Instituut voor Veiligheids- en Crisismanagement

rapportage

veiligheidsmanagement en crisisbeheersing

in het

hoger onderwijs

en het

wetenschappelijk onderzoek

Dr. I. Helsloot
Drs. W. Jong
Drs. A.G.W. Ruitenberg
Drs. M.P. Verhaar
Prof. mr. dr. E.R. Muller

COT Instituut voor Veiligheids- en Crisismanagement
Den Haag, 9 juli 2004

Inhoudsopgave

MANAGEMENTSAMENVATTING

Inleiding

De directie hoger onderwijs van het ministerie van Onderwijs, Cultuur en Wetenschap (OCW) heeft het COT, Instituut voor Veiligheids- en Crisismanagement de opdracht gegeven onderzoek te doen naar veiligheidsmanagement en crisisbeheersing in het hoger onderwijs en het wetenschappelijk onderzoek (voor definities van de gebruikte begrippen wordt verwezen naar de hoofdstuk 1).

De resultaten van het onderzoek moeten de sector ondersteunen bij het vormgeven van eigen inspanningen om mogelijke risico's te onderkennen en te beheersen. In het onderzoek worden daartoe, op basis van (internationale) literatuurstudie en de ervaringen van de instellingen zelf, de risico's benoemd die de instelling bedreigen. Vervolgens wordt de huidige stand van zaken met betrekking tot veiligheidsmanagement en crisisbeheersing in de sector in beeld gebracht. Het gaat hierbij om tot nu toe gevoerd beleid en *'best practices'*. Voor het destilleren van deze feiten en ervaringen van de instellingen zijn enquêtes uitgezet bij hogescholen, universiteiten en wetenschappelijke instellingen. Voorts zijn interviews gehouden met veiligheidscoördinatoren binnen de instellingen en bij ministeries (zie bijlage IX). Tot slot zijn twee werkconferenties georganiseerd voor operationeel en bestuurlijk verantwoordelijken om de voorlopige resultaten van het onderzoek te bespreken.

De context: een veranderende maatschappij

Het hoger onderwijs wordt grotendeels met dezelfde 'nieuwe' en dezelfde 'klassieke' veiligheidsvraagstukken geconfronteerd als andere sectoren in de samenleving.

De volgende maatschappelijke macrotrends hebben een directe invloed op de risico's binnen de instellingen:

- *Toenemende agressie en geweldpleging* binnen de maatschappij. Deze trend is, zo blijkt bijvoorbeeld uit dit onderzoek, ook zichtbaar binnen de sector van het hoger onderwijs en het wetenschappelijk onderzoek.
- *Bezuinigingen en efficiencyoperaties* (al dan niet in het kader van privatisering en

bevordering van marktwerking). Deze romen veelal de redundantie in personeel en middelen af die voorheen als vanzelfsprekend een bijdrage leverden aan risicopreventie. Ook binnen instellingen van het hoger onderwijs en wetenschappelijk onderzoek is deze trend zichtbaar.

- *Ontwikkeling en toenemend gebruik van ICT* verhoogt de afhankelijkheid hiervan. Instellingen binnen de sector zijn in toenemende mate kwetsbaar voor virussen, hackers, stroomuitval en ander elektronisch ongemak.
- *'Gedogen is uit'*; regelgeving dient nageleefd te worden. De overheid, maar ook verzekeraars, treden steeds meer handhavend op. Niet naleving van wettelijke eisen maakt instellingen kwetsbaar voor bijvoorbeeld aansprakelijkheidsstelling.
- De *multiculturalisering van de samenleving* neemt toe. Deze multiculturalisering kan behalve als culturele verrijking ook gezien worden als een potentiële bron van spanning. Zo kan de spanning tussen groepen studenten met verschillende culturele achtergronden bijvoorbeeld door gebeurtenissen elders in de wereld soms oplopen.

De risicobeschrijving: drie domeinen en twee dimensies

Instellingen zijn met betrekking tot de risico's die zij lopen niet zonder meer vergelijkbaar. Elke instelling kent specifieke risico's. Dit heeft onder andere te maken met de geografische ligging van de instelling, de studentenpopulatie en de aard van de opleiding of het onderzoek. Aan de andere kant zijn veel veiligheidsrisico's wel vergelijkbaar, zoals brand, inbraak en kennisfraude. Ook kan worden opgemerkt dat de risico's verschillen in termen van beïnvloedbaarheid door de instelling of van diegenen die het effect van het risico ondergaan.

In het rapport is gekozen voor de volgende categorisering van de risico's in drie domeinen:

- Risico's op het gebied van 'het hoger onderwijs als spiegel van de samenleving';
- Risico's op het gebied van 'het hoger onderwijs als organisatie;'
- Risico's op het gebied van 'het hoger onderwijs als kennisbeheerder'.

De risico's die vallen onder het domein *'hoger onderwijs als spiegel van de samenleving'* zijn de algemeen maatschappelijke risico's die als vanzelfsprekend weerspiegeld worden in het hoger onderwijs met haar publieke functie. Het gaat dan vooral om bedreigingen van de

sociale veiligheid.

De risico's die vallen onder het domein *'hoger onderwijs als organisatie'* zijn de risico's die elke organisatie bedreigen en dús ook de onderwijssector. Het gaat daarbij om uiteenlopende zaken als bijvoorbeeld fraude, diefstal en brand. Omdat het nadrukkelijk méér betreft dan alleen fysieke veiligheid, kiest dit rapport voor de terminologie *'organisatieveiligheid'*.

De risico's die vallen onder het domein *'hoger onderwijs als kennisbeheerder'* zijn de risico's die samenhangen met de kwetsbaarheid van het primaire proces van het onderwijs en het wetenschappelijk onderzoek: kennis verwerven, beheren en verspreiden. Deze kennis kan op verschillende manieren verloren gaan of onbedoeld verspreid worden. Een belangrijke risico dat in dit domein valt is de kwetsbaarheid van de ICT-infrastructuur binnen instellingen. Kennisverlies kan wetenschappelijke, commerciële of maatschappelijke belangen bedreigen.

Het praktisch nut van deze driedeling is dat ze inzichtelijk maakt welke risico's uniek zijn voor het hoger onderwijs (de kennisbeheerfunctie), welke risico's afhankelijk zijn van maatschappelijke ontwikkelingen (de spiegel van de samenleving) en welke risico's voor een onderwijsinstelling niet anders zijn dan voor elke andere organisatie (onderwijs als organisatie).

Binnen deze drie domeinen zullen de risico's in dit onderzoek vervolgens verder onderscheiden worden naar de dimensies 'oorzaak' en 'effect'. Hierdoor wordt zichtbaar welke risico's door de instellingen binnen het hoger onderwijs en het wetenschappelijk onderzoek primair zelf te beïnvloeden zijn en welke risico's hun effect primair binnen of buiten de instellingen hebben.

Uitkomsten inventarisatie van het huidige veiligheidsbeleid binnen de sector

Uit de inventarisatieronde (enquêtes, bijeenkomsten en interviews) blijkt dat de instellingen in het hoger onderwijs nog geen structurele en integrale aandacht voor veiligheidsmanagement en crisisbeheersing hebben. Binnen instellingen zijn de drie deelgebieden (sociale veiligheid, organisatieveiligheid en kennisveiligheid) veelal verkokerd. Instellingen, medewerkers en

studenten zijn zich beperkt bewust van de verschillende risico's die zij alsook hun omgeving lopen.

Er vindt betrekkelijk weinig uitwisseling plaats van ervaringen die de instellingen opdoen. Ook binnen instellingen is de betrokkenheid van medewerkers en studenten bij het veiligheidsbeleid en de implementatie daarvan veelal gering.

Op *sociaal veiligheidsgebied* blijken de instellingen momenteel vooral gericht op inmiddels klassieke risico's als diefstal, sexuele intimidatie of problemen van individuele studenten waarvoor veelal al voorzieningen zijn getroffen in de vorm van de aanwezigheid van vertrouwenspersonen, klachtenprocedures en een sanctiebeleid. Instellingen lijken nog minder oog te hebben voor de risico's die de gesignaleerde maatschappelijke ontwikkelingen met zich meebrengen. Ook op incidenten die zich buiten de instelling afspelen waarbij studenten of medewerkers zijn betrokken, zijn instellingen minder goed voorbereid.

Op het gebied van de *organisatieveiligheid* blijken de instellingen zich vooral voor te bereiden op de binnen dat domein bekende risico's zoals brand en inbraak. Bijzondere risico's zoals fraude, het vrijkomen van gevaarlijke stoffen of organismen vanuit laboratoria of de dreiging van aanslagen hebben nog lage prioriteit. Instellingen ervaren juist binnen dit domein een toenemende druk van externe partijen, zoals vergunningverleners, inspecties en verzekeraars.

Binnen het domein van de *kennisveiligheid* zijn instellingen momenteel vooral gericht op de ICT-risico's. De inzet op de beheersing van andere risico's binnen dit domein, zoals kennisfraude en het voorkomen dat gevoelige informatie in handen komt van ongewenste personen en organisaties, blijft daarbij in het algemeen nog sterk achter.

Een handvat voor het beperken van risico's binnen de instelling

Teneinde de sector te ondersteunen bij het vormgeven van eigen inspanningen om mogelijke risico's te onderkennen en te beheersen, is een (zelf)auditkader ontwikkeld voor bestuurlijk en operationeel verantwoordelijken. In de Hoger Onderwijs Veiligheidsaudit (opgenomen als

bijlage I) worden normen voor veiligheidsmanagement en crisisbeheersing aangereikt. Deze zijn gekoppeld aan specifieke risico's binnen de drie risicodomeinen.

De normen uit de Hoger Onderwijs Veiligheidsaudit kunnen als volgt worden samengevat:

Bestuurlijk niveau: Voor veiligheidsbeleid is een gelijke beleidscyclus ingericht als voor andere beleidsterreinen. Dat wil zeggen veiligheidsbeleid voor alle drie risicodomeinen is vastgesteld op basis van een risicoanalyse. Beleidsdoelen zijn geprioriteerd en gebudgetteerd. Over de uitvoering van het beleid wordt gerapporteerd aan het bestuur. Het bestuur legt op haar beurt verantwoording af over het veiligheidsbeleid in jaarverslagen.

Operationeel niveau, algemeen: Concrete uitvoeringsplannen zijn vastgesteld, inclusief budget en prioriteiten. Over de uitvoering wordt gerapporteerd aan het bestuur. (Bijna)incidenten worden geregistreerd – hiervoor bestaat onder andere een (anonieme) meldingsstructuur – en geanalyseerd. Jaarlijkse risico- en incidentanalyses leiden tot bijstelling van beleid en uitvoeringsplannen.

Operationeel niveau, sociale veiligheid: Binnen dit risicodomein houdt de instelling rekening met de toenemende agressie binnen de maatschappij, met de toenemende multiculturalisering van de samenleving, met problemen van individuele studenten, met de effecten van extern ongewenst gedrag van studenten en stagairs en met de effecten van sociale onveiligheid buiten de instelling op studenten en medewerkers van de instellingen.

Operationeel niveau, organisatieveiligheid: Binnen dit risicodomein bestaat veel relevante regelgeving, de instelling leeft deze regels na. De instelling houdt verder rekening met de risico's van diefstal, van fraude, van brand, van extreme weersomstandigheden, van experimenten waarbij gevaarlijke stoffen of organismen zijn betrokken, van controversiële experimenten en van infectieziekten.

Operationeel niveau, kennisveiligheid: De instelling voldoet aan de eisen van ISO-17799 ter beveiliging van kennis. De instelling onderkent in het bijzonder de kwetsbaarheid van ICT-

infrastructuur en neemt daarom adequate maatregelen ter beveiliging. Kennis is zodanig geborgd dat deze bij calamiteiten – zoals brand – niet verloren gaat. Voor kennis die commercieel of vanuit het oogpunt van de proliferatie van massavernietigingswapens gevoelig is, kent de instelling geclassificeerde toegang.

HOOFDSTUK 1
INLEIDING

1.1 Inleiding

De directie hoger onderwijs van het ministerie van Onderwijs, Cultuur en Wetenschap heeft het COT Instituut voor Veiligheids- en Crisismanagement de opdracht gegeven onderzoek te doen naar veiligheidsmanagement en crisisbeheersing[1] in het hoger onderwijs en de bijbehorende onderzoeksinstituten. De resultaten van het onderzoek moeten deze sector ondersteunen bij het vormgeven van eigen inspanningen om mogelijke risico's te onderkennen en te beheersen.

Dit onderzoek is daarmee primair gericht op de instellingen voor hoger onderwijs en wetenschappelijk onderzoek die vallen onder de verantwoordelijkheid van het ministerie van Onderwijs, Cultuur en Wetenschap.

De primaire reden voor deze opdracht is het feit dat het hoger onderwijs grotendeels met dezelfde 'nieuwe' en dezelfde 'klassieke' veiligheidsrisico's wordt geconfronteerd als andere sectoren in de samenleving. Voor de andere sectoren zoals het bedrijfsleven geldt dat deze risico's een directe bedreiging kunnen zijn voor de kwaliteit en continuïteit van de eigen bedrijfsvoering. Binnen de onderwijssector hebben vergelijkbare risico's directe invloed op de continuïteit van het hoger onderwijs en onderzoek.

Een voorbeeld van een veiligheidsvraagstuk in het hoger onderwijs is de kwetsbaarheid van informatiesystemen in de virtuele leeromgeving (authenticiteit, manipulatie en diefstal van informatie). Een tweede voorbeeld is de kwetsbaarheid van de zich uitbreidende fysieke infrastructuur van het hoger onderwijs (diefstal, complexer wordende arbo-omstandigheden, brand). Het meest spraakmakende voorbeeld was de recente brand in het rekencentrum van de TU Twente. Dit voorbeeld van een 'klassieke' calamiteit werd door de locatie van de brand

[1] Veiligheidsmanagement wordt hier gedefinieerd als alle activiteiten gericht op het beheersen van risico's, dat wil zeggen het voorkomen dat zij zich materialiseren als incident. Crisisbeheersing is het bestrijden van de gevolgen van een eenmaal ontstaan incident. In de hoofdstukken 2 en 3 wordt hier nader op ingegaan.

direct verbonden met een ‘nieuw’ veiligheidsvraagstuk: het beschermen van informatie en het tijdelijk vervangen en opnieuw opstarten van een essentieel ICT-systeem voor onderzoek en onderwijs.

Op 20 november 2002 wordt brand gesticht op het complex van de TU Twente. De brand verwoest het computercentrum van de universiteit en legt de werkkamers van tientallen medewerkers van drie faculteiten in de as. De geschatte schade is 40 tot 50 miljoen euro. Voor verzekeraars is de brand aanleiding om de polissen in heel Nederland te herzien en de risicobeoordeling van universiteiten, hogescholen en onderzoeksinstellingen tegen het licht te houden.

Bovenstaande voorbeelden illustreren de noodzaak voor zowel veiligheidsmanagement als crisisbeheersing. De onderwijs- en onderzoeksinstituten kunnen zich immers niet onttrekken aan ontwikkelingen in en rond het eigen veld, de veiligheidsvraagstukken die dat met zich meebrengt en het daaruit voortvloeiende wens om beleid en verantwoording. De verantwoordelijkheid hiervoor ligt bij de instellingen zelf. ‘Organisaties zoals de IB-Groep in Groningen, het Primatencentrum in Rijswijk, maar ook scholen, hogescholen en universiteiten hebben een bepaalde zelfstandigheid. De minister is niet staatsrechtelijk verantwoordelijk voor deze organisaties. De minister heeft wel een zekere ‘morele’ verantwoordelijkheid voor deze organisaties.’[2]

Dit onderzoek beoogt bij te dragen aan de ontwikkeling van inzichten en hulpmiddelen ten behoeve van veiligheids- en crisismanagement voor het hoger onderwijs. Kernbegrippen in het onderzoek zijn anticipatie op risico’s, realiteitszin bij de voorbereiding erop en begrip voor de context van het hoger onderwijs en de onderzoeksinstellingen. Het onderzoek is gebaseerd op een integrale aanpak die aansluit bij bestaande structuren en uitgangspunten voor beleid zoals de autonomie van de instellingen. Het onderzoek streeft naar aanvulling van de bestaande structuren en uitgangspunten vanuit het oogpunt van veiligheid en crisismanagement.

Dit eerste inleidende hoofdstuk geeft in paragraaf 1.2 een kort overzicht van de verschillende betrokkenen en hun rol bij de veiligheidsvragen in het hoger onderwijs en de

[2] Ministerie van OCW, Risicoanalyse normale bedrijfsvoering, 2004, p. 4

wetenschappelijke onderzoeksinstituten. In paragraaf 1.3 worden de uitgangspunten van het onderzoek geschetst. In de afsluitende paragraaf 1.4 wordt ingegaan op inhoud en inrichting van het onderzoek.

1.2 Veiligheid in het hoger onderwijs en het wetenschappelijk onderzoek

De verantwoordelijkheid voor de voorbereiding op crises en calamiteiten is, zoals hierboven al vermeld, primair neergelegd bij de instellingen zelf. In dit en eerder onderzoek[3] blijkt dat mede daardoor de mate van voorbereiding op crises en calamiteiten per instelling sterk verschilt. Er is geen gangbare norm waaraan de instellingen geacht worden te voldoen met betrekking tot de voorbereiding op crises en calamiteiten; geen richtlijn voor het inrichten van een crisisorganisatie, geen uniforme methode voor risico-inschatting, anders dan volgend uit Arbo-verplichtingen. Onderlinge afstemming –tussen instellingen– over dergelijke maatregelen blijkt niet of beperkt (en dan vaak ad hoc of informeel) plaats te vinden. Koepelorganisaties, zoals de VSNU en de HBO-raad kunnen een belangrijke functie vervullen in de afstemming tussen instellingen, maar hebben dat tot op heden slechts in beperkte mate gedaan.

Wettelijke verantwoordelijkheden voor de instellingen liggen vast in verschillende wetten en lagere regelgeving. De Arbeidsomstandighedenwet is daarvan de meest generieke; zij vereist inventarisatie en analyse van alle risico's die werknemers en andere aanwezigen kunnen lopen. Vervolgens dienen dan adequate maatregelen getroffen te worden. Specifieke wet- en regelgeving biedt het kader voor verplichte maatregelen voor specifieke risico's zoals brand (Woningwet, gebruiksvergunningen) of verontreiniging van het milieu (Wet milieubeheer).

Hoger onderwijsinstellingen geven op diverse manieren invulling aan hun verantwoordelijkheid voor de veiligheid binnen en buiten hun instelling. Zo kent elke instelling een of meer arbo-coördinatoren. Ook op het gebied van sociale veiligheid en ICT-beveiliging worden op veel plaatsen activiteiten ontplooid binnen de hoger

[3] Zie bijvoorbeeld COT, Aandachtspunten OCW dreiging oorlog Irak, 2003, p. 3

onderwijsinstellingen. Veel projecten zich door hun oriëntatie op geïsoleerde risico's. Ze vloeien niet voort uit niet een integraal risicobeleid.

Behalve de instellingen zelf hebben nog meer partijen een deelverantwoordelijkheid voor de veiligheid op en rondom hoger onderwijsinstellingen. Zo is het ministerie van OCW verantwoordelijk voor het functioneren van het hoger onderwijsstelsel. Vanuit die verantwoordelijkheid kan zij randvoorwaarden stellen aan de bedrijfsvoering (waaronder veiligheidsmanagement en de voorbereiding op crisisbeheersing valt). Daarnaast houdt het ministerie toezicht op de wijze waarop de instellingen deze randvoorwaarden invullen. Het ministerie heeft tot nu toe vooral specifieke aandacht besteed aan veiligheids- en crisismanagement door het attenderen van de instellingen op bijzondere risico's. Een voorbeeld hiervan zijn de brieven uit 2001 en 2003 aan de instellingen waarin op risico's van (bio)terreur werd gewezen.[4]

Gemeenten hebben een algemene verantwoordelijkheid voor de veiligheid en voorbereiding op calamiteiten op het gemeentelijk grondgebied. Zij zijn uit dien hoofde ook veelal de vergunningverlener voor tal van activiteiten. 'Gebieden *rondom* scholen zijn onderdeel van het publieke domein, waarvoor gemeenten in eerste instantie verantwoordelijk zijn'.[5] Afstemming tussen hoger onderwijsinstellingen en gemeente(lijke diensten) is daarmee noodzakelijk.

Een bijzonder veiligheidsvraagstuk is na 11 september 2001 meer dan ooit actueel. Bedreigingen van de staatsveiligheid kunnen kiemen hebben binnen het hoger onderwijs. In de Nederlandse praktijk ligt de focus met name op de ongewenste kennistransfer naar bepaalde landen of groepen. Ook (de voorbereiding op) een terreuraanslag kan echter plaatsvinden binnen het hoger onderwijs of de wetenschappelijke onderzoeksinstellingen. In het kader van dit onderzoek is aansluiting gezocht bij de activiteiten van de AIVD op dit vlak en wordt er op basis daarvan aandacht besteed aan deze risico's in deze rapportage.

[4] 'OWB/NTM/01/39501 2 november 2001 en WO/2003/9260 6 maart 2003.
[5] TK 21761, Schriftelijk overleg inzake de monitor Sociale veiligheid, 24 juni 2003.

1.3 Uitgangspunten van het onderzoek

Voor de acceptatie en een succesvolle implementatie van de onderzoeksresultaten in het hoger onderwijs en het wetenschappelijk onderzoek wordt aansluiting gezocht bij de cruciale kenmerken van en uitgangspunten bínnen de sector. Bij het onderzoek zijn de resultaten daarom steeds getoetst aan de onderstaande uitgangspunten:

Context: Autonomie van de instellingen.
Met andere woorden: de instellingen bepalen zelf, binnen de daartoe bestaande kaders, wat ze willen doen met de uitkomsten van het onderzoek. Dit betekent dat instellingen vanaf het eerste moment betrokken zijn geweest bij het onderzoek. In sessies met een begeleidingsgroep van vertegenwoordigers van de instellingen en in twee conferenties zijn de resultaten van dit onderzoek besproken (en daar waar nodig aangepast).

Context: Eerbiediging van de kerntaak van het hoger onderwijs en wetenschappelijk onderzoek: het vrij verspreiden, verzamelen en uitwisselen van kennis.
Het hoger onderwijs en wetenschappelijk onderzoek is gericht op kennisuitwisseling en -verzameling en doet dit in een relatie tot grote groepen mensen en/of organisaties. Aanbevelingen en initiatieven die zich richten op het verbeteren van het veiligheids- en crisismanagement, moeten recht doen aan deze doelstellingen en kenmerken. Weliswaar tracht dit onderzoek de bewustwording van de nadelen van een ongeremde vrije kennisuitwisseling te stimuleren, maar het is aan de instellingen om daarover zelf de nodige afwegingen te maken.

Context: Aandacht voor de implementatie van veiligheids- en crisismanagement in het bestaande management
Het is belangrijk voortdurend de resultaten van het onderzoek te toetsen op toepasbaarheid en inpasbaarheid. Wil veiligheids- en crisismanagement effectief kunnen zijn, dan zal dit integraal onderdeel moeten worden van het reguliere management binnen instellingen. Het onderzoek tracht dan ook aan te sluiten bij bestaande structuren en instituties binnen instellingen.

Realiteitszin: incidenten met een lage frequentie vereisen een aanpak met lage kosten (tijd en geld), tenzij de verantwoordelijkheidsvraag en de aansprakelijkheidvraag dit niet toestaan.
Veiligheid vergt investeringen waarvoor de ruimte niet onbeperkt is. Ervaring leert dat incidenten met een lage frequentie grotendeels worden voorkomen met maatregelen die relatief goedkoop zijn. Daarbij geldt de spreekwoordelijke 80/20 regel: 80% van de incidenten kan met een extra investering van 20% worden voorkomen, maar om de resterende 20% van de incidenten uit te kunnen sluiten is tenminste nog eens 80% aan extra inspanningen benodigd.

Realiteitszin is echter méér dan kansberekening: na bepaalde typen incidenten kan de vraag om verantwoording, boetedoening en schadeloosstelling dermate krachtig (maar ook verstorend) zijn, dat ongeacht het risico het wenselijk is om het incidenttype met beleidsinspanningen te vermijden. Dit heeft als consequentie dat niet alleen de objectieve risico's en incidenten onderdeel zijn van het veiligheidsmanagement, maar ook de subjectieve beleving van die risico's en incidenten.

1.4 Inhoud en inrichting van het onderzoek

Het onderzoek is in vier fasen uitgevoerd.

Fase 1: Vooronderzoek en projectplan
Fase 1 van het onderzoek bestond uit het vormgeven van een projectplan waarin de vorm en de inhoud van het onderzoek nader werd uitgewerkt op basis van een vooronderzoek. Het vooronderzoek leverde in het bijzonder een onderzoekskader op voor het uitvoeren van de risicoscan in de volgende stap.

Het vooronderzoek strekt zich uit over het gehele hoger onderwijs en wetenschappelijk onderzoek. Het COT maakte daarbij gebruik van:

- Uitgebreide deskresearch: wetenschappelijke literatuur, onderzoeksrapporten, beleidsnotities, wet- en regelgeving en internet.

- Face-to-face interviews met sleutelinformanten van het ministerie van OCW en andere ministeries, onderwijsinstellingen, onderzoeksinstituten, hulpdiensten en externe deskundigen. (De respondentenlijst is opgenomen in bijlage II).
- Een telefonische ronde langs een selectie van instellingen om praktische informatie te verkrijgen over de stand van zaken met betrekking tot veiligheidsmanagement in brede zin.

Fase 2: Risicoscan

Fase 2 bestond uit het uitvoeren van een enquête die de onderkende risico's in het hoger onderwijs inzichtelijk maakt en ook weergeeft welke structuren en instituties ('best practices') al bestaan voor het management van deze risico's. Uit deze risicoscan bleken, na een vergelijking met de resultaten van het vooronderzoek, de hiaten in het huidige veiligheidsmanagement maar kwamen ook *best practices* naar voren die het waard zijn gedeeld te worden.

Ten behoeve van de risicoscan is een gestructureerde vragenlijst opgesteld. De lijst is gedifferentieerd naar instellingen, risicotypen en verantwoordelijken binnen de instellingen. Na het testen van de vragenlijst in een aantal proefinterviews is de lijst toegestuurd aan alle instellingen in het hoger onderwijs.

Fase 3: Rol- en strategiebepaling

Op basis van de resultaten uit fase 1 en 2 is een conceptrapportage opgesteld die input was voor twee werkconferenties over veiligheidsmanagement en crisisbeheersing binnen het hoger onderwijs en het wetenschappelijk onderzoek. De eerste werkconferentie (op 8 april 2004) was gericht op de operationeel verantwoordelijken binnen de instituten. In deze werkconferentie is het conceptrapport besproken en zijn oplossingsrichtingen voor de door het COT geïnventariseerde risico's besproken. De tweede werkconferentie (op 13 mei 2004) was gericht op de bestuurlijk verantwoordelijken. In bijlage VI en VII zijn de aanwezigen op deze conferenties vermeld.

Aan de hand van de conceptrapportage zijn in de werkconferenties de 'witte vlekken' in het

huidige veiligheids- en crisismanagementbeleid geïdentificeerd en nader besproken. Het verslag van de bestuurlijke werkconferentie is als bijlage V op genomen in deze rapportage. Genoemde opmerkingen zijn logischerwijs in dit verslag verwerkt.

Fase 4: Ontwikkeling Hoger Onderwijs Veiligheidsaudit

Het onderzoekskader voor de risicoscan is doorontwikkeld tot een (zelf)auditkader voor het periodiek bepalen van de stand van zaken met betrekking tot veiligheidsmanagement, wat heeft geleid tot de Hoger Onderwijs Veiligheidsaudit. Deze Hoger Onderwijs Veiligheidsaudit is als bijlage I opgenomen in dit rapport.

HOOFDSTUK 2
RISICO'S EN CRISES

2.1 Inleiding

In dit hoofdstuk wordt ingegaan op risico's en crises. Hierbij zal in eerste instantie meer algemene theorie gepresenteerd worden om daarna meer specifiek aandacht te besteden aan de relevante aspecten ervan voor het hoger onderwijs en het wetenschappelijk onderzoek.

In paragraaf 2.2 wordt ingegaan op het begrip 'risico'. In paragraaf 2.3 wordt een risicoclassificatie voor het hoger onderwijs geïntroduceerd die in deze rapportage gebruikt wordt. Paragraaf 2.4 definieert het begrip crisis en gaat in op relevante crisistrends.

2.2 Risico's

Wat is een risico?
In de hier voorafgaande tekst is het begrip 'risico' gebruikt zonder dat daar een solide introductie aan vooraf is gegaan. Voor de meeste lezers zal het geen probleem zijn geweest om toch de inleiding te kunnen begrijpen. Het woord 'risico' kent bij de meeste van ons een natuurlijke connotatie waar begrippen als 'gevaar', 'mogelijkheid' en 'ongewenstheid' bij horen.

Vanuit dat natuurlijke begrip van het woord 'risico' is de eenvoudige samenvatting van deze paragraaf verrassend: er bestaat geen een eenduidige definitie van het begrip risico welke door alle deskundigen binnen het vakgebied 'veiligheid' wordt gedragen. In de literatuur worden tal van uiteenlopende omschrijvingen van het begrip 'risico' gebruikt. Gratt bijvoorbeeld, presenteerde in 1993 veertien definities van risico. Vlek deed in 1990 vergelijkbaar werk en distilleerde twintig definities van risico uit de literatuur.

Risico impliceert 'onzekerheid' en 'ongewenstheid' . 'Risico' is met andere woorden de

mogelijkheid dat een ongewenste gebeurtenis optreedt.

> Risico is de mogelijkheid, met een zekere mate van waarschijnlijkheid, van schade aan de gezondheid van mens, aan het milieu en aan goederen in combinatie met aard en omvang van die schade [6]

Wie risico's echter objectief wil vergelijken, bijvoorbeeld om tot een prioritering van veiligheidsmaatregelen te komen, wil bij voorkeur een harde maatlat hebben waaraan hij soort en omvang van een risico kan bepalen. In de verzekeringswereld hanteert men daartoe al sinds jaar en dag een simpele formule: risico is kans maal schade (in euro's). Deze formule is zeer bruikbaar voor deze doelgroep.[7] Vanzelfsprekend blijft ook voor de verzekeraar het probleem om tot significante data te komen, waarop de kans op een bepaald type ongeval met een bepaalde financiële schade kan worden gebaseerd.

Wanneer deze formule breder wordt toegepast dan op verzekerden en de financiële schade van ongevallen die zij veroorzaken of die hen overkomen, komt de problematiek aan de orde hoe men de kans en het effect kan kwantificeren. Controversen over risicobeheersing zijn vaak terug te voeren op keuzes over de begrenzing van het beschouwde systeem.[8] De discussie gaat vaak over wat nu de risicodragende activiteiten zijn, wat de schade is, welk causaal verband bewezen is en binnen welke tijd effecten moeten optreden.

Voor het hoger onderwijs en het wetenschappelijk onderzoek geldt bijvoorbeeld dat het problematisch is de kans op laboratoriumongevallen te berekenen of het effect van bijvoorbeeld imago- of reputatieschade te kwantificeren. Het is daarom voorspelbaar onmogelijk om binnen het hoger onderwijs en het wetenschappelijk onderzoek te komen tot een uniforme harde maatlat waaraan risico's gemeten kunnen worden. De afweging van risico's en investeringen in risicobeheersing dient daarom op bestuurlijk niveau en met vooral gezond verstand plaats te vinden.

---

[6] Gezondheidsraad, Commissie Risicomaten en risicobeoordeling, Niet alle risico's zijn gelijk. Kanttekeningen bij de grondslagen van de risicobenadering in het milieubeleid, Den Haag, advies 1995/06, 1995.

[7] De geabstraheerde versie van deze formule is in kringen van veiligheidsdeskundigen breed geaccepteerd: risico is kans maal effect. De onvergelijkbaarheid van 'appels en peren', maakt dat deze formule beperkt bruikbaar is in de (bestuurlijke) praktijk.

[8] RIVM, Nuchter omgaan met Risico's, Milieu- en Natuurplanbureau (MNP), rapport 251701047/2003, 2003, p. 19.

Anticipatie versus veerkracht

Een klassieker op het gebied van veiligheidsonderzoek en risicoanalyses is Wildavsky.[9] Hij onderscheidt twee manieren waarop door individuen, organisaties en de samenleving als geheel omgegaan wordt met risico's. Enerzijds kan ingezet worden op het zoveel vermijden van risico's, anderzijds kan een zekere mate van risico geaccepteerd worden. Wildavsky begint zijn bekende boek met het joggersdilemma: wie jogt accepteert een klein verhoogd risico op een inspanningshartaanval tijdens het joggen, maar verhoogd gemiddeld gesproken zijn gezondheid. Evenzo heeft de samenleving zich volgens Wildavsky vooral kunnen ontwikkelen dankzij de risico's die in de loop der eeuwen genomen zijn.

Het mijden van risico's - of juist risico's durven nemen - vergt volgens hem derhalve een bewuste keuze tussen een tweetal strategieën: anticipatie versus veerkracht.

- Anticipatie is gericht op het vermijden van onzekerheden en risico's; dit kan bijvoorbeeld door strenge eisen te stellen aan de toegang tot hoger onderwijsinstellingen of door bepaalde experimenten geheel te verbieden.
- Veerkracht is daarentegen een geheel ander soort strategie. Hierbij accepteert men (beperkte) risico's en organiseert men zich op zo'n manier, dat het mogelijk is flexibel te reageren op een eventueel incident of onregelmatigheid.

In de praktijk is 'anticipatie' een veelgekozen strategie. In essentie gaat het dan om situaties waarin er sprake is van een hoge kans of een groot (onomkeerbaar) effect. Brand komt bijvoorbeeld dermate vaak voor dat de maatschappij brandpreventieve eisen stelt. Door de eisen toe te passen wordt de grote kans op brand teruggebracht tot een geaccepteerde kans. Een mogelijke ontsnapping van het pokkenvirus heeft een dermate groot effect, dat hiermee wereldwijd niet geëxperimenteerd mag worden.

De afweging tussen de strategieën anticipatie en veerkracht wordt in de praktijk vaak niet bewust gemaakt. In de huidige samenleving is anticipatie een zodanig dominante strategie dat de keuze voor veerkracht veelal slechts impliciet gemaakt wordt , met name als anticiperende

[9] A. Wildavsky, Searching for Safety, New Brunswick, 1988.

maatregelen onrealistisch duur zijn. Maatschappelijk gezien nemen we, als het even kan, liever het zekere voor het onzekere.

Risico is perceptie

De onderkenning dat het effect van een risico voor een groot deel samenhangt met de perceptie ervan dateert al van lang geleden. De stelling*: 'If men defines their situations as real, they are real in their consequences'* werd al in 1928 door Thomas en Thomas geponeerd.[10]

Er zijn vele factoren die de perceptie van een risico beïnvloeden. Het maakt bijvoorbeeld een groot verschil in de waardering van het risico of een risico samenhangt met een techniek met vaak optredende ongevallen, maar met relatief geringe gevolgen, of met een techniek met zelden voorkomende ongevallen maar met ernstigere gevolgen en grote aantallen slachtoffers. Zo wordt het risico op een verkeersongeval (met ongeveer duizend doden per jaar in Nederland) als aanvaardbaarder ingeschat dan het risico op een industrieel zwaar ongeval (met gemiddeld een enkele dode per jaar). Ook het verschil tussen een vrijwillig genomen en een onvrijwillig genomen risico is zichtbaar in de perceptie van de gemiddelde mens.

Er is daarmee geen sprake van een bruikbaar onderscheid tussen een geobjectiveerd risico en een perceptie van een risico. 'Een risico is een sociale constructie: betrokken actoren construeren een risico. Geobjectiveerde gegevens kunnen daarbij een rol spelen, maar noodzakelijk is dat niet. Betrouwbare data zijn veelal niet beschikbaar, aannamen waarop de berekening zijn gebaseerd zijn vaak aanvechtbaar, terwijl een risico per definitie een element van onvoorspelbaarheid kent.'[11]

Perceptiefactoren die in de afweging van risico's een rol spelen

Als risico perceptie is, dan is de vraag voor diegenen die risico's moeten afwegen welke aspecten van een risico een belangrijke rol spelen in die perceptie.

[10] W.J. Thomas, D.S. Thomas, The child in America, New York, 1928, p. 572
[11] J.A. de Bruin en E.F. ten Heuvelhof, Management in netwerken, Lemma, Utrecht, 1999, p 125.

Een eerste systematische poging tot het onderzoeken wanneer de voordelen van een activiteit of technologie in de publieke perceptie opwegen tegen de ermee verbonden veiligheidsrisico's is gedaan door Starr.[12] Hij concludeerde in 1969 bijvoorbeeld dat de acceptatie van vrijwillig genomen risico's (zoals verkeersdeelname en roken) ongeveer duizend maal groter is dan die van onvrijwillig genomen risico's. Later onderzoek (vooral door Slovic en Fischoff in Amerika[13] en Vlek en Stallen in Nederland[14]) wijst op een aantal (soms samenhangende) belangrijke aspecten van een risico die de perceptie ervan bepalen:

- de potentiële mate van rampzaligheid ('catastrophic potential' of 'perceived dread')
- onvrijwilligheid in de zin van onbillijkheid (wie profiteert, wie draagt de gevolgen?)
- onvrijwilligheid in de zin van gebrek aan persoonlijke invloed (onbeheersbaarheid)
- nieuwe risico's versus bekende risico's (dus bijvoorbeeld verbonden met nieuwe technologie)
- verborgen of uitgestelde effecten van het risico (bijvoorbeeld kanker vele jaren na blootstelling)
- onhelderheid over maatschappelijke voordelen van risicodragende activiteit.

De laatste jaren wordt in onderzoek naar risicoperceptie ook gewezen op de factoren:

- (gebrek aan) vertrouwen in of openheid van verantwoordelijke instanties
- verwijtbaarheid van het risico in de zin dat bewust onveilig of crimineel gedrag de oorzaak is van het optredende ongeval.

Tot consistente modellering van bovenstaande factoren op een wijze die enige praktisch voorspellende waarde heeft is men echter nog niet gekomen.[15]

[12] C. Starr, 'Social benefits versus technological risk', in: Science, 1969, pp. 1232-1238.
[13] Zie voor een overzicht bijvoorbeeld: P. Slovic, The perception of risk, Earthscan, Londen, 2000.
[14] C.A.J. Vlek en P.J.M. Stallen, 'Persoonlijke beoordeling van risico's', Instituut voor Experimentele Psychologie, Groningen, 1979; A multi-level, multi-stage, multi-attribute perspective on risk assesment, decision making and risk control, in: Risk Decision Policy, 1996, pp. 9-31.
[15] De Zweed Sjöberg is een bekende criticaster van de waarde van alle huidige modellering. Zie daarvoor bijvoorbeeld: L. Sjöberg, 'Are received risk models alive and well?', in: Risk Analysis, 2002, pp. 665-669.

2.3 Een classificatie van risico's in het hoger onderwijs en onderzoek

In dit onderzoek worden de risico's die zich in het hoger onderwijs voordoen c.q. op termijn voor kunnen gaan doen, beschreven op basis van een categorisering in drie domeinen. Deze beoogt recht te doen aan de diversiteit van elementen die een rol spelen bij veiligheid in het hoger onderwijs.

De risico's zijn ingedeeld in de volgende drie domeinen:

a. Het hoger onderwijs als spiegel van de samenleving (sociale veiligheid)
b. Het hoger onderwijs en wetenschappelijk onderzoek als organisatie (organisatieveiligheid)
c. Het hoger onderwijs en wetenschappelijk onderzoek als kennisbeheerder (kennisveiligheid).

Vanzelfsprekend moet rekening worden gehouden met het feit dat risico's zich niet in strikte categorieën laten indelen: brandrisico is beschouwd als een primair risico voor de fysieke veiligheid, maar het heeft nadrukkelijk raakvlakken met de sociale veiligheid (verslonzing verhoogd het risico op brand en brandstichting). Kwetsbaarheid van ICT is een risico voor elke organisatie maar in het hoger onderwijs en het wetenschappelijk onderzoek een essentieel risico voor kennisveiligheid.

Ad a. De risico's die vallen onder het domein *'hoger onderwijs als spiegel van de samenleving'* zijn de algemeen maatschappelijke risico's die als vanzelfsprekend weerspiegeld worden in het hoger onderwijs met haar publieke functie. Het gaat dan vooral om bedreigingen van de sociale veiligheid.

Ad b. De risico's die vallen onder het domein *'hoger onderwijs als organisatie'* zijn de risico's die elke organisatie bedreigen en dús ook de onderwijssector. Het gaat daarbij om uiteenlopende zaken als bijvoorbeeld fraude, diefstal en brand. Omdat het nadrukkelijk méér betreft dan alleen fysieke veiligheid, kiest dit rapport voor de terminologie *'organisatieveiligheid'*.

Ad c. De risico's die vallen onder het domein *'hoger onderwijs als kennisbeheerder'* zijn de risico's die samenhangen met de kwetsbaarheid van het primaire proces van het onderwijs: kennis verwerven, beheren en verspreiden. Deze kennis kan op verschillende manieren verloren gaan of onbedoeld verspreid worden. Een belangrijke risico dat in dit domein valt is de kwetsbaarheid van de ICT-infrastructuur binnen instellingen. Kennisverlies kan wetenschappelijke, commerciële of maatschappelijke belangen bedreigen.

Het praktisch nut van deze driedeling is dat het inzichtelijk maakt welke risico's uniek zijn voor het hoger onderwijs (de kennisbeheerfunctie), welke risico's afhankelijk zijn van maatschappelijke tendensen (de spiegel van de samenleving) en welke risico's voor een onderwijsinstelling niet anders zijn dan voor elke andere organisatie (onderwijs als organisatie).

Twee dimensies voor risico's in het hoger onderwijs en wetenschappelijk onderzoek
Om binnen de domeinen sociale, fysieke en kennisveiligheid de risico's verder onder te verdelen, wordt gebruik gemaakt van twee dimensies: a) de ontstaansgrond en b) de gevolgen die zich voordoen als het risico zich manifesteert.

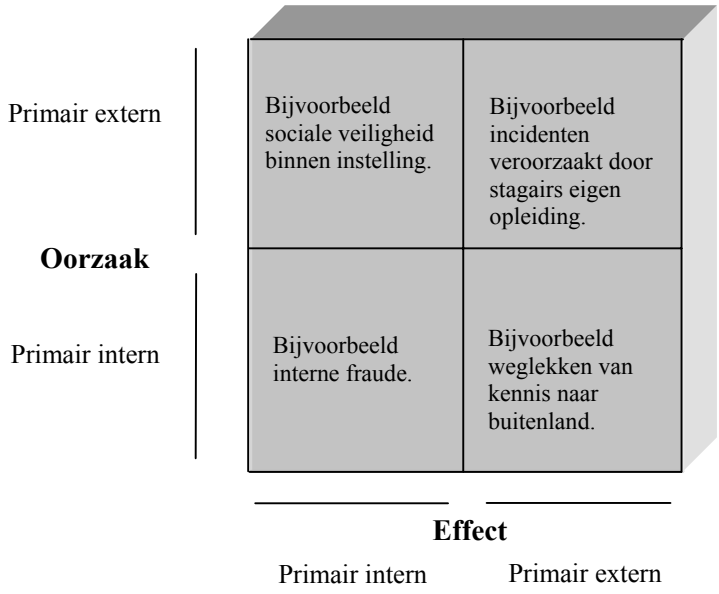
a. Risico's kunnen het resultaat zijn van twee bronnen: een interne oorzaak (binnen de hoger onderwijsinstelling) of een externe oorzaak (buiten de hoger onderwijsinstelling)

   Deze tweedeling geeft de hoger onderwijsinstelling een handvat voor veiligheids- en crisismanagement, omdat het inzichtelijk maakt in hoeverre de instelling zelf invloed kan uitoefenen op het vóórkomen van het risico. Een risico dat het gevolg is van externe oorzaken, is minder te beïnvloeden dan een risico dat binnen de muren van de eigen onderwijsinstelling ontstaat.

b. Als tweede onderscheid kunnen risico's worden ingedeeld naar het effect dat ermee gepaard gaat: het kan gaan om een intern effect of om een extern effect.

   Bij een intern effect is de instelling primair probleemeigenaar en daarmee als eerste

verantwoordelijk voor de aanpak van de situatie. Bij een extern effect is de instelling waarschijnlijk niet de primaire probleemeigenaar. De aanpak van het probleem vergt in ieder geval samenspraak met externe partners (zoals de gemeente, politie, psychosociale dienst).



Met behulp van dit onderscheid kan ook bewust worden gekeken naar het effect van macro- en microtrends:

- Macrotrends zijn ontwikkelingen binnen de maatschappij die invloed hebben op aard en omvang van (bestaande) risico's. Macrotrends hebben derhalve met name een directe invloed op de risico's in het hoger onderwijs met een primair externe oorzaak.[16]
- Microtrends zijn ontwikkelingen binnen de instelling die invloed hebben op aard en omvang van risico's. Microtrends hebben derhalve vooral een direct effect op de risico's in het hoger onderwijs met een primair interne oorzaak.

[16] Zie bijvoorbeeld U. Rosenthal, 'Veiligheidsniveaus: over menselijke fouten, het systeem en nieuwe zondebokken' in 'Ramp en Recht', Boom Juridische Uitgevers, 2001.

Om voldoende inzicht te krijgen in de ontwikkeling van risico's binnen het hoger onderwijs en de instellingen voor wetenschappelijk onderzoek is een bewuste monitoring van macro- en microtrends noodzakelijk.

Macrotrends

De voor dit onderzoek relevante macrotrends zijn:

- De toenemende agressie en geweldpleging, vaak met vuurwapens, binnen de maatschappij en zelfs binnen middelbare scholen vraagt om bewuste overweging van de kans dat deze trend zich ook binnen het hoger onderwijs manifesteert.
- Bezuinigingen en efficiencyoperaties (al dan niet in het kader van privatisering en bevordering van marktwerking) romen veelal de redundantie in personeel en middelen af die mede zorg dragen voor risicopreventie. Ook binnen instellingen van het hoger onderwijs en wetenschappelijk onderzoek is dit zichtbaar.
- Ontwikkeling en toenemend gebruik van ICT verhoogt de afhankelijkheid hiervan. Instellingen zijn in toenemende mate kwetsbaar voor virussen, hackers, stroomuitval en ander elektronisch ongemak.
- 'Gedogen is uit'; regelgeving dient nageleefd te worden. Handhavingsarrangementen worden steeds vaker ontwikkeld, zowel op lokaal als nationaal niveau. Door de vuurwerkramp in Enschede en de cafébrand in Volendam zijn gemeenten zich bewust geworden van de noodzaak tot integrale handhaving van vergunningen en algemene verordeningen. De rijksoverheid heeft haar rijksinspecties fors uitgebreid. Deze trend leidt vanzelfsprekend primair tot een vermindering van allerhande risico's. Secundair echter vergroot deze trend de effecten van elk incident: blijkbaar was er immers sprake van onvoldoende controle, toezicht en/of handhaving. In vele van de incidenten van 2003 is deze reflex zichtbaar. Hoger onderwijsinstellingen hebben hier enerzijds als vergunningaanvrager mee te maken, maar daarnaast wordt ook van hen een visie op handhaving binnen de eigen instelling verwacht
- De multiculturalisering van de samenleving neemt toe. Deze multiculturalisering kan behalve als culturele verrijking ook gezien worden als een potentiële bron van spanning. Zo kan de spanning tussen bevolkingsgroepen met verschillende culturele achtergronden bijvoorbeeld door gebeurtenissen elders in de wereld soms oplopen.

Door rekening te houden met deze macrotrends kan de instelling pro-actief proberen actuele risico's te beperken. Zo speelde de Universiteit van Amsterdam vanuit de onderkenning van de macrotrend 'multiculturalisering' pro-actief in op de dreigende oorlog in Irak: een preventief opgeschaald Crisis Management Team beoordeelde de risico's op het gebied van sociale veiligheid die voortvloeiden uit de gespannen situatie.

Microtrends

Een microtrend beïnvloedt de kans dat een risico dat zich binnen de muren van een specifieke instelling manifesteert. De onderkenning van microtrends vergt bewuste inzet op risicobewustzijn, meldingsprocedures en analyse van incidenten.

Een belangrijke type microtrends wordt wel structureel incidentalisme genoemd: het regelmatig voorkomen van kleine incidenten van een specifiek type is vaak de voorbode van een ernstig incident van dat type. Een voorbeeld hiervan is het risico op brand. Wanneer binnen de schoolmuren in korte tijd na elkaar papierbakken in brand worden gestoken, is het van belang om dit te signaleren als een samenhangend patroon. Een toenemend aantal kleine brandstichtingen geeft immers een indicatie voor een toenemend risico op een toekomstige en mogelijk grotere brand.

Andere voorbeelden van microtrends binnen het hoger onderwijs en het wetenschappelijk onderzoek zijn: het aanbrengen van graffiti op bepaalde plaatsen is een indicatie voor beperkte sociale veiligheid op die locaties, het op verschillende plaatsen opduiken van racistische leuzen kan een indicatie zijn voor oplopende spanning binnen de instelling.

In de hoofdstukken 4 tot en met 6 wordt per risicodomein gedetailleerd op de verschillende relevante macrotrends en de bijbehorende risico-ontwikkeling ingegaan. Ook zullen daar voorbeelden van incidenten binnen instellingen worden gegeven waarvan achteraf kan worden geconstateerd dat de voorbodes zichtbaar waren.

2.4 Crises

Risico materialiseren zich als een incidenten. Veel van die incidenten worden al dan niet optimaal afgehandeld op veelal decentraal niveau binnen instellingen. Sommige incidenten ontwikkelen zich echter tot een crisis waarvan de beheersing alle mogelijke inspanning vergt.

Een crisis wordt hier gedefinieerd als een bedreiging van de basisstructuren (binnen het hoger onderwijs en het wetenschappelijk onderzoek) waarbij kritieke beslissingen noodzakelijk zijn die onder tijdsdruk en met onvolledige informatie genomen moeten worden.[17]
Voor de beheersing van incidenten en crises is het noodzakelijk om inzicht te hebben in de algemene crisistrends die onderscheiden worden in de literatuur. Dit inzicht helpt niet alleen bij het adequaat beheersen van een crisis, maar ook bij de afweging vooraf aan welke risico's meer aandacht moet worden besteed.

Politisering
Een crisis gaat tegenwoordig al snel over meer dan de crisis *an sich*. Het functioneren van het betreffende systeem en de betrokkenen zelf staat vrijwel meteen ter discussie. De roep om publieke verantwoording kan niet worden weerstaan. Onafhankelijk onderzoek is veelal bijna een eerste vereiste.

Mediatisering
De aandacht van de media voor crises is sterk toegenomen. Zij draagt in hoge mate bij aan de politisering van crises. De 'slag om de beeldvorming' is daarmee een belangrijke taak voor met name de betrokken bestuurders geworden. Belangrijk is het besef dat het begrip 'mediamanagement' op een illusie duidt, namelijk dat de media te sturen zijn. Het gaat veeleer om het 'verdienen' van het publiek vertrouwen, dan om het 'sturen' ervan.

[17] Dit is een specificatie van de algemene crisisdefinitie die het COT hanteert. Zie hiervoor bijvoorbeeld COT, 'Crisis; oorzaken, gevolgen en kansen', Leiden, 1998.

Mobilisering

De moderne burger is veel mondiger dan voorheen. Hij mobiliseert medeslachtoffers, media en justitie in zijn poging 'recht' gedaan te krijgen. Geen crisis zonder belangen- of actiegroep. Binnen het hoger onderwijs is de zich mobiliserende student natuurlijk als sinds de jaren zestig van de vorige eeuw een bekend gegeven.

Juridisering

Met de voorgaande trend hangt direct de toenemende juridisering van crises samen. In de eerste plaats is een toenemend strafrechterlijk activisme zichtbaar: aan het strafrecht wordt door betrokkenen een hoog waarheidsvindend en vergeldