeggen anderen zien de grond of redelijkheid van de teleurstelling niet. Er kan van bitterheid sprake zijn die kan leiden tot sabotage, spionage, diefstal, fraude en afpersing.
5. Carrièredieven. Heeft bij aantreden zijn eigen doelstellingen die alleen het eigen voordeel dienen, heeft geen relatie met het werk.
6. Mollen. Werknemers die spioneren voor een andere werkgever, vreemde overheid of als freelancer in opdracht.

Er is sprake van gedeeltelijke overlap met Albert & Dorofee, bijvoorbeeld spies/mollen of criminals/carrièredieven. Er zijn 9 verschillende klassen te onderscheiden.

5.2.2 Classificatie naar functie van de insider

Roebuck maakt een indeling op grond van rol of positie en verbindt er tegelijk een risico aan [ROEB]:

1. Programmeurs en databasespecialisten, gewoonlijk gezien als 'high risk' maar volgens Roebuck niet, als standaardbeheersingsmaatregelen zijn genomen.
2. Managers vormen een groter risico, ze combineren soms bijzondere rechten in productiesystemen met relatief veel kennis van de bedrijfsprocessen en geautomatiseerde functies.
3. Systeemanalisten en -ontwerpers hebben kennis van controles op functioneel niveau en de zwaktes daarin en vormen derhalve een potentieel risico.
4. Gebruikers, met name degenen switchen tussen operationele afdelingen vormen een serieus risico (maar vallen buiten de afbakening van dit referaat).
5. Systeembeheerders vormen een hoog risico omdat ze vaak onbeperkte rechten hebben, in combinatie met kennis van de bedrijfsprocessen en -controles is het risico hoger.

Deze classificatie sluit goeddeels aan bij de indeling gebruikersorganisatie, ontwikkelorganisatie en verwerkingsorganisatie van Moonen [MOON]. Als er een relatie zou zijn met soorten daden en de waarschijnlijkheid ervan, zou dat vanuit managerial oogpunt handig zijn.

5.2.3 Classificatie naar operationele mogelijkheden van de insider

Anderson stelt voor om te onderscheiden naar [AND2]:

1. Soort gebruik: normaal, abnormaal (fouten zonder opzet) en kwaadwillend (fouten met opzet). Alleen de laatste valt binnen de afbakening van dit referaat.
2. Mate van vaardigheid: novice of gevorderd.
3. Kennis van de omgeving.
4. Rechten (fysiek en logisch).
5. Mate van affiliatie met de organisatie.
6. Soort actor: mens, programma, middleware, etc. Hoewel Anderson hier een punt heeft om bij stil te staan, valt het buiten de afbakening van dit referaat dat de insider definieert als mens.

Ook deze classificatie zou, als er een relatie is met soorten daden en de waarschijnlijkheid ervan, goede handvaten kunnen bieden.

6. Theorieën en modellen

6.1 Overzicht

In de literatuur zijn enkele theorieën[4] en modellen gevonden die voldoende inhoud lijken te hebben om iets te kunnen bijdragen aan beantwoording van de vraagstelling. Opgesomd zijn dat de volgende:

- Psychodynamische benadering.
- Statistische benadering.
- Criminologische benadering.
- Voorwaardenbenaderingen.

Om te beginnen is er een *psychodynamische benadering*, waarbij vooral in de psyche van de dader wordt gekeken. Het leidt tot een bepaalde profilering van daders. De term psychodynamisch wijst op een stroming in de persoonlijkheidsleer waarbij de psychische fenomenen in de persoon worden beschreven en verklaard. Bekende psychologen als Freud, Jung, Adler en Euler kunnen tot die richting worden gerekend. Er is veel wetenschappelijke kritiek op deze richting, omdat de bevindingen en verklaringen niet of nauwelijks bewijsbaar en repliceerbaar zijn. Het gedachtengoed spreekt wel sterk tot de verbeelding en heeft ingrijpende maatschappelijke gevolgen[5]. Een kijkje in de hoofden van daders door deskundigen levert dan ook iets interessants op.

De *statistische benadering* is een inspanning om gedragingen in relatie tot informatiebeveiliging op een wetenschappelijk/statistische manier te ordenen. Het levert een gedragstaxonomie op die iets te betekenen heeft voor de vraagstelling. De onderzoekers noemen hun aanpak Behavioral Information Security.

Voorts is er een *criminologische benadering*, een profilering van personen en relevante factoren in de omgeving levert een model op dat verklarend en voorspellend kan zijn. De benadering heet binnen de criminologie Three Dimensional Profiling.

Tenslotte worden drie modellen gepresenteerd die *waarschijnlijkheidsbenadering* kunnen worden genoemd. Beide beschrijven een aantal voorwaarden waaraan moet zijn voldaan alvorens een insider threat manifest wordt. Ze verschillen in de voorwaarden en in het mechanisme. De eerste, het SKRAM-model noemt 5 voorwaarden die alle noodzakelijk zijn. Het Insider Threat Model for Adversary Simulation voegt hier nog iets aan toe. De derde, het heterogeen model van Schulz, noemt een aantal voorwaarden die geen van alle noodzakelijk zijn, maar de optelsom van de mate waarin aan de voorwaarden is voldaan leidt tot een waarschijnlijkheid van manifestatie.

[4] Een theorie wordt hier opgevat als systeem van denkbeelden of hypothesen ter verklaring van waargenomen verschijnselen of feiten [KRUY].

[5] Zo komt het begrip ontoerekeningsvatbaarheid in het strafrecht mede voort uit de veronderstelling dat er onbewuste krachten in de mens leven waar hij zelf geen weet van heeft, die hij niet kan besturen en hem dus ook niet aan te rekenen zijn. Die gedachte is van Freud afkomstig is. In de geschiedenis van de psychologie is er een tegenstroming geweest, het Behaviorisme dat uitsluitend wilde uitgaan van het zintuiglijk waarneembare. Deze stroming geeft vaak te beperkte resultaten; in extreme vorm kent het geen aanhangers meer.

6.2 Psychodynamische benadering

6.2.1 Inleiding

In 1997 is door het Department of Defense (DoD) in de Verenigde Staten is een opdracht verstrekt aan E. Shaw (hoogleraar klinische psychologie), J. Post (psychiater) en K. Ruby (onderzoeker van o.a. hackers en groepsdynamica bij terroristen) van de University of Washington. De opdracht was het gevolg van de toenemende zorg binnen het ministerie over het toenemend aantal 'insider violations' met de bedoeling om inzicht in de psychologie van daders en voor zover mogelijk generieke profielschetsen te verkrijgen. Die profielschetsen zouden een bijdrage kunnen leveren aan het beveiligingsbeleid van overheid en bedrijfsleven en aan maatregelen ter afschrikking of detectie van sabotage, spionage, fraude, diefstal en afpersing.

Uit een pool van 100 zijn 46 daders uitgebreid geïnterviewd. De bevindingen uit die interviews zijn gecombineerd met rapportages opgesteld door onderzoekers, aanklagers en beveiligingsspecialisten. Het resultaat [SHA1, SHA2] levert een aantal verrassende inzichten op, die hieronder worden weergegeven. Eerst wordt een beeld geschetst van relevante psychologische kenmerken die vaak bij IT-ers worden aangetroffen en die een voorwaarde vormen voor gedrag dat vooral in specifieke situaties ontstaat. De onderzoekers putten hierbij uit eerder onderzoek naar algemene kenmerken van IT-ers dat door hen is uitgevoerd in een andere (niet nader genoemde) context.

6.2.2 Algemene kenmerken van de IT-er

Psychologische assessments van programmeurs, systeembeheerders, informatica-wetenschappers en -studenten laten een gemeenschappelijk trek zien: introversie. Vanuit managementoogpunt is introversie een kenmerk waar rekening mee kan worden gehouden omdat er veelal een aantal andere verschijnselen mee gepaard gaat. Een introvert persoon is minder sociaal vaardig en is gevoeliger voor stressfactoren op het werk. Hij gaat ook op een andere manier om met stress en frustraties dan anderen. Frustraties worden niet snel op een openlijke en constructieve manier besproken met leidinggevenden. De introvert bespreekt problemen niet snel met de leiding maar eerder met een 'peer', direct of via e-mail.

Door het centraal stellen van het begrip introversie, rijst de vraag wat dat precies is. Introversie is in de persoonlijkheidsleer een reeds lang aanvaard begrip. De Zwitserse psychiater Carl Jung meldde begin vorige eeuw reeds [MISC] dat introverte mensen sterk geneigd zijn zich in zichzelf terug te trekken in geval van emoties of bij een conflict. De Amerikaanse psycholoog en onderzoeker Hans Eysenck [MISC] specificeert introversie bijvoorbeeld als 'reserved, unsociable, thoughtful en pessimistic' tegenover extraversie als 'talkative, sociable, impulsive, optimistic'. Behalve dat de polariteit introversie-extraversie een oud psychologisch begrip is, is het ook een psychologisch construct, dat wil zeggen dat het bestaan door statistisch wetenschappelijk onderzoek is aangetoond, zoals mede blijkt uit het feit dat het een onderdeel is in enkele door de CoTaN (Commissie Testaangelegenheden Nederland van het Nederlands Instituut voor Psychologie) erkende psychologische tests zoals de Minnesota Multiphasic Personality Inventory [NUTT] en de Amsterdamse Biografische Vragenlijst [WILD].

