DIE BEVEILIGING VAN INLIGTING EN TOERUSTING

Referaat gelewer op onlangse simposium „Bestuur en die Rekenoutomaat".

C. J. J. Coetzee
Hoof, Materiaal- en Voorraadbeheer, KRYGKOR.

1. INLEIDING

As daar, veral in ons land, in enige organisasie net gepraat word van beveiliging of sekuriteit, is daar gewoonlik onmiddellik 'n gevoel van antipatie en selfs antagonisme te bespeur. Dit is waarskynlik te wyte aan die feit dat ons in Suid-Afrika nog nie veel te doen gehad het met elemente soos kwaadwillige sabotasie en industriële spioenasie nie.

By bestudering van hierdie onderwerp blyk dit 'n uiters kontensieuse en tegelykertyd 'n onrusbarende faset van die rekenaarwese te wees, veral sover dit bestuur aangaan. Om die omvang en trefkrag te illustreer: In 'n artikel "The Technology of Computer Destruction" wat onlangs in 'n ondergrondse publikasie "Broadside/Free Press" verskyn het, word volledige inligting gegee oor hoe om ponskaarte nutteloos te maak, hoe om 'n magnetiese band te beskadig, hoe om 'n rekenaar se geheue te vernietig, en hoe en waar om drade effektief te knip. Die anonieme skrywer sluit dan ook met die gedagte dat die dinge wat 'n mens aan 'n klompie vierkante jaart tweeduimdiep drade kan doen die verbeelding gaande maak.

Hierdie illustrasie bring ons onmiddellik by die werklikheid naamlik die beveiliging en sekuriteit van rekenaarinligting en -toerusting. Almal is bewus van eerstens die massa inligting en tweedens die geldwaarde gekonsentreer in 'n rekenaarsentrum. Kan Bestuur met eerlikheid en oortuiging antwoord op die volgende vrae:

(a) Kan die organisasie voortgaan met sy normale verrigtinge as die hele rekenaarsentrum met alles daarin skielik vernietig word?

(b) Word sekuriteit en beveiliging van rekenaarlêers (bande, kaarte, skyfpakke) voorsien soos wat aan soortgelyke inligting in die dae voor die koms van die blikbrein verskaf is?

(c) Is daar voldoende beskerming en beveiliging van programme, lêers, en toerusting teen sabotasie?

2. DIE RISIKOS VERBONDE AAN INLIGTING EN TOERUSTING

2.1 Omgewingsfaktore

Enigiets wat veroorsaak dat jou rekenaar en verwante toerusting vir 'n onbepaalde tydperk nie beskikbaar is vir verwerkingsdoeleindes nie, kan katastrofies wees. Die belangrikste omgewingsrisiko is brand a.g.v. die frekwensie van voorkoms daarvan, maar daar is ook ander faktore soos oorstromings, tornados, aardbewings, ontploffings, opstande en oorlog en ernstige krag- en lugreëlingonderbrekings.

'n Voorbeeld van die skade wat vuur kan veroorsaak, is die brand wat in 1959 'n veronderstelde brandveilige rekenaarinstallasie in die Pentagon vernietig het. Die totale skade is nie-amptelik geraam op tiene van miljoene dollars.

Redelik onlangs is 'n brandveilige rekenaarsentrum op die tweede vloer van 'n gebou vernietig toe die vloer ingestort het a.g.v. 'n brand op die eerste vloer. Dit wil voorkom of Bestuur vir so 'n moontlikheid moes voorsiening gemaak het toe die sentrum beplan is.

In 1966 het 'n gaslekkasie 'n ontploffing veroorsaak wat 'n 290 000 dollar Honeywell met alle verwante toerusting totaal vernietig het. Gelukkig is 'n absolute katastrofe verhoed deur-

dat voorsiening gemaak is vir duplikaatlêers in 'n vuurvaste brandkas.

2.2 **Meganiese Probleme**

Onbeskikbaarheid a.g.v. meganiese defekte word gewoonlik spoedig bespeur en kan reggestel word voordat groot skade kan voorkom. Dit is egter die kleiner op-die-oog-af onbenullige en onopgespoorde defekte wat kritiese probleme en mislukkings kan veroorsaak. Laasgenoemde kan eers op so 'n laat stadium ontdek word dat 'n groot klomp skade intussen aangerig is.

As voorbeeld: in 'n sekere rekenaarsentrum is daar 'n foutiewe magnetiese banddryfeenheid ontdek nadat honderde spoele band foutiewelik geprosesseer is. Die fout is nie onmiddellik opgespoor nie omdat die toerusting, t.s.v. die feit dat dit besig was om data willekeurig te verwring, dit voortdurend self gekontroleer het en aangedui het dat alles korrek funksioneer.

2.3 **Operateursfoute**

Onervare en/of nalatige rekenaaroperateurs kan sonder behoorlike toesig per abuis waardevolle programme en datalêers vernietig. Hulle kan swak kontrole uitoefen oor 'n program en sodoende lêers wysig of vernietig. Hulle kan ook toerusting beskadig wat weke se herstelwerk kan beteken.

Voorbeelde hier is: In 'n groot vervaardigingsmaatskappy waar die belangrikste bate rekenaargesproke 'n volledige klantelêer was, is binne duime daarvan gekom om 2/3 van hierdie lêer te verloor a.g.v. prosedurefoute deur 'n onervare operateur. Die lêer is in drievoud gehou, 'n redelike voorsorgmaatreël, maar in twee agtereenvolgende weke is 2/3 des van twee van die lêers vernietig. Slegs per toeval, a.g.v. skedule- en skofverandering met die derde gang, het 'n ervare operateur agtergekom dat die taak baie vinniger verrig word as gewoonlik, dit ondersoek, en die fout ontdek. Indien die gang volgens skedule gedoen is, sou die inligting permanent verlore gewees het en die koste volgens raming in die miljoene.

Die Dataverwerkingsdienstebestuurder van 'n groot Lugdiens het agtergekom dat verliese aan data gely word. Hy het die antwoord gevind een aand tydens 'n besoek aan die rekenaarsentrum. Nagskofoperateurs het sake „bespoedig" deur 'n outomatiese veiligheidspatent op banddryfeenhede te omseil gedurende terugwenteling. Hulle het daarmee weggekom as hulle versigtig was, maar af en toe bande laat breek en sodoende inligting verloor.

2.4 **Programfoute**

Dit is wel waar dat die meeste programfoute slegs kleiner probleme veroorsaak, maar veral die oorskakeling van 'n groot handstelsel na die rekenaar, of oorskakeling van een stel toerusting na 'n ander (gewoonlik groter) kan chaoties verloop en met hoë koste gepaard gaan a.g.v. vertragings deur programfoute en -aanpassings.

As voorbeeld het 'n sekere maatskappy in 1968 'n koste-item van 2,8 miljoen dollar gerapporteer a.g.v. 'n fout in die oorskakeling van hul rekeningstelsel na 'n rekenaarstelsel.

In 'n ander maatskappy het 'n programmeerder wat verantwoordelik was vir die salarisprogram sy eie naam as sleutel gebruik vir die kontrolering daarvan. Sy stelsel het goed gefunksioneer totdat hy van werkgewer verander het — toe wou die salarisprogram net nie werk nie.

2.5 **Diefstal en Bedrog**

'n Tipiese rekenaarsentrum met die groot konsentrasie van duur toerusting en belangrike inligting moet uit die aard van die saak hoë prioriteit geniet by die oneerlike werknemer. Nog nooit tevore was soveel noodsaaklike lewensbelangrike data so gerieflik in 'n klein area gekonsentreer nie, en dit is verbasend dat nie meer gevalle van diefstal en bedrog aangemeld word nie.

Die volgende basiese metodes kan deur die potensiële misdadiger gevolg word:

(a) diefstal van inligting (bande, lêers, ens.);
(b) manipulasie d.m.v. die konsole;
(c) onreëlmatighede tydens program- en meesterlêerbywerking; en
(d) manipulasie van toevoerdata.

Gevalle wat voorgekom het, is: 'n Ontevrede werknemer van die Encyclopaedia Britannica het onlangs hul meesterlêer met meer as 2 miljoen klantename daarop gesteel en dit aan 'n konkurrent verkoop. Die geraamde verlies vir Britannica bedra in die omgewing van R2½ miljoen.

In 1969 het 'n diensburo-eienaar tien jaar

tronkstraf gekry vir bedrog. Oor 'n periode van 4 - 5 jaar het hy meer as 'n miljoen dollar van een van sy klantefirmas verduister. Hy is uiteindelik nie deur die betrokke klant betrap nie maar wel deur 'n suspisieuse bankbeampte.

'n Welbekende geval is dié waar 'n programmeerder in 'n bank groot bedrae geld in die hande gekry het deur eenvoudig te programmeer dat sy rekeningnommer omseil word wanneer verslag gedoen word oor bankoortrekkings. Hy kon dus sy rekening te enige tyd met enige bedrag oortrek.

By instansies waar hoogsvertroulike inligting hanteer word en waar faktore soos industriële en internasionale spioenasie ter sprake kom, bied stelsels wat van tyddeling en dataversending d.m.v. kommunikasiekanale en terminale gebruik maak, 'n Achilles-hiel in die borswering van enige sekuriteitstelsel. Infiltrasie van die inligtingstelsel vind plaas d.m.v. elektroniese en elektromagnetiese luisterapparate, die regte sleutelwoord vir toegang te kry, ens.

2.6 Sabotasie

Van al die risikos verbonde aan elektroniese dataverwerking is sabotasie seker die een wat die meeste vrees inboesem — en weer a.g.v. die groot konsentrasie van inligting en toerusting bied dit uitstekende geleenthede daartoe. Basies kan onderskeid gemaak word tussen onopsetlike en opsetlike sabotasie.

Gevalle aangeteken van onopsetlike sabotasie is:

By een maatskappy het 'n werknamer sy magnetiese flitslig aan die kant van 'n bandkabinet geplaas terwyl hy besig was met opruimingswerk. Die gevolg was dat 6 vol dae rekenaartyd, verlore gegaan het a.g.v. die data wat deur die magneet van die bande gevee is.

'n Ander rekenaardiensbeampte het vergeet dat daar 'n magneet in sy gereedskapkis is terwyl hy naby die bande gewerk het. Die gevolg was dat 80 000 van 'n kredietmaatskappy se klanterekords vernietig is. Dit kon gelukkig herskep word teen 'n koste van 10 000 dollars.

Uit bogenoemde blyk dit hoe 'n gevaarlike wapen 'n magneet in die hande van 'n moedswillige saboteur is. 'n Magneet so groot soos 'n muntstuk kan 'n biblioteek met tot 50 000 bandspoele binne minute vernietig. 'n Ontevrede werknemer in dataverwerking het dan ook onlangs magnete gebruik om feitlik elke lêer en program in besit van sy werkgewers te vernietig. Die ouditeure betwyfel dit of genoeg inligting gerekonstrueer kan word om die betrokke maatskappy in besigheid te hou.

In Amerika word veral probleme ondervind van militante studente-organisasies. In Februarie 1969 het opstandige studente van die Sir George Williams Universiteit in Montreal hul CDC 3300- rekenaar met toerusting en bande ter waarde van 1,6 miljoen dollars totaal vernietig. Dit sou hulle glo minstens 8 maande neem om normale verwerking te hervat.

In Maart 1969 het vandale 'n IBM 360/40 van die Bostonse Universiteit beskadig deur gebruik te maak van draadknippers en suur. Radikale studente het ook in die begin van 1970 by die rekenaarsentrum van Dow Chemical ingebreek en meer as 1000 bande, waarop jare se navorsing i.v.m. senuweegasse en ander geheime chemiese wapens geberg was, skoongevee.

3. WAAROM BLY HIERDIE RISIKOS VOORTBESTAAN?

Dit is eintlik moeilik begrypbaar waarom die algemene toestand van gebrekkige beheer en sekuriteit by rekenaaraanwendings, wat vandag in die meeste organisasies gevind word, wel bestaan. Die redes blyk gedeeltelik histories en gedeeltelik sielkundig te wees.

Die geskiedenis van elektroniese dataverwerking in die meeste maatskappye dui op een van voortdurende blitsprojekte. Streng beveiliging- en sekuriteitsmaatreëls sou aan die belaglike gegrens het as die grootste prestasie was om die verskeidenheid projekte en programme aan die gang te kry. Vandag is dit of behoort dit nie meer 'n verskoning te wees nie, en Bestuur sal pertinent hieraan herinner moet word.

'n Ander faktor is dat die kompleksheid van rekenaarstelsels 'n valse gevoel van sekuriteit verskaf. Mense dink blykbaar dat a.g.v. ingewikkelde apparaat, tale en programme 'n buitestaander nie in staat is tot manipulasie of wange-

bruik daarvan nie. Die argument hou nie meer steek nie aangesien vandag meer van interpreteerbare tale soos COBOL gebruik gemaak word, en veral aangesien die risikos veel groter is sover dit manipulasie uit eie geledere aanbetref.

Topbestuur het ook nog nooit werklik onder die besef gekom dat hul dataverwerking aan sulke risikos blootgestel is nie. Dit is dalk te wyte aan gebrek aan belangstelling, onkunde oor die probleem, of 'n onvermoeë om die mistiek van die rekenaar te deurdring. Met die ontwikkelende neiging in die rigting van gesofistikeerde intydse stelsels, teleprosessering en multiprogrammering, word die risikos verbonde aan ontwrigting van normale aktiwiteite natuurlik nog verder verhoog en beklemtoon.

4. WAT KAN BESTUUR HIERAAN DOEN?

In die eerste instansie moet Bestuur die mate van blootstelling aan verskeie risikos vasstel, 'n raming maak van die koste van totale en permanente onderbreking van rekenaarverwerking, en 'n raming maak van die koste van volkome beveiliging. 'n Goue middeweg moet nou gevind word. In kort moet Bestuur dieselfde basiese besigheidsbeginsels, -metodes, en -dissipline hier toepas as by enige ander vertakking in die organisasie.

Vervolgens moet Bestuur aandag gee aan:

4.1 Plasing van die rekenaar

Reeds in die beplanningstadium van die rekenaarsentrum kan gesonde oordeel aan die dag gelê word om voorsiening te maak vir beveiliging teen omgewingsrisikos soos vuur. Die sentrum behoort geïsoleer te wees, nie naby bergplekke waar ontvlambare materiaal gehou word nie, of in kelders, of naby 'n lughawe nie. Dit moet waar moontlik met vuurvaste materiaal opgerig word en voorsiening moet gemaak word vir 'n gevoelige waarskuwingstelsel en sprinkelstelsel. Vuurvaste brandkaste en/of brandkamers is noodsaaklik vir die veilige bewaring van magnetiese bande.

4.2 Gekontrollerde toegang

Gekontroleerde toegang na die rekenaarsentrum is noodsaaklik vir die beveiliging en sekuriteit van toerusting. In baie organisasies was die rekenaarkamer altyd 'n statussimbool waarheen besoekende belangstellendes en selfs lede van die publiek gewoonlik genooi is. 'n Groot versekeringsmaatskappy het onlangs lede van 'n damesklub op 'n toer deur die rekenaarsentrum laat neem. Die roterende bande en blinkende ligte het een besoeker so beïndruk dat sy gevoel het dat sy graag 'n aandenking van die geleentheid sou wou bekom. Sy het by 'n latere geleentheid gesê "I hope I didn't do anything wrong. There were all those boxes of cards on the table, and I just reached into the middle of a box and took one". Miskien het hierdie dame slegs veroorsaak dat 'n program oorgedoen moes word, miskien is daar baie lank gesoek na die oorsaak van die ontwrigting wat daarop gevolg het.

'n Verskeidenheid van maniere en metodes kan toegepas word om gekontroleerde toegang te verseker. Dit kan wissel van fisiese wagte op 'n 24 uur skofbasis, identifikasiewapens en -kaarte, kleurkodering vir sekuriteit, logboeke, ontvangsdames, tot gesofistikeerde elektroniese tegnieke soos deure wat slegs sal open as 'n spesiale toegangskaart aangebied word, dalk ook gekoppel met foto-identifikasie en magneetsensitiewe opsporingsapparaat. 'n Tegniek wat deesdae groot veld wen is gebruikmaking van geslote baantelevisie om alle besoekers d.w.s. ingange te kan dophou en identifiseer, asook sekere sekuriteitareas.

Uit al bogenoemde sal Bestuur die mees geskikte metodes moet vind met inagneming van die risikos geweeg teenoor die koste van beveiliging.

4.3 Rugsteuning (Backup)

Geen stelsel kan een honderd persent veilig gewaarborg word nie, veral nie wat apparatuurfoute of beskadiging of verlies van lêers aanbetref nie. Daar moet dus voorsien word vir 'n veiligheidsplan wat deeglik beplan en getoets is om die stelsel aan die gang te hou in geval van 'n katastrofe. Hierdie veiligheidsplan moet aan twee behoeftes voldoen. Eerstens moet dit voorsiening maak vir toegang tot duplikaat rekenaartoerusting vir noodverwerking van die stelsel, en tweedens moet voorsien word vir die beskikbaarheid van alle lêers, programmatuur en programme wat noodsaaklik is vir verwerking van die stelsel.

Die beskikbaarheid van duplikaat rekenaar-

toerusting lewer 'n definitiewe probleem aan Bestuur. Min organisasies kan dit bekostig om 'n tweede rekenaar met alle nodige toerusting elders te huisves net indien dit skielik benodig sou word. 'n Alternatief is om twee of meer rekenaars gedesentraliseerd te plaas en te benut soos Yskor tans doen. Indien nie binne die organisasie beskikbaar nie, kan 'n wedersydse ooreenkoms met 'n naburige instansie met soortgelyke apparaat aangegaan word. Hierdie reëlings moet nie net op papier bestaan nie. Kritiese programme en lêers moet ten tye van die ooreenkoms op die apparatuur getoets word asook gereeld hertoets word met die implementering van modifikasies.

Die sleutelgedeelte van die rugsteunstelsel is die instandhouding van die stel duplikaatlêers van alle dringendnoodsaaklike inligting en rekords van die organisasie. Voordat hierdie lêers geskep word, moet eerstens vasgestel word watter inligting en rekords so belangrik en noodsaaklik is dat dit nodig is om duplikaatlêers daarvan in stand te hou. Vervolgens moet bepaal word waar hierdie lêers geberg gaan word — verkieslik in 'n brandvrye veilige bewaarplek sover soos doenlik vanaf die rekenaarsentrum. Die meeste organisasies maak gebruik van die sogenaamde „seun, vader en oupa" wyse van bywerking waardeur die twee tot vier vorige opgedateerde lêers gehou word as rugsteun indien die nuutste een vir een of ander rede nie geskik vir bywerking blyk te wees nie.

4.4 Kontroles

Die belangrikheid van doeltreffende rekenaarkontroles is steeds besig om te verhoog a.g.v. verskeie faktore:

(a) Die groeiende grootte en kompleksheid van dataverwerkingstelsels veroorsaak dat foute duurder word asook moeiliker om te bespeur;

(b) Die sofistikasie van derdegeslag rekenaars met toevoer d.m.v. terminale bring mee dat soveel meer bronne bestaan vanwaar foutiewe, toevoere geïnisieer kan word;

(c) Ons vind ook vandag 'n steeds stygende afhanklikheid van bestuursinligting, nie net sover dit die finansiële sy aangaan nie maar ook wat betref bemarking, produksie en vooruitskatting;

(d) 'n Voortdurende tekort aan geskikte rekenaarpersoneel lei tot 'n hoë omset en dus tot die indiensneming van marginale werknemers.

'n Verskeidenheid van kontroles kan oor 'n wye front ingestel word maar Bestuur moet in die eerste instansie die behoefte daaraan raaksien, hulle moet kennis dra van die verskillende kontrolemaatreëls. Bestuur se primêre taak sal dan ook wees die formulering van 'n basiese beleid vir kontrolemaatreëls met inagneming van alle voor- en nadele, risikos en koste.

Riglyne vir 'n goedgekontroleerde stelsel is die volgende:

(a) Alle programme en stelsels moet deeglik getoets word voordat dit geïmplementeer word. Dit is noodsaaklik dat parallelle gange, vir 'n bepaalde periode van die ou en nuwe stelsels geprosesseer word waar die resultate deeglik vergelyk moet word. Die nuwe stelsel behoort ook getoets te word d.m.v. toetspakke waar van fiktiewe lêers en transaksies gebruik gemaak word. Hierdie toetspakke moet so volledig moontlik opgestel word sodat alle geldige en ongeldige moontlikhede gekontroleer word. Gedurende oorskakeling moet absoluut verseker word dat alle data korrek in die nuwe stelsel opgeneem word en dat dit slegs een keer gedoen word.

(b) Kwaliteitsbeheer is uiters belangrik en die instelling van 'n afdeling wat daarmee belas is 'n noodsaaklikheid. Die hooffunksie is om ooglopend onrealistiese data te kan beheer. Kleiner probleme word bespeur en uitgeskakel voordat dit groot probleme word. In die eerste instansie moet alle toevoere gekontroleer word en verseker word dat dit realisties en volledig aangebied word. Die volledigheid en verspreiding van alle afvoere moet beheer word en waar moontlik gekontroleer word met kontroletotale vanuit die rekenaar. Alle foute behoort deeglik aangeteken te word sodat die oorsake en bronne vasgestel en die nodige korrektiewe aksie geneem kan word.

(c) Die bandbiblioteek verdien meer aandag as wat dit gewoonlik geniet. Die verlies van 'n produksie- of programband kan 'n duur transaksie wees, en nougesette beheer moet uitgeoefen word sodat bande slegs verwyder word as hulle benodig word, dat slegs gemagtigde personeel toegang het tot die biblioteek, dat alle bande duidelik en noukeurig geregistreer en gemerk word, en dat vol-

ledige rekords van bande in gebruik gehou word. Beheer moet ook hiervandaan uitgeoefen word oor alle bande vir rugsteundoeleindes.

(d) Alle programwysigings moet streng beheer word, asook die getal en gehalte persone wat gemagtig is om wysigings aan te bring. Die geringste verandering kan eienaardige gevolge meebring. Byvoorbeeld: 'n Ruimtelansering te Kaap Kennedy het onlangs misluk a.g.v. 'n rekenaarsimbool ekwivalent aan 'n komma wat per abuis weggelaat is tydens 'n programwysiging. Die weglating het die vuurpyl so ver van koers gestuur dat dit vernietig moes word.

(e) Interne Oudit moet uit wans uit betrek word in die ontwikkeling van stelsels. Bestuur het hier 'n kragtige beheermaatreël en hulle moet daarvan gebruik maak. Die doelwitte van 'n groep ouditeure betrek by die ontwikkeling van rekenaarstelsel kan soos volg opgesom word:

(i) Ontwikkel nuwe geoutomatiseerde ouditegnieke en dra sorg dat dit ingebou word in die stelsel;

(ii) Ontwikkel kontrolebehoeftes en -tegnieke en benadruk die nodigheid vir 'n deeglike beheerstelsel by stelselontledingpersoneel;

(iii) Evalueer die doeltreffendheid van die beheerstelsel terwyl dit in die ontwikkelingstadium is;

(iv) Evalueer alle ander areas soos stelseltoetsing en -oorskakeling waar kontroles noodsaaklik is.

(f) Geen enkele groep moet totale verantwoordelikheid vir die beveiliging van rekenaarstelsels ontvang nie. Die behoefte aan en nodigheid vir kontroles moet deur die hele organisasie benadruk en toegepas word, van topbestuur af na alle betrokke personeel.

4.5 Sekuriteitsklaring van Werknemers

Die gedagte van sekuriteitsklaring van werknemers is besig om veld te wen. Waar immigrasie en die gevolglike kosmopolitiese kleur wat aan organisasies verleen word 'n algemene verskynsel is vandag, is dit noodsaaklik dat van een of ander streng keuringsmetode gebruik gemaak word. In die besonder dan behoort elke werknemer met toegang tot die rekenaarsentrum aan 'n sekuriteitsklaring onderwerp te word.

4.6 Versekering teen verliese

Nadat Bestuur toegesien het dat alle redelike stappe geneem is om die beveiliging van inligting en toerusting te waarborg, moet sterk oorweging geskenk word aan die koop van assuransie as dekking teen verliese a.g.v. een of ander onvoorsiene katastrofe. Daar bestaan vier moontlike gebiede waarvoor versekering gekoop behoort te word.

(a) verlies of beskadiging van toerusting;
(b) koste van rekonstruering van lêers en programme;
(c) ander kostes aangegaan tydens terugkering na normale verwerking, en
(d) enige bedryfsverliese a.g.v. ontwrigting van normale bedryfsaktiwiteite.

5. SLOT

Alhoewel perfekte beveiliging- en sekuriteitstelsel miskien buite bereik is vir die meeste organisasies, kan enige organisasie 'n realistiese stelsel daarstel teen redelike koste. Die groot behoefte tans is om deur te dring tot Bestuur, want die verskeie probleme sal slegs deur bemiddeling van topbestuur opgelos kan word. Wat dus nodig is van Bestuur is:

(a) hul bewuswording van die probleem;
(b) 'n waardering van die risiko betrokke, en
(c) 'n besliste voorneme om ernstige katastrofes te voorkom.