6.2.3 Specifieke risicoverhogende persoonlijkheidskenmerken van de IT-er

Introversie is op zich een neutraal attribuut en is wijdverspreid. De groep van voornamelijk introverte IT-ers bestaat dan ook vooral uit eerlijke en gezagsgetrouwe mensen. De combinatie met een of meer andere specifieke kenmerken levert een verhoogd risico op. Bij de kleine subgroep die tot 'malicious acts' of kwaadwillige acties over kan gaan, zijn 6 risicoverhogende factoren te onderkennen:

1. *Een geschiedenis van persoonlijke frustraties.* Veel van de overtreders hadden een historie van gezinsproblemen, problemen op school en op het werk, die leiden tot een negatieve houding tegenover gezag. Deze gegevens zijn in lijn met wat een andere onderzoeker onafhankelijk van hen heeft gevonden (behalve de naam Prof. Caldwell ontbreken referenties). Een subgroep van IT-ers kan worden geïdentificeerd die zich niets van autoriteit aantrekt, vaak boos is en 'poised to strike out at the system'. Caldwell spreekt ook van een 'revenge syndrome'. Hoewel niet duidelijk is wat hier nu precies bedoeld wordt, is de tendens zichtbaar.
2. *Computerafhankelijkheid.* Psychologisch onderzoek (helaas ook zonder referenties) laat zien dat computerverslaafden een grotere kans hebben op agressie en eenzaamheid, maar belangrijker in dit verband, primaire belangstelling hebben voor doorbreken van security, hacken en exploreren van netwerken. Dit vonden de auteurs ook bij hun 46 geïnterviewde overtreders. Een extra risico is de vatbaarheid voor manipulatie door bewuste zoekers van teleurgestelde werknemers via chatboxen en andere anonieme media om hen in te zetten voor spionage en fraude.
3. *Flexibele ethiek.* In lijn met de bevindingen van Shaw, Post & Ruby vond S. Harrington in 1995 dat 7% van de IT-ers geen bezwaar had tegen het kraken van computers, sabotage en spionage. Kraken wordt gezien als een eerlijke strijd van aanvaller tegen verdediger zonder dat ethiek kennelijk een rol speelt, alsof het spel is. Sociale factoren die aan deze houding bijdragen zijn gebrek aan aandacht voor computerethiek binnen bedrijven, gebrek aan specifiek beleid en regels op het vlak van security, gebrek aan legale straffen en anonimiteit van het slachtoffer.
4. *Verminderde loyaliteit.* In een studie naar computerfraude bij het U.S. Department of Health and Human Service in 1986 bleek dat loyaliteit met het bedrijf een rol speelt, maar dat programmeurs zich in het algemeen meer bij hun beroepsgroep dan bij hun bedrijf betrokken voelen. Verminderde loyaliteit leidt vaak tot verminderde conformiteit aan geschreven en ongeschreven bedrijfsregels.
5. *Bijzondere rechten.* Veel overtreders menen bijzondere mensen te zijn, die recht hebben op overeenkomstige erkenning en privileges en op een uitzonderingspositie. Zij gingen eerder tot 'malicious acts' over nadat ze zich niet goed behandeld of achtergesteld voelden, terwijl daar volgens anderen in hun werkomgeving geen sprake van was. Corresponderend hiermee zijn twee kenmerken die Gelles vond bij 98 oorspronkelijk loyale werknemers die tot spionage waren overgegaan[GELL]:
   - *Antisocial personality disorder*: het zich verheven voelen boven regels.
   - *Narcissism*: een sterke discrepantie tussen het zelfbeeld en het beeld dat anderen hebben, leidend tot een belemmering voor normale relaties, die immers een bedreiging kunnen vormen voor het gekoesterde zelfbeeld. Narcisten erkennen wel regels, maar vinden zichzelf van een bijzondere categorie voor wie de regels niet gelden. Gelles noemt twee factoren die de genoemde predisposities tot een risico kunnen maken: persoonlijke, financiële of carrièrecrisis. Een risico is ook het onvermogen van de organisatie om te zien dat er bij een collega een ongewenste ontwikkeling gaande is die een bedrijfsrisico kan vormen.
6. *Gering empathisch vermogen.* Bij overtreders werd vaak een gering vermogen aangetroffen om zich iets aan te trekken van gevolgen van de eigen daden voor anderen.

6.2.4 Discussie

De vraagstelling van dit referaat vindt hier een aantal positieve antwoorden. Kan een organisatie opzettelijk schadelijk handelen van IT-personeel voorspellen en voorkomen door gebruik te maken van kennis van dit gedrag en de totstandkoming ervan? De psychodynamische benadering biedt aanknopingspunten voor de praktijk. Bij de personeelsselectie of interne positiewijzigingen kan expliciet worden gelet op de specifieke risicoverhogende factoren in combinatie met introversie bij de kandidaat. Bij 'zittende' werknemers ligt er een taak voor het management om een openhartig contact op te bouwen, teneinde een permanente risicoinschatting te kunnen doen. Dat is van belang omdat veel 'malicious insiders' niet kwaadwillend binnenkwamen, maar dat werden als gevolg van werksituaties of behandeling door meerderen. Het opbouwen van een openhartig contact is diverse redenen aanbevelenswaardig, alleen om reden van risicoinschatting komt zoiets niet gemakkelijk hoog op de priori-

teitenlijst van een drukke manager. Vanuit het standpunt van de auditor is het van belang dat de manager zijn risico's kent en zinnige adviezen krijgt, daarmee heeft hij zijn werk gedaan.

Er zijn diverse kanttekeningen te maken. Ten eerste voor de praktische toepasbaarheid:

- Wie kan een betrouwbare inschatting maken van de psychologische staat van een medewerker? Vereist dat niet een speciale kwalificatie en/of opleiding? Bourassa vindt, in een algemeen artikel over de 'human risk factor' in het kader van interne controle, dat het beoordelen van human risk factors thuis hoort bij human resource specialisten [BOUR]. De IT manager is dus niet zomaar geschikt. Gudaitis waarschuwt daarbij nog dat HR-specialisten in het algemeen ook niet zijn opgeleid in 'psychological assessment' [GUDA]. Als we deze oplopende lijn volgen, zouden we kunnen concluderen dat een auditor op dit vlak de hoogste eisen moet stellen en het beoordelen van mensen moet voorbehouden aan medewerkers die geschoold zijn in psychodiagnostiek. Voor de praktijk is dat echter geen realistische optie, niet ieder bedrijf kan zich dat veroorloven. De auditor zou kunnen volstaan met de eis dat de aanpak is beoordeeld en goedgekeurd door een deskundige.
- Wat is de voorspellende waarde van de kenmerken? De predictieve validiteit van de profilering is niet door onderzoek vastgesteld. Daar schuilt een gevaar in van onzorgvuldig en ondeskundig gebruik.

Ten tweede is, naast de predictieve validiteit, de inhoudsvaliditeit onbekend. Eigenlijk moeten we maar op het gezag van de onderzoekers afgaan.

- De meest uitgesproken criticus is Gudaitis. De sterke nadruk op persoonskenmerken (met name introversie) vindt hij veel te simpel [GUDA]. Er zijn meerdere factoren die in hun samenhang moeten worden bekeken: individu, organisatie en maatschappij.
- Gudaitis vindt voorts een statische benadering van de persoonlijkheid geen juiste weergave van de realiteit: "The individual is a dynamic entity. Although some core personality traits may always exist with an individual, change is always occurring. An individual's charachteristics, skills, traits, personality, behavior, motivations and expectations are shifting and altering. Due to this dynamic phenomenon, a single profile can not be generated for a criminal - conventional or cyber." Tenslotte wijst hij op het gevaar van generalisaties vanuit een te eenvoudig daderprofiel.

Vanuit wetenschappelijk oogpunt is er wel wat af te dingen op de onderzoeksmethode, waarover door de onderzoekers ook nog eens weinig gedetailleerde verantwoording wordt afgelegd. De kritiek is terecht. Dat neemt niet weg dat hier interessante en bruikbare resultaten liggen die, mits professioneel en zorgvuldig gebruikt, praktische waarde hebben. De kleurrijke en contrastrijke typeringen roepen wel de vraag op of er niet naar een opdracht toegewerkt is om zoveel als mogelijk iets tastbaars en bruikbaars op te leveren. Het is te hopen dat de realiteit daarbij volledig in haar waarde is gelaten én het is te hopen dat critici een serieuze poging ondernemen om de resultaten te bevestigen of te ontkrachten.

Het onderzoek is Amerikaans, maar extrapolatie naar de Nederlandse situatie is goed te maken: uit onderzoek met beroepskeuzetests sinds de 2e wereldoorlog blijkt dat de psychische opmaak van beroepsgroepen in westerse landen sterk overeenkomt [EVER].

6.3 Statistische benadering

6.3.1 Inleiding

Onderzoekers van de Syracuse University New York concluderen na een literatuurverkenning dat het dominante perspectief op informatiebeveiliging systeemgericht is: "Security is something that is

provided (ostensibly by technology) rather than something that is enacted by users and system administrators" [STAN]. Uitzonderingen zijn onderzoeken naar de effectiviteit van security awareness progamma's, de invloed van ethische regels en de invloed van sancties op beveiligingsgerelateerd gedrag.

De onderzoekers hebben een poging gedaan om een landkaart te maken van beveiligingsgerelateerd gedrag, zowel 'positief' als 'negatief'. Vervolgens hebben ze via statistische analyse geprobeerd categorieën bloot te leggen én onderliggende verklarende factoren voor die categorieën. Ze noemen het een 'taxonomy of information security behavior'. Ze proberen kortom een systematiek of begrippenkader vast te stellen dat als uitgangspunt kan dienen voor verder onderzoek en de communicatie erover.

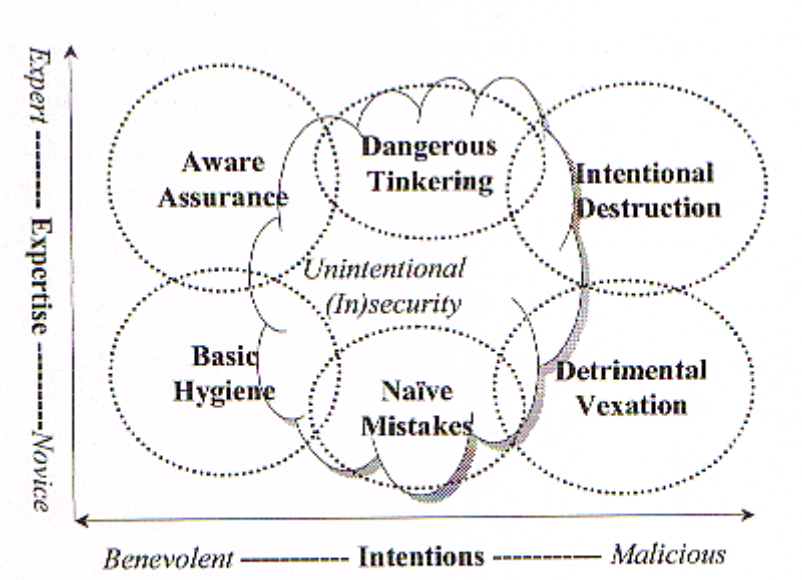
Waar de vertegenwoordigers van de psychodynamische benadering vrijelijk uitpakken met zelf gekozen en niet altijd helder omschreven begrippen, is deze benadering fundamenteler van opzet: het bestaan van onafhankelijke begrippen wordt onderzocht en van betekenis voorzien.

6.3.2 Behavioral Information Security

Het onderzoeksterrein wordt met Behavioral Information Security aangeduid. Het feitelijke onderzoek besloeg 4 fasen: inventariseren van gedragingen, hypothesevorming, toetsing, analyse.

- *Inventarisatie van gedragingen.* In 110 interviews met IT-managers en -professionals en 'regular employees' werden 82 gedragingen (later uitgebreid naar 94) geïnventariseerd die aangeduid kunnen worden als relevante en veel genoemde beveiligingsgerelateerde gedragingen. Voorbeelden: "she forged her email header information to make it look like her boss had sent a message", "he intentionally introduced a Trojan horse program into the network", "she constructively criticised organisational security policies to her boss".
- *Hypothesevorming.* Een team van 10 experts werd gevraagd de gedragingen te categoriseren. Zij deden dat met grote mate van overeenstemming, leidend tot de hypothese dat er 6 categorieën bestaan, die langs twee polariteiten zinvol gerangschikt kunnen worden. De eerste polariteit is intentionaliteit, van kwaadwillend naar goedwillend. De tweede is de mate van aanwezige kennis, van novice tot expert. Grafisch weergegeven ziet het er uit als in figuur 1. De namen van de categorieën vereisen enige uitleg: met Aware Assurance wordt bedoeld de positieve bijdrage van getraind personeel, aan het andere uiterste staat Detrimental Vexation, opzettelijk kwaadwillend gedrag van een ondeskundige. De andere 4 begrippen worden niet toegelicht, maar spreken wellicht voor zich.
- *Hypothesetoetsing.* Een groep van 49 informaticastudenten wordt gevraagd iedere gedraging te scoren op intentionaliteit en expertise met een 5-puntsschaal.
- *Analyse.* Hoewel enkele gedragingen een geringe mate van overeenstemming te zien geven, dat wil zeggen dat de respondenten ze steeds aan andere categorie toewijzen, is het overall beeld overtuigend: er zijn 6 discrete gedragscategorieën aan te wijzen.

Het is aannemelijk gemaakt dat er 6 categorieën van beveiligingsgerelateerd gedrag te onderscheiden zijn en dat ze (grotendeels) te verklaren zijn uit 2 onderliggende factoren: mate van expertise en intentionaliteit. De onderzoekers spreken van een 'manageable taxonomy' waarin de meeste gedragingen in een organisatie een plaats kunnen krijgen. Deze ordening biedt de mogelijkheid voor de praktijk om grip te krijgen op de grote diversiteit aan gedragingen, vaststellen welke maatregelen moeten worden genomen en daardoor het algemene beveiligingsniveau op peil te brengen en beleid te maken. Verder zou met het model sturing gegeven kunnen worden aan het gedrag van de medewerkers door bewust de factoren Expertise (y-as) en Intentions (x-as) te beïnvloeden.



Figuur 1: zes categorieën van informatiebeveiligingsgedrag en twee factoren (x- en y-as)

6.3.3 Discussie

Het onderzoek heeft twee belangrijke gevolgen, een die voor verder onderzoek van belang is en een voor de praktijk. Er is een stevig begrippenkader neergezet en de kwaadwillende insider is kennelijk de uitvoerder van een aangetoonde onafhankelijke gedragscategorie: hij valt onder 'intentional destruction' of 'detrimental vexation'. Voor verder onderzoek is dat nuttig.

Voor de vraagstelling van dit referaat, de praktijk dus, zijn de evalueerbaarheid en de bestuurbaarheid het algehele niveau van beveiligingsgedrag van een organisatie(onderdeel) van belang. Met gebruik van de x- en y-variabele kan een inschatting worden gemaakt van waar de organisatie staat en kan tevens sturing worden gegeven in een gewenste richting. De onderzoekers gaan helaas niet zo ver dat ze een concrete uitwerking geven van hoe je die sturing moet uitvoeren.

Als we kijken naar de x-variabele (intentions) dan behoort beïnvloeding tot de mogelijkheden: "Any interventions that shift intentionality towards the benevolent end of the continuum ought to improve the organisation's security status". Voor de kwaadwillende insider zijn de mogelijkheden echter beperkt. Dat wordt ook toegegeven: "with the exception of those employees who may have malevolent intentions".

Met de y-variabele 'expertise' is ook sturing te geven. Een beleidslijn om de algehele expertise op te voeren is gebruikelijk (ervaring, opleiding, training), maar het is ook mogelijk om de expertise te willen verlagen, hoewel dat moeilijker te realiseren is (overplaatsing, job rotation, ontslag). Uit de data-analyse blijkt overigens een verband tussen de mate van expertise en mate van maliciousness. Het verband is niet sterk en biedt beperkt praktisch nut, hooguit zou je kunnen concluderen dat je aan de 'novice' geen aandacht hoeft te schenken. Over de y-variabele, zeggen de auteurs: Het klinkt veelbelovend, maar de lezer blijft met lege handen achter omdat niet wordt uitgelegd hoe je dat moet doen.

Het onderzoek kent enige methodologische zwakten. De onderzoekers geven o.a. zelf aan dat het toetsen van een hypothese met behulp van studenten, die merendeels geen praktijkervaring hebben, niet fraai is. Verder geven ze aan dat er mogelijk nog andere categorieën bestaan, waarvan ze het bestaan niet weten. Deze voorzichtigheid is theoretisch terecht, maar de kans is niet groot gezien het aantal materie- en ervaringsdeskundigen dat ze hebben geraadpleegd. Ze geven aan dat verder onderzoek

nodig is, ook moet gekeken worden of dit onderzoek herhaalbaar is. Het is jammer dat ze uit de voorhanden zijnde data geen factoranalyse hebben uitgevoerd om te zien of er duidelijk 2 en niet meer dan 2 factoren verantwoordelijk zijn voor de variantie. Stel dat er 3 even sterke factoren zouden zijn, dan hebben ze een kans gemist op een meer volledige verklaring.

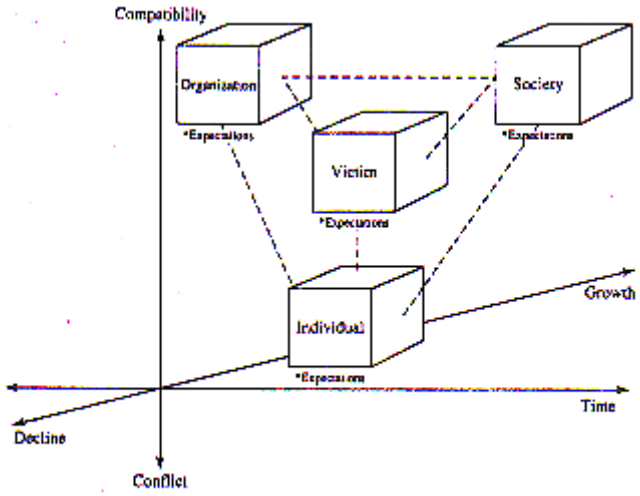
6.4 Criminologische benadering

6.4.1 Inleiding

Inkadering van waarschijnlijke daders in één duidelijk profiel zou handig zijn voor de praktijk. Gudaitis doet, in een overigens serieus artikel, een voorzet: blanke man, leeftijd tussen 25 en 42 jaar, middenmanagement, gescheiden, groene tennissokken [GUDA]. Zo eenvoudig is de realiteit klaarblijkelijk niet. De criminoloog Gudaitis meent niet alleen dat een eenvoudig daderprofiel niet bestaat, hij meent óók dat het niet volstaat om alleen de dader te profileren. Alleen een multidisciplinaire benadering, waarbij ook slachtoffer, organisatie en maatschappij in beeld worden gebracht zou tot succesvolle oplossingen kunnen leiden.

6.4.2 Three Dimensional Profiling

Gudaitis stelt een profileringsysteem voor dat de FBI's Behavioral Science Unit gebruikt voor 'gewone' criminaliteit, dat wil zeggen niet computergerelateerde criminaliteit. Een multidimensionele benadering heeft al tot veel succes geleid bij diverse typen criminaliteit, zoals sexuele vergrijpen en seriemoorden. De methode heet 3-Dimensional Profiling en is het resultaat van het combineren van kennis uit de psychologie, sociologie en criminologie.



Figuur 2: Three Dimensional Profiling

In figuur 2 wordt een manifestatie van een bedreiging weergegeven, met andere woorden een misdaad of een overtreding. Om die overtreding te kunnen begrijpen, moeten 4 elementen (kubussen) in hun onderlinge samenhang worden begrepen en dat vanuit 3 perspectieven. Hoe meer stukjes van deze puzzel we begrijpen, hoe beter we in staat zijn om te voorspellen en adequate maatregelen te treffen. Essentieel is het begrip verwachtingen in het model: het gedrag van de elementen (individu, slachtoffer, organisatie, maatschappij is sterk afhankelijk van wederzijdse verwachtingen. Een toelichting bij de elementen laat het volgende zien:

- De *Individual* is de dader, werknemer of insider. Het is van belang om zijn persoonsprofiel te kennen, zijn situatie (frustraties, loyaliteit, etc.), motieven en vooral zijn verwachtingen van de andere 3 entiteiten omdat die sturend en begrenzend zijn voor zijn handelen.
- De *Victim* is in dit geval het informatiesysteem of de informatie. Informatie of een systeem kunnen op zich geen verwachtingen hebben, maar ze zijn wel ontworpen en geïmplementeerd door mensen die verwachtingen van de omgeving hebben vertaald naar infrastructurele, applicatieve of andere maatregelen. Zo bekeken, zou je toch kunnen zeggen dat een informatiesysteem verwachtingen heeft. Op gedragingen van 'individuals' is geanticipeerd, evenals op eisen vanuit de samenleving (b.v. wetgeving) en de organisatie (regels en afspraken). Naarmate de 'individual' al deze verwachtingen doorgrondt, neemt de kans op een overtreding toe.
- *Organisation* en *Society* oefenen ook met hun verwachtingen een sturende en begrenzende invloed uit zowel 'victim' als 'individual'.

Alle elementen zijn steeds in verandering: de organisatie, de maatschappij, de persoonlijke situatie en het informatiesysteem. De tijdsfactor (x-as) moet daarom een rol spelen. De z-as growth/decline geeft aan dat iedere parameter die van invloed is op het gedrag van de 'individual' een tendentie heeft. Het beschouwen van de tendenties kan inzicht geven in het verloop van de daad, de daad gezien als inclusief een aanloopfase en afrondingsfase. Hiermee is ook aangegeven dat de feitelijke daad of overtreding een culminatie is in een reeks van gebeurtenissen/beslissingen/afwegingen gedurende een tijdstraject. Met 'compatibity/conflict' worden alle mogelijke bronnen van conflict (of overeenstemming) bedoeld die de 'individual' kan hebben binnen dit stelsel. Kennis van verwachtingen kan ook hier een belangrijke rol spelen, immers een conflict is veelal een verstoorde verwachting.

Gudaitis prijst de door hem voorgestelde methode aan omdat het iedere case vanuit diverse relevante perspectieven bekijkt en niet vanuit één of twee. Verder is de methode, zoals vanuit het gebruik in de criminologie is aangetoond, 'cross-cultural'. Hij verwijst daarbij naar het veelvuldig gebruik van psychometrie (gestandaardiseerde tests en vragenlijsten) in het kader van andere benaderingen. Psychologische tests zijn vaak niet 'cross-cultural validated'. De in de westerse psychiatrie veel gebruikte standaard voor psychodiagnostiek DSM III (Diagnostic and Statisical Manual of Mental Disorders [APA] is dat evenmin[6]. Douglas merkt in dat verband overigens op dat de Crime Classification Manual veel meer nut heeft dan DSM III [DOUG].

6.4.3 Discussie

De methodiek van Three Dimensional Profiling is een belangwekkende aanvulling vanuit de criminologie. Bij een dergelijk breed perspectief is de kans op fouten die individuen kunnen schaden kleiner dan wanneer vanuit een beperkt kader wordt gekeken. Onderzoekers, beveiligers, auditors en anderen krijgen vanuit dit perspectief de problematiek in volle omvang en dynamiek te zien. Het is niet zonder betekenis als een criminoloog over 'computer crime' zegt: "few types of crime are so complex". Het is niet onbelangrijk dat mensen, of dat nou onderzoekers, beveiligers of auditors zijn, zich met de juiste mind set en reële verwachtingen op dit gebied begeven. Simpele oplossingen passen niet in dit perspectief.

Ondanks de kritiek die Gudaitis heeft op Shaw, Post & Ruby, stellen deze wel een groot aantal praktische maatregelen voor. (Gudaitis heeft duidelijk aangegeven dat hij daar weinig in ziet.) Op korte termijn is het nut van Three Dimensional Profiling voor informatiebeveiliging dan ook niet concreet aan te wijzen en geeft het geen direct bruikbare antwoorden op de vraagstelling van dit referaat. Het voorspellen en voorkomen van opzettelijk schadelijk handelen door IT-personeel met dit model is

[6] Gudaitis weet kennelijk dat gebruik van psychologische tests veel voorkomt in dit verband. Zijn waarschuwing is dan ook terecht, zeker in een samenleving die steeds meer multi-etnisch wordt. Een voor de hand liggend en eenvoudig hulpmiddel om te gebruiken is bijvoorbeeld de (bekende) lijst van 'ten most stressfull life events' in DSM III, waarin zaken voorkomen als 'overlijden van de partner' en 'verhuizen'. Voor mensen van niet-westerse afkomst geldt misschien wel een hele andere lijst.

alleen mogelijk nadat substantiële hoeveelheden gegevens zijn verzameld en duidelijker is hoe met het model moet worden omgegaan. Als Ravestijn gelijk heeft, is de bereidheid om te investeren in beveiliging in het Nederlandse bedrijfsleven [RAVE] gering, de uitwerking van dit model ligt voorlopig bij grote onderzoeksinstituten.

De praktijk heeft wel iets gekregen om over na te denken. Een goed doordacht model van de werkelijkheid kan een remedie tegen te simplistisch denken zijn en heeft op zichzelf waarde voor de praktijk. De auditor is ook gewaarschuwd tegen het positief beoordelen van een te beperkte benadering van de werkelijkheid van computer crime die, als Gudaitis gelijk heeft, uiterst complex is.

6.5 Waarschijnlijkheidsbenaderingen

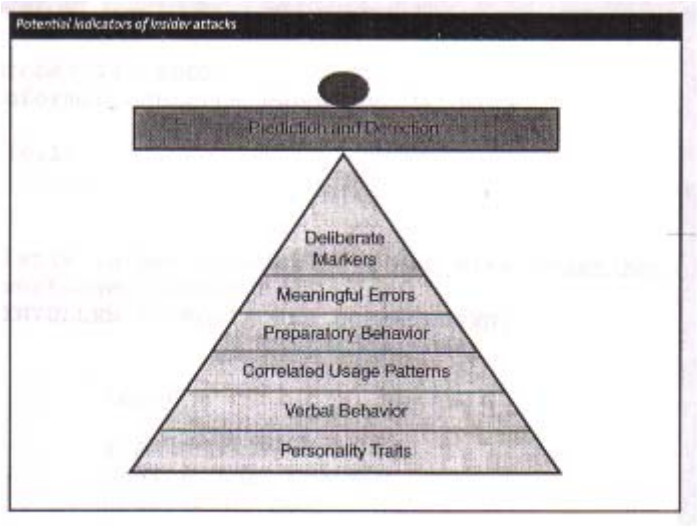
6.5.1 Overzicht

De waarschijnlijkheidsbenaderingen komen er in het kort op neer dat een aantal indicatoren tezamen een voorspellende waarde geven voor een kwaadaardige daad door een IT-er. Ze verschillen in de keuze van indicatoren en er zijn twee methodieken: de eerste (zie 6.5.2) die neerkomt op een eenvoudige optelsom en de tweede (6.5.4) die uitgaat van indicatoren die alle noodzakelijk aanwezig moeten zijn.

6.5.2 Heterogeen model van Schulz

Schulz stelt een model samen uit -voornamelijk- ideeën van anderen. Hij definieert categorieën van indicatoren zoals in figuur 3 zijn weergegeven. "From this set of indicators, clues can be pieced together to predict and detect an attack. [SCHU]" Hij veronderstelt dat kwantitatieve analysemethoden zijn model in de toekomst kunnen valideren. Hoewel de lagen in de pyramide een bepaalde relatie veronderstellen, worden die niet aangegeven, evenmin waarom voor een pyramidevorm is gekozen. De indicatoren worden als volgt door Schulz worden toegelicht:

- *Personality traits*: hoewel er potentiële ethische en andere problemen zijn, beloven deze indicatoren bruikbaar te zijn, zoals bijvoorbeeld introversie.
- *Verbal behavior*: agressief verbaal gedrag in de 'technische arena' kan in verband worden gebracht met agressief, dominant of andere soorten ongewenst gedrag [COLL] en Schulz veronderstelt dat dit type gedrag voorspellende waarde voor een aanval kan hebben. Verbaal gesproken normale, maar functioneel gezien abnormale aanvragen voor speciale autorisaties of privileges zijn ook vormen van deze indicator.
- *Correlated usage patterns*: typisch computergebruik (bijvoorbeeld gebruik van het UNIX-commando grep) op meerdere platforms kan indicatief zijn.
- *Preparatory behavior*: te denken valt aan opvallend inzamelen van informatie door iemand, door laten schemeren van intenties, maar ook gebruik van (UNIX-)commando's als whois, nslookup, finger, rwho, ping, zonder dat dat aanwijsbaar nuttig is.
- *Meaningful errors*: fouten die gemaakt worden door iemand die niet goed de weg kent (trial and error) en in logs terug te vinden zijn als a-typische sequenties van commando's.
- *Deliberate markers*: vaak worden met opzet tekens achtergelaten waaruit de identiteit van een (eventueel wraakzuchtige) dader kan worden afgeleid [SULE]. Het achterlaten van markers komt voort uit een kennelijke behoefte van de dader dat het slachtoffer weet dat hij de dader was.



Figuur 3: Heterogeen model van E. Schulz (potential indicators of insider attacks)

Schulz stelt zich voor dat als aan iedere indicator een gewicht kan worden gehangen op basis van de analyse van empirische gegevens, dat uit het model een formule kan worden opgesteld die een grote voorspellende waarde kan hebben. Als we de 6 indicatoren X_1 t/m X_6 de voorspellende waarde Y, dan kan een formule ontstaan zoals:

$Y=1{,}034 * X_1 - 0{,}588 * X_2 + 0{,}331 * X_3 + \ldots$

Hoe groter de uitkomst Y hoe groter de kans op een aanval.

6.5.3 Discussie

Op het eerste gezicht lijkt Schulz niet veel meer te doen dan het bij elkaar 'vegen' van enkele indicatoren die hij kent. Er ligt geen conceptueel kader onder zijn model, wat een inherente zwakte is waardoor het waarschijnlijk niet veel verklarende kracht zal krijgen. In de praktijk kan het misschien wel iets opleveren. De pretentie van voorspellend of detectief hulpmiddel kan niet waargemaakt worden totdat nader onderzoek met dit model op het tegendeel wijst. Voorlopig zijn het interessante aandachtspunten. Aan de nauwkeurigheid van de determinanten (3 cijfers achter de komma wordt zelden gehaald) kunnen lezers ten onrechte de verwachting ontlenen dat menselijk gedrag zeer voorspelbaar zou zijn als je maar genoeg weet, een wellicht hoopvolle maar onjuiste gedachte.

6.5.4 SKRAM-model en het Insider Threat Model for Adversary Simulation

De twee hieronder gepresenteerde modellen van Parker respectievelijk Wood vertonen sterke overeenkomsten [PARK, WOOD].

Parker beroept zich op (niet nader gespecificeerde) bronnen uit de criminologie en stelt in zijn boek "Fighting Computer Crime" vast dat mensen die zich richten op misbruik van informatie via computers (ook aangeduid als perpetrators, computer of cyber criminals) zich onderscheiden van andere (witte boorden-)criminelen door 5 kenmerken, aangeduid met SKRAM: Skills, Knowledge, Resources, Authority, Motives. Er is in zijn optiek alleen sprake van een (insider) threat als de (potentiële) dader beschikt over voldoende gehalte van de 5 kenmerken. Ze hebben de volgende betekenis:

- S. Met skills wordt bedoeld: ervaring met informatiesystemen, formele opleiding en niet in de laatste plaats social skills. Parker legt nadruk op social skills die een tekort aan andere skills tot op zekere hoogte kunnen compenseren. Social skills zijn nodig om vertrouwen te wekken en bijvoorbeeld succesvol social engineering te plegen.
- K. Knowledge ofwel kennis van de omgeving waarin wordt geopereerd en van de hulpmiddelen waarmee wordt gewerkt. Parker acht kennis van de omgeving cruciaal. Daarbij hoort ook kennis van de stabiliteit van de omgeving. Net zoals criminelen niet van een veranderende omgeving houden, houden computercriminelen daar ook niet van. Het feit dat beveiligingsmaatregelen een vaste en voorspelbare systematiek volgen en dat auditors hun bezoek altijd ruim tevoren aankondigen, helpt daarbij.
- R. Resources ofwel middelen, daarbij moet worden gedacht aan technische resources zoals een PC, netwerktoegang, terminalemulatie etc.
- A. Authority, waarmee wordt bedoeld de middelen om via identificatie en authenticatie toegang tot de informatie te krijgen.
- M. Motives, zonder motief zal iemand niet gauw een dader worden, het lijkt een obligate gedachte, maar als geen motief is, is er volgens Parker geen dader[7].

Het Insider Threat Model for Adversary Simulation van Wood voegt aan deze elementen nog toe: risk, en process. Risk houdt hier in dat de insider in hoge mate risicomijdend is: hij werkt waarschijnlijk alleen, als hij anderen betrekt dan doet hij het zo dat ze het niet weten. In het proces beschrijft Wood de processtappen 'gemotiveerd raken' 'doel kiezen' 'operatie plannen' 'aanval uitvoeren'. Opvallend is dat waar Parker zegt dat een taxonomie van motieven nauwelijks te noemen is, Wood gewoon een lijstje opsomt: 'profit' 'provoke change' 'subversion' en 'personal motive'.

6.5.5 Discussie

Het SKRAM-model blinkt uit door eenvoud: als je mocht denken dat er een 'threat' is, maar niet alle 5 elementen zijn aannemelijk aanwezig, dan heb je dus geen threat. Het heeft er alle schijn van dat Parker hier een stuk common sense expliciet heeft gemaakt, hetgeen verdienstelijk kan worden genoemd. De praktische bruikbaarheid is groot, het is gemakkelijk in te zetten. De validiteit moet echter nog vastgesteld worden

Het idee dat auditors vaker onverwacht langs moeten komen is, afhankelijk van de situatie, waard om ter harte te nemen. Wood voegt geen wezenlijk nieuw element toe aan wat Parker reeds heeft genoemd.

[7]Parker ontvouwt enige interessante gedachten met betrekking tot motieven. Hij heeft in vele interviews gemerkt dat daders bijna zonder uitzondering met grote privé-problemen hadden te kampen. Hij noemt als voorbeelden relatieproblemen en vastgelopen ambities of carrières. De carrièredief komt in zijn beleving percentueel weinig voor. Dat geldt ook voor de gelegenheidsdader. Een populaire gedachte dat de gelegenheid de dief maakt heeft zijns inziens geen geldigheid: er zijn miljoenen mensen in de gelegenheid, zonder motief worden ze zelden een dader. Opvallend is verder dat hebzucht -ook een populaire veronderstelling- zelden een motief is, is zijn ervaring.

7. Normen

7.1 Inleiding

Zoals in de inleiding van dit referaat reeds is aangekondigd en ook in de vraagstelling aan de orde komt, zal worden bezien of er iets kan worden opgemerkt ten aanzien van de gedachte dat standaard-normenkaders met het gedragsapect geen of weinig rekening houden. Deze vraag zal paragraaf 7.3 aan de orde worden gesteld. In 7.2 zullen eerst de normen worden gepresenteerd die tijdens het literatuur-onderzoek zijn gevonden of geformuleerd.

In de in dit referaat gebruikte literatuur zijn veel maatregelen en ook wel aanzetten tot normen gesuggereerd. Geen van de gevonden documenten is er expliciet op gericht geweest om normen te formuleren. De in 7.2 te presenteren normen zijn dan ook afgeleid uit de literatuur. Een aantal normen is door mijzelf geformuleerd (in de kolom 'verwijst naar' aangeduid met Spee). Het is niet de bedoeling om in 7.2 een normenkader te presenteren dat het gebied van informatiebeveiliging volledig dekt. Hier wordt slechts een subset gepresenteerd voor zover die gedestilleerd kan worden uit bovenstaande tekst en een relatie heeft met het mitigeren van 'insider threats'.

Ten behoeve van een vergelijking met een standaardnormenkader in 7.3 is COBIT gekozen. De keuze voor COBIT als vergelijkingsmateriaal komt voort uit het besef dat de 'control objectives' van COBIT een wereldwijd (en ook in Nederland) veel gebruikt normenkader vormen, ontwikkeld door de globaal georiënteerde beroepsorganisatie van IT auditors, ISACA. COBIT heeft een ontwikkeling doorgemaakt dankzij input van vele auditors uit de gehele wereld. Het antwoord op de vraag heeft daardoor meer betekenis dan wanneer een normenkader zou zijn uitgekozen dat een beperkter gebruik kent.

In de herinnering wordt geroepen dat de afbakening alleen IT-medewerkers in de systeemontwikkel- en de transport- en verwerkingsorganisatie insluit en dus de gebruikersorganisatie uitsluit.

7.2 Normen

Er worden 38 normen gepresenteerd. De normen zijn ingedeeld naar eigen inzicht, daarbij is getracht zoveel mogelijk een 'natuurlijke' groepering op basis van inhoud te maken. Als een standaardindeling zou worden gehanteerd, zouden de verschillen met COBIT wellicht minder duidelijk zichtbaar worden. De volgende indeling is gebruikt:

- beleid en controle;
- management;
- personeelsselectie;
- beheersing van risicogedrag.

De tabellen bevatten achtereenvolgens:

- volgnummer;
- geformuleerde norm;
- referentie naar geraadpleegde literatuur;
- nummer van een (enigszins tot sterk) overeenstemmend 'control objective' in COBIT;
- pijltje (↑) dat aangeeft dat deze norm een plaats in COBIT zou kunnen verdienen. De betekenis van deze kolom kan op dit leesmoment worden genegeerd. In 7.3 komt het alsnog aan de orde, het zal daar worden uitgelegd.

Voor de volledigheid zij opgemerkt dat de gepresenteerde normen een eerste aanzet zijn die verdere rijping behoeven als ze bruikbaar worden geacht door derden. Ze zijn dan ook *niet* bedoeld zijn om

kritiekloos in de praktijk te gebruiken. Integendeel: ze moeten *zeer kritisch* beschouwd worden omdat enkele normen mogelijk de grenzen van het aanvaardbare raken of zelfs overschrijden. De uit de normen voortvloeiende maatregelen komen *niet* in de plaats van beheersingsmaatregelen waarvan de effectiviteit is aangetoond of kennelijk voldoende aannemelijk is, ze kunnen daar wel een *aanvulling* op vormen.

7.2.1 Normen: beleid en controle.

	norm in referaat	verwijst naar	# in cobit	norm in cobit	↑
1	De organisatie heeft expliciete en eenduidige gedragsregels. Eventuele 'grey areas' op het gebied van gedragsregels zijn of worden in kaart gebracht en worden tot duidelijkheid gebracht.	[GUDA] [NEYS]	PO 6.1	COBIT heeft een zeer genuanceerde norm voor gedragsregels en een awareness program om de bekendheid ervan te bevorderen. COBIT spreekt zich niet uit over grey areas.	
2	De organisatie communiceert en publiceert deze gedragsregels.	[NEYS]	PO 6.11 DS 7.3	Het securitybeleid wordt gecommuniceerd (PO 6.11) en (ethische) gedragsregels zijn onderdeel van opleiding/training (DS 7.3), publicatie wordt niet genoemd.	
3	Non-conformiteit aan de gedragsregels heeft sancties tot gevolg. Deze sancties worden als uitgangspunt altijd uitgevoerd.	Spee	PO 6.6	Compliance wordt genoemd. De wijze waarop met sancties wordt omgegaan wordt vrij gelaten.	↑
4	Uitvoering van een sanctie wordt, met inachtneming van de anonimiteit van personen, gepubliceerd.	Spee	-		
5	Kleine overtredingen van regelgeving worden als uitgangspunt gesanctioneerd om te voorkomen dat er grey areas in de regelgeving en/of de handhaving ervan ontstaan.	Spee	-		↑
6	Om de bewustwording van de regelgeving te bevorderen, tekenen alle medewerkers voor inachtneming van de gedragsregels.	[KRIM]	-		↑
7	De bedrijfscultuur, en het beloningsbeleid in het bijzonder, is niet zo dat het individuele belang strijdig kan worden met het organisatiebelang en dat risicovol gedrag wordt gestimuleerd.	[DHIL] [GRAB]	-		
8	Een jaarlijkse en zo nodig tussentijdse risicoanalyse bevat een onderdeel waarin de medewerkers uit het medewerkersbestand op eventuele gedragsrisico's worden geanalyseerd. (Daarbij wordt onderscheid gemaakt naar typische risico's die behoren bij: IT-managers, systeemontwikkelaars (analisten, ontwerpers, programmeurs, database-	[WOOD]	-	De enige overeenstemming die in COBIT is gevonden is PO 9.3, daarin wordt de term 'human resources risk' genoemd als een van de risico's waarop gelet moet worden, maar de term wordt niet nader gespecificeerd.	↑

	specialisten, testspecialisten, etc.), IT-managers, systeembeheerders, netwerkbeheerders en andere niet genoemde IT-specialisten in de systeemontwikkel-, verwerkings- en transportorganisatie.				
9	De organisatie maakt gebruik van c.q. kan in gevallen van twijfel gebruik maken van, een onafhankelijke instantie (intern of extern) die normen, regels, werkwijzen, aanwijzing van uitvoerders etc. toetst aan wet- en regelgeving, beroepsregels, algemeen aanvaarde maatschappelijke opvattingen en algemeen geaccepteerd fatsoen. Deze instantie (noem het ethiekcommissie) wordt geaccepteerd door alle belangenvertegenwoordigers binnen de organisatie.	Spee	-	In PO 8.1 en 8.1 is voorzien dat de organisatie voeling houdt en afstemming zoekt met externe wet- en regelgeving. De norm in het referaat wordt breder bedoeld: ook interne regelgeving en zaken als gedragscode en ethische code worden bedoeld, het toetsen op draagvlak is daarbij van belang en vindt veelal geen basis in formele teksten.	
10	Het personeelsbeleid laat niet toe dat werknemers bijzondere, niet formeel geregelde, privileges of uitzonderingsposities genieten.	Spee	-		
11	De organisatie laat het IT-personeel regelmatig een training en/of opleiding volgen in het kader van security awareness, waarbij de bewustwording en signalering van risicoverhogende factoren in de sociale omgeving worden behandeld.	[GELL] [DOD] [JONE]	DS 7.3	Hoewel het onderwerp 'leren signaleren in de omgeving' niet specifiek wordt genoemd, mag het als geïncorporeerd worden verondersteld in de genoemde training/opleiding.	
12	De controle op beveiligingsprocedures wordt op niet-voorspelbare tijdstippen uitgevoerd.	Spee	-		↑
13	Controles en audits die naar opzet én bestaan van beheersmaatregelen toetsen, vinden onverwachts en onaangekondigd plaats.	[DOD] [WOOD]	-	In M 4.5 is juist het plannen van regelmatige audits onderdeel van de normstelling. Hoewel 'regelmatig' niet hetzelfde is als 'voorspelbaar', ontbreekt de gedachte van niet aangekondigde audits.	↑
14	De assessment of evaluatie van kenmerken van mensen wordt gedaan door gekwalificeerde personen of wordt kwalitatief en procedureel gedaan volgens een methode die is goedgekeurd door een gekwalificeerd persoon. Het risicoaspect is een onderdeel van de assessment of evaluatie.	[GUDA] [BOUR]	-		↑
15	De organisatie heeft zoveel mogelijk gedaan om een beeld te hebben van de intenties van de medewerkers en waakt ervoor dat (zeer) deskundige medewerkers met een verhoogde kans op 'verkeerde' motieven in de positie verkeren dat ze zonder grote moeite	Spee	-		

	schade kunnen toebrengen. In mindere sterke mate geldt een risico voor laag-deskundige medewerker met verhoogde kans op 'verkeerde' motie-ven, deze moet binnen de beperkte mogelijkheden die hij heeft, goed worden gemonitord.				
16	De *gepercipieerde* pakkans voor kwaadwillend IT-gedrag binnen een organisatie moet worden gemaximali-seerd. Dat kan bijvoorbeeld worden gedaan door het bestaan van intern controlewerk duidelijk en regelmatig te communiceren en de bijbehorende sancties en de feitelijke uitvoering ervan, maar de kwaliteit en intensiteit van het controlewerk, alsmede de frequentie waarmee het plaats vindt, geheim te houden.	Spee	-		↑

7.2.2 Normen: management

	norm in referaat	verwijst naar	# in cobit	norm in cobit	↑
17	Een managementstijl wordt bevorderd waarin tijd en aandacht is voor gesprek-ken met individuele werknemers over hun persoonlijke problemen, ook als ze niet aan de organisatie verwijtbaar zijn en verweten worden in geval die problemen de organisatie negatief zouden kunnen beïnvloeden.	[SHA1] [VER1]	-		
18	Managers worden geselecteerd of opge-leid in lijn met een managementstijl die gekenmerkt wordt door aandacht voor individuen en hun achtergronden en omstandigheden, voor zover deze de organisatie negatief zouden kunnen beïnvloeden.	[SHA1] [VER1]	-		
19	Counseling, zelf uitgevoerd of uitbe-steed, is een van de management tools.	Spee	-		
20	Bij het constateren van persoonlijke problemen van een medewerker kan en zal er voor professionele hulp worden gezorgd.	[GELL]	-		
21	Leidinggevenden moeten worden getraind in het opmerken van signalen die gerelateerd kunnen worden aan riskant gedrag.	[GELL]	-		↑
22	De mate van baanzekerheid of de even-tuele kans op ontslag wordt bij aanname altijd expliciet door de manager gecom-municeerd. Ontslag wordt gecommuni-	[GAUD] [SHA2] [KRIM]	-	PO 7.8. besteedt aandacht aan ontslag, maar focust op tijdige acties om ervoor te zorgen dat interne controle- en securitymaatregelen	↑

	ceerd op een respectvolle en anderszins acceptabele wijze. Maximale inspanning wordt gedaan om de redelijkheid of de onvermijdelijkheid van het ontslag aanvaard te krijgen.			niet kunnen worden omzeild. Het risico van het ontstaan van sterke wraakzuchtige motieven die de organisatie of de reputatie ervan zullen kunnen schaden, komt niet aan de orde.	

7.2.3 Normen: personeelsselectie

	norm in referaat	verwijst naar	# in cobit	norm in cobit	↑
23	Personeel wordt bij selectie gescreend op een verleden van computermis-bruik, hacking, algemeen crimineel gedrag, vandalisme en (bedrijfs)spionage op manieren die binnen de wet zijn toegestaan, zoals interviewen, contact met referenties (zo nodig inclusief persoonlijk bezoek), raadplegen van daartoe inge-richte bestanden. Als er enige grond is voor verdenking van terrorisme, moeten de daartoe aangewezen instanties worden geraadpleegd.	[BOUM] [KRIM]	-	PO 7.4. pleit voor screening afhan-kelijk van de gevoeligheid van de positie bij aanname, overplaatsing en promotie. Er wordt niet vermeld waarop gelet moet worden.	↑
24	Tijdelijke krachten worden behandeld als bij 23 als hun functie dat vereist.	[BOUM]	-		↑
25	De organisatie stelt tevoren expliciet en schriftelijk vast welke kenmerken of combinaties van kenmerken van kandidaten voor functies niet gewenst zijn uit beveigingsoogpunt, vergezeld van een uitleg. Normen van wet- en regelgeving en goed fatsoen worden daarbij in acht genomen. De gebruikte kenmerken sluiten aan bij de constructen uit de gebruikte geva-lideerde psychologische tests.	Spee	-		
26	De 'cultural fit' in de organisatiecul-tuur van kandidaatmedewerkers wordt bepaald m.b.v. gevalideerde psychologische tests. Te behalen norm in deze is expliciet vastgesteld.	[SHA3]	-		↑
27	De organisatie moet erop toezien dat managers niet meer ex-collega's rekruteren dan op grond van versprei-ding van geschikte kandidaten in het wervingsgebied redelijk geacht mag worden.	[COH3] [JONE]	-		↑

7.2.4 Normen: beheersing van risicogedrag

	norm in referaat	Verwijst naar	# in cobit	Cobit	↑
28	Tekenen van frustratie of teleurstelling van medewerkers, die door de organisatie worden veroorzaakt of eraan worden toegeschreven, worden serieus genomen en besproken en er wordt zo veel mogelijk aan gedaan om te voorkomen dat de verwijtbare frustraties respectievelijk de attributie van verwijten blijven bestaan.	[SHA1]	-		↑
29	De IT-gerelateerde activiteiten van medewerkers van wie bekend is dat ze een geschiedenis hebben van problemen met autoriteiten, worden regelmatig extra gemonitord teneinde overtredingen van de regelgeving tijdig te kunnen signaleren.	[SHA1]	-		↑
30	De IT-gerelateerde activiteiten van medewerkers bij wie een verminderde loyaliteit aan de organisatie wordt waargenomen, eventueel in combinatie met een opvallend streven naar maximalisatie van de eigen voordelen, dan wel bij wie dit redelijkerwijs kan worden verwacht door bijvoorbeeld ongewild(e) demotie of ontslag, worden regelmatig extra gemonitord teneinde overtredingen van de regelgeving tijdig te kunnen signaleren.	[SHA1] [AND1]	-		↑
31	De IT-gerelateerde activiteiten van medewerkers die in de positie verkeren dat ze kunnen spioneren voor concurrerende organisaties, worden regelmatig extra gemonitord teneinde overtredingen van de regelgeving tijdig te kunnen signaleren.	[AND1]	-		
32	De IT-gerelateerde activiteiten van introverte medewerkers die een evidente geschiedenis van persoonlijke frustraties hebben, worden regelmatig extra gemonitord teneinde overtredingen van de regelgeving tijdig te kunnen signaleren.	[SHA1]	-		↑
33	De IT-gerelateerde activiteiten van introverte medewerkers die last hebben van computerverslaving, worden regelmatig extra gemonitord teneinde overtredingen van de regelgeving tijdig te kunnen signaleren.	[SHA1] [TAMU]	-		↑
34	De IT-gerelateerde activiteiten van introverte medewerkers van wie bekend is dat ze andere en meer flexibele regels	[SHA1]	-		↑

	hanteren voor wat als aanvaardbaar en onaanvaardbaar gedrag wordt beschouwd dan de hen omringende gemeenschap, worden regelmatig extra gemonitord teneinde overtredingen van de regelgeving tijdig te kunnen signaleren.				
35	De IT-gerelateerde activiteiten van medewerkers bij wie niet (meer) wordt voldaan aan de claim op het recht op een bijzondere positie, bijzonder voorrechten of een uitzonderingspositie, worden regelmatig extra gemonitord teneinde overtredingen van de regelgeving tijdig te kunnen signaleren.	[SHA1]	-		↑
36	De IT-gerelateerde activiteiten van medewerkers die in financiële nood verkeren, dan wel een gedragspatroon hebben dat hiertoe leidt (drugs-, drank- of gokverslaving, overdreven hang naar luxe), worden regelmatig extra gemonitord teneinde overtredingen van de regelgeving tijdig te kunnen signaleren [LUX].	[TAMU] [GELL]	-		
37	De IT-gerelateerde activiteiten van medewerkers die een van de volgende kenmerken of een combinatie ervan vertonen: constante boosheid, neiging anderen de schuld te geven van hun problemen, neiging tot dehumanisering of objectivering van anderen door haatdragende of grove opmerkingen, worden regelmatig extra gemonitord teneinde overtredingen van de regelgeving tijdig te kunnen signaleren.	[SHA1]	-		↑
38	De IT-gerelateerde activiteiten van medewerkers die vaak ongebruikelijk lang doorwerken, nooit vakanties of vrije dagen opnemen of vaak werken op tijden dat ze alleen zijn zonder dat het werk dit duidelijk lijkt te vereisen, worden regelmatig extra gemonitord teneinde overtredingen van de regelgeving tijdig te kunnen signaleren.	[GRAB] [HIND]	-		

7.3 Normen uit dit referaat met COBIT vergeleken

7.3.1 Werkwijze

De vraag is welke normen die uit dit referaat voortkomen niet in COBIT *zouden mogen* ontbreken. Daartoe moet eerst worden overwogen wanneer zulks het geval is en een norm in de tabel wordt voorzien van een ↑-teken. Er worden twee eisen gesteld:

- brede toepasbaarheid in organisaties, landen en culturen;
- de norm is gebaseerd op onderzoeksresultaten of inzichten met een aanvaardbare kwaliteit. Aanvaardbaar is hier een subjectief criterium, maar dat wordt voldoende geacht om een goede indruk te krijgen van de eventuele tekortkomingen in een standaardnormenkader.

De norm met ↑ moet leiden tot een activiteit/maatregel die in iedere organisatie van toepassing is en ook in alle delen van de wereld zinvol en acceptabel is. Zo is een norm als "De bedrijfscultuur, en het beloningsbeleid in het bijzonder, is niet zo dat het individuele belang strijdig kan worden met het organisatiebelang en dat risicovol gedrag wordt gestimuleerd" (norm 7) denkelijk geschikt voor veel westerse organisaties, maar niet voor bijvoorbeeld Japanse, waar het spanningsveld tussen individueel en collectief belang anders van aard is, er staat dan ook geen ↑ achter. Een norm als "De beveiligingsprocedures worden ook op niet-voorspelbare tijdstippen uitgevoerd" (norm 12) is universeler bruikbaar, er staat wel een ↑ achter. Hoewel bij deze inschatting ongetwijfeld wel iets over het hoofd wordt gezien, is dat voor het doel dat hier wordt nagestreefd niet onoverkomelijk: het gaat er immers om een algehele indruk te verkrijgen van het tekort schieten van COBIT op het gedragsmatige aspect.

Voorts wordt de eis gesteld dat alleen normen met een zekere onderzoekskundige onderbouwing worden voorzien van een ↑ . Bijvoorbeeld " De IT-gerelateerde activiteiten van medewerkers die vaak ongebruikelijk lang doorwerken, nooit vakanties of vrije dagen opnemen of vaak werken op tijden dat ze alleen zijn zonder dat het werk dit duidelijk lijkt te vereisen, worden regelmatig extra gemonitord teneinde overtredingen van de regelgeving tijdig te kunnen signaleren." (norm 38) komt niet voort uit onderzoek, maar uit het deskundig inzicht van een auteur en voldoet daarmee niet aan de eis.

Het totaalbeeld van de pijltjes geeft grond voor een overallevaluatie van COBIT: ontbreekt er misschien iets in COBIT? En stemt dat overeen met het in een bepaalde mate ontbreken van het gedragsaspect in standaardnormenkaders, zoals is gesuggereerd door Nuijten en v.d. Pijl [NUIJ]?

7.3.2 Resultaat van de vergelijking met normen uit COBIT

De normen uit dit referaat, die sterk gericht zijn op *het gedragsaspect* overlappen in zeer geringe mate met COBIT, zo blijkt uit een blik op een groot aantal pijltjes in de laatste kolom. De vraag van Nuijten en v.d. Pijl kan, althans binnen de beperking van dit referaat, bevestigend worden beantwoord: de invulling van het gedragsmatige aspect vertoont hiaten in COBIT. Daarmee is *waarschijnlijk* ook iets gezegd met betrekking tot hun vermoeden dat een normenkader inclusief gedragsaspecten een beter middel is om de kwaliteit van de beheersing van de informatievoorziening te evalueren. Met nadruk wordt het woord waarschijnlijk gebruikt, omdat beproeving in de praktijk en verder onderzoek meer materiaal moeten aandragen om de hier gemaakte indruk te bevestigen en zo mogelijk te versterken.

7.4 Meetbaarheid van normen

Het is gebruikelijk dat normen zoveel mogelijk in meetbare of in ieder geval eenduidig registreerbare vorm worden geformuleerd. Er is in dit referaat geen extra moeite gedaan om de normen zoveel

mogelijk in meetbare termen te formuleren. Goed beschouwd zou het meetbaar maken van normen een onderwerp voor een geheel apart referaat kunnen vormen. Overigens is een deel van de normen wel degelijk meetbaar, het is bijvoorbeeld goed vast te stellen of een manager geschoold is in counseling. Het wordt wel moeilijker om vast te stellen of het personeelsbeleid ruimte laat voor uitzonderingsposities voor individuele medewerkers, erg moeilijk wordt het om bijvoorbeeld vast te stellen bij welke werknemers er iets aan de loyaliteit jegens de organisatie schort. Alle normen overziende, valt het toch heel erg mee met de in de inleiding uitgesproken vrees dat dit literatuuronderzoek onvermijdelijk zal leiden tot normen die geen harde evidence kunnen opleveren. Een aanzienlijk deel is gewoon bruikbaar voor de auditor, zonder dat hij psycholoog hoeft te zijn.

8. Conclusie

Hoewel duidelijke en eenvoudige oorzaak-gevolg-relaties voor het ontstaan en de manifestatie van een insider threat niet zijn gevonden (er is geen silver bullet) is er wel degelijk een aantal factoren aanwijsbaar die positief verband houden met die threat. Met name de onderzoekers Shaw, Post & Ruby [SHA1, SHA2, SHA3] hebben veel interessante grondstoffen aangedragen op het vlak van risicoverhogende persoonskenmerken. Vanuit diverse hoeken komt verder de 'disgruntled employee' naar voren als serieuze threat die bovendien met gerichte managementactiviteit te beïnvloeden kan zijn. Keren we terug naar de vraagstelling van dit referaat die als volgt luidt:

Kan een organisatie opzettelijk schadelijk handelen van IT-personeel voorkomen en voorspellen door gebruik te maken van kennis van dit gedrag en de totstandkoming ervan?

8.1 Voorkomen van opzettelijk schadelijk handelen door IT-personeel

Een organisatie *kan in enige mate* opzettelijk schadelijk handelen van IT-personeel *voorkomen* door gebruik te maken van kennis van dit gedrag en de totstandkoming ervan. In dit referaat zijn diverse factoren genoemd die verband houden met opzettelijk schadelijk handelen van IT-personeel, daaruit zijn preventieve maatregelen te destilleren. De belangrijkste zijn:

- Duidelijkheid van regelgeving, communicatie erover, bewustwording van de regels bevorderen, grey areas in de regelgeving verminderen of vermijden en consequent sanctioneren volgens de regels.
- De bedrijfscultuur zo vormen dat regelovertredend gedrag geen vanuit de organisatie zelf komende en bedoelde materiële en/of immateriële beloningen oplevert.
- Personeel niet alleen als een asset, maar ook als een risicofactor beschouwen die regelmatig geanalyseerd moet worden.
- Vermijden dat er ' disgruntled employees' ontstaan door een diversiteit aan managementactiviteiten te ondernemen, zoals tijdig signaleren dat er iets mis gaat met een werknemer, anderen laten en leren signaleren, counselen, het personeel fair behandelen (individueel en onderling), ontslag op de juiste wijze verlenen, etc.
- Audits (en controles) vaker onverwacht plaats laten vinden.
- Screening verbeteren en uitbreiden met background checks op diverse risicoverhogende antecedenten.
- Letten op de aanwezigheid of ontwikkeling van kenmerken bij medewerkers die risicoverhogend zijn (zie normen 28 t/m 38) en tijdig interveniëren.

Het verband tussen genoemde factoren en het feitelijke handelen is vaak indirect, daarom heeft het beïnvloeden van factoren niet altijd direct een effect en evenmin een direct effect, maar eerder een indirect effect dat vaak pas op langere termijn uitwerking heeft.

Twee aspecten moeten goed in de gaten worden gehouden bij gebruik van hier genoemde normen of maatregelen. Ten eerste is dat voorzichtigheid, de hier vermelde inzichten zijn altijd van betwijfelbaar nut in concrete specifieke gevallen. Bovendien moet rekening worden gehouden met de nog geringe aangetoonde validiteit van de inzichten: er is nog niet veel vaste grond onder de voeten. Ten tweede moet het economisch aspect in de gaten worden gehouden: de maatregelen moeten in verhouding staan tot het ingeschatte risico. Hoewel veel maatregelen (of normen) die hier de revue zijn gepasseerd ook andere gunstige neveneffecten kunnen hebben (persoonlijke aandacht van een manager heeft bijvoorbeeld vaak een productiviteitsverhogend effect) die bijdragen aan de gebruikswaarde, moeten ze natuurlijk niet kritiekloos ingevoerd worden. Daarbij moet bedacht worden dat de kans op de manifestatie van een ‘insider threat’ met grote schade niet erg groot is. Laten we nuchter blijven: er zijn niet zoveel ‘malicious insiders’. In een bedrijf met 20 werknemers kan er een werken, maar het zou niet

economisch zijn om ervan uit te gaan en de volle waaier van mogelijk effectieve maatregelen te treffen. Bij een bank met 50.000 werknemers kun je er daarentegen bijna zeker van zijn dat er enkele medewerkers in dienst in dienst zijn met kwade bedoelingen. Afhankelijk van de omgeving waarin de persoon werkt en de bijgaande risico's kunnen maatregelen zoals in deze tekst genoemd worden getroffen.

Kijkend naar de classificaties uit hoofdstuk 5, blijken in dit kader de functionele indelingen van mensen niet te passen op de tot nu toe verworven inzichten. Een meer psychologische indeling past beter. De indeling van Albert & Dorofee laat bijvoorbeeld zien dat de beheersing van de 'disgruntled employee' tot op zekere hoogte binnen het vermogen ligt van een organisatie. Dat geldt in veel mindere mate voor de andere 5 soorten: attackers, terrorists, vandals, criminals en spies. Met name voor terroristen, criminelen en spionnen geldt dat in belangrijke mate gesteund moet worden repressieve maatregelen, hoewel goede signalering, risicoanalyse met inbegrip van de mens als risicofactor en studie van de motieven van daders ook hier kunnen helpen.

8.2 Voorspellen van opzettelijk schadelijk handelen door IT-personeel

Een organisatie kan *in geringe mate* opzettelijk schadelijk handelen *voorspellen*. Het best haalbare is gericht waakzaam te zijn door kennis van de diverse indicatoren. Ethiek en effectiviteit strijden hier echter om voorrang. Het is ethisch niet aanvaardbaar als uit de noties over persoonskenmerken en -omstandigheden vooroordelen worden afgeleid die worden geprojecteerd op medewerkers die 'binnen het plaatje' passen. Immers, *alle* inzichten die tot nu toe zijn gepresenteerd hebben niet die aangetoonde validiteit die is vereist om mogelijke 'collateral damage' zoals bijvoorbeeld onterechte verdenking van personen te rechtvaardigen. Het is verder zaak geen grote illusies te hebben over een verbeterde voorspelbaarheid in de toekomst. Menselijk gedrag is niet erg voorspelbaar omdat individuen te verschillend zijn en er al met al weinig begrepen wordt van de complexiteit van het ontstaan van individueel gedrag. Toch is het aanvaardbaar dat organisaties waar de insider threat tot grote risico's kan leiden, maatregelen treffen op grond van hier naar voren gebrachte inzichten, als dat met voorzichtigheid en deskundigheid gebeurt. Het gebeurt al lang: gedrag voorspellen is in wezen wat al decennia wordt gedaan bij personeelselectie en gebruik van screening-gegevens. Het is niet onethisch om een kandidaat minder snel aan te nemen als hij een paar minpuntjes scoort op risicoindicaties zoals bijvoorbeeld genoemd in een van de normen 28 t/m 38. Sterker nog: het is ethischer om dat te doen op grond van *enig* onderzoek, dan op grond van wat tegenwoordig wel het buikgevoel wordt genoemd of nog erger, het onderbuikgevoel. Een matig onderbouwde aanpak is meestal beter dan een toevallige of gevoelsmatige en dus willekeurige aanpak. Zo bezien levert dit literatuuronderzoek wel degelijk iets bruikbaars op.

8.3 Epiloog

Al met al blijft het toch dun ijs waar we over lopen. Dat kan ook niet anders als we ons realiseren dat onderzoek naar gedragsmatige aspecten van informatiebeveiliging nog maar net gestart is. Als we daarbij in ogenschouw nemen dat de wetenschappelijke psychologie pas na decennia onderzoek over de gehele wereld enige bruikbare vruchten begon af te werpen, dan weten we dat we geduldig moeten zijn. Intussen is het zaak te gebruiken wat er reeds is, want er zijn overal bepaalde gaten in de informatiebeveiliging die alleen beetje bij beetje kunnen worden gedicht met kennis over mensen en hun drijfveren binnen de organisatiecontext waar ze werken. Er is geen keuze dan gebruik te maken van de kleine beetjes inzicht die tot nu toe op de weerbarstige realiteit veroverd zijn.

Intussen moet de auditpraktijk zich afvragen op welke wijze ze zich op een verantwoorde wijze meer zal gaan inlaten met de zachte factoren die hier ook aan de orde zijn geweest. De manier waarop dat moet worden gedaan is: kennis nemen van het menselijk gedrag als risicofactor en zinvolle normen hanteren. Dat is makkelijker gezegd dan gedaan: het *toepassen* van normen met een psychodiagnosti-

sche component (28 t/m 38) behoort meestal niet tot zijn competentie. De auditor is geen psycholoog, maar gedrag en menselijke kenmerken kunnen wel degelijk object van onderzoek zijn. Ze moeten dat zelfs zijn, of de auditor het nou leuk vindt of niet. Het is een interessante vraag of de opleidingen tot EDP auditor meer zouden kunnen of moeten faciliteren in het verwerven van inzicht in gedragsaspecten c.q. in het beoordelen van management op dergelijk inzicht.

Geraadpleegde literatuur

[ALBE] Albert, C. & Dorofee, A.. Octave Threat profiles. Software Engineering Institute. Carnegie Mellon University.

[AND1] Anderson, R.H., Bozek, T., Longstaff, T., Meitzler, W., Skroch, M., van Wyk, K., 2000. Conference proceedings. Research on mitigating the insider threat to information systems - #2. National Defense Research Institute, 2000.

[AND2] Anderson, R.H., 1999. Research and Development Initiatives Focused on Preventing, Detecting, and Responding to Insider Misuse of Critical Defense Information Systems. National Security Research Division, 1999.

[APA] American Psychiatric Association. Diagnostic and Statistical Manual of Mental Disorders. Washington, D.C.: American Psychiatric Association.

[BOUM] Bouma, H. Wat voor vlees zit er in de kuip? Financieel Dagblad, 20 maart 2003.

[BOUR] Bourassa, J. SAS No. 94 - The human risk factor. http://accountingmalpractice.com/0005/articles/ga-200206h.pdf

[BURG] Burghoorn, A., Persson, M. Cyberaanslag verwoestender dan een bom. De Volkskrant, 2 juli 2003.

[COH1] Cohen, B., 2000. The human equation. Hacked off … experts call hacker motivations key to prevention. Infosec Outlook, Vol. 1, Issue 2, 2000.

[COH2] Cohen, F., 2003. The All.Net Security Database. http://all.net/CID/Threat/Threat1.html.

[COH3] Cohen, F., 2001. The new cyber gang - a real threat profile. http://all.net/journal/netsec/2001-05.html

[DHIL] Dhillon, G., 2001. Violation of safeguards by trusted personnel and understanding related information security concerns. Computers & Security, Vol. 20, p. 165-172, 2001.

[DOD] Department of Defence, 2000. DoD Insider Threat Mitigation. Final report of the insider threat integrated process team. April, 2001.

[DOUG] Douglas, J. & Olshaker, M., 1995. Mindhunter. New York: Scribner.

[EVER] Evers, A. 1986. Interessen gemeten en gewogen. Validering van de Amsterdamse Beroepen Interessen Vragenlijst. Lisse, Swets & Zeitlinger B.V.

[GAUD] Gaudin, S., 2002. Corporate Layoffs Create Security Havoc for IT Pros. Datamation, July 2, 2002. http//itmanagement.earthweb.com/secu/article.php/1380141

[GELL] Gelles, M. Exploring the mind of the spy. http//rfweb.tamu.edu/security/secguide/treason/mind.htm. Zie ook: Ames: too many weaknesses. http//rf-web.tamu.edu/security/secguide/spystory/ames.html en Pollard: grandiose imagination. http//rf-web.tamu.edu/security/secguide/spystory/pollard.htm

[GRAB] Grabosky, P. & Duffield, G., 2001. Red flags of fraud. Australian Institute of Criminolgy, Trends & Issues. Queensland Government. March 2001.

[GUDA] Gudaitis, T.M., 1998. The missing link in information security: three dimensional profiling. CyberPsychology & Behavior, Volume 1, Number 4, 1998. Mary Ann Liebert, Inc.

[HIND] Hinde, S., It was déjà vu all over again. Elsevier Science Ltd., 2002.

[HUND] Hundley, R.O. & Anderson, R.H., 1996. Emerging challenge: security and safety in cyber-space. IEEE Technology and Society Magazine, pp. 19-28, 1996.

[ISAC] ISACA IT Governance Institute, 2000. COBIT, 3rd edition..

[JONE] Jones, A.K., Quarles, L.R., 2000. Cyber security and the insider threat to classified information. Computer science and telecommunications board. November, 2000.

[KPMG] KPMG, 2003. Monitor Internetbeveiliging 2003. Veiligheid en betrouwbaarheid. Een kwantitatieve verkenning. In opdracht van het Ministerie van Economische Zaken. Ministerie van Economische Zaken, 2003.

[KRIM] Krimkowitz, H., 2000. Mitigating risks to the insider threat within your organisation. Sans Infosec Reading Room, October 2000.

[KRUY] Kruyskamp, C., 1982. Van Dale, Groot Woordenboek der Nederlandse taal. 's Gravenhage, Martinus Nijhoff, 1982.

[LUX] Lux, A.G., Fitiani, S., 2002. Fighting internal crime before it happens. Information Systems Control Journal, Vol. 3, 2002.

[MILL] Miller, H.N., 2000. The Love Bug Virus: Protecting Lovesick Computers from Malicious Attack" Government Affairs, ITAA, Arlington, 2000.

[MISH] Mishel, W., 1976. Introduction to personality. New York, Holt, Rhinehart and Winston.

[MOON] Moonen, H.B., 1991. Kwaliteitsbeheersing van de Informatievoorziening; Algemeen. Handboek EDP Auditing. Deventer, Kluwer.

[NEYS] Neys, C., 2003. IT'ers, regels en security awareness. Afstudeerthesis in het kader van de Masteropleiding Security in Information Technology aan de TUE, 2003.

[NUIJ] Nuijten, A. & v.d. Pijl, G., 2000. Niet altijd volgens het boekje - Standaardmodellen schieten soms tekort. De EDP Auditor, nummer 3, 2000.

[NUTT] Nuttin, J., Beuten, B., 1963. Minnesota Multiphasic Personality Inventory (MMPI). Lisse, Swets & Zeitlinger.

[PARK] Parker, D.B., 1998. Fighting computer crime: A new framework for protecting information. New York, John Wiley and Sons.

[POWE] Power, R., 2002. 2002 CSI/FBI Computer Crime and Security Survey. Computer Security Issues & Trends, VOL VIII, no. 1, 2002.

[RAVE] Ravestijn, W. v., 2003. Roeien met de riemen die er niet zijn. Computable, 04.07.03.

[ROEB] Roebuck, T.A. The insider threat. http://abyss.asask.ca/~roebuck/threats.html.

[SCHU] Schultz, E.E., 2002. A framework for understanding and predicting insider attacks. Paper to be presented at Compsec 2000, London, 30 October 2002. Elsevier Science Ltd.

[SCHU] Schultz, E.E. & Shumway, R. Incident response: a strategic guide for system and network security breaches. Indianapolis, New Riders.

[SHA1] Shaw E.D., Ruby K.G., Post J.M., 1998. The insider threat to information systems. Security Awareness Bulletin 2-98. Department of Defense Security Institute.

[SHA2] Shaw E.D., Post J.M., Ruby K.G. Inside the mind of the insider. Security Management Online: www.securitymanagement.com/library/000762.html.

[SHA3] Shaw, E.D., 2000. Sample PSA evaluation approaches. Information Security Magazine, July, 2000.

[STAN] Stanton, J.M., Caldera, C., Isaac, A., Stam, K.R., Marcinkowski, S.J., 2003. Behavioral Information Security: Defining the Criterion Space. Symposium presentation at the 20003 meeting of the Society for Industrial and Organisational Psychology, Orlando, Florida.

[SULE] Suler, J., 1998. The bad boys of cyberspace: deviant behavior in on-line multimedia communities and strategies for managing it. On-line document, www.rider.edu.users.suler.psycyber.

[TAMU] N.N. Security and Suitablity issues.
http://rf-web.tamu.edu/security/secguide/s5improp/security.htm.

[THOM] Thomsen, D., 2002. Centrally managed Network Security: hope or reality? SC Infosec Opinionwire. http://www.infosecnews.com/opinion/2002/11/20_02.htm

[TUGL] Tuglular, T., 2000. A preliminary structural approach to insider computer misuse incidents. Ege University, Turkey, 2000.

[VER1] Verton, D., 2002. Insider threat may be harder to detect, experts say. Computerworld, April 2002.

[VER2] Verton, D., 2002. Terrorism 101 with Eric Shaw. Computerworld, April 2002.

[WILD] Wilde, G.J.S., 1963 Amsterdamse biografische vragenlijst (ABV). Amsterdam, van Rossen.

[WOOD] Wood, B.J., 2000. An insider threat model for adversary simulation. SRI International. Cyber Defense Research Center, System Design laboratory, Albequerque, New Mexico, USA.

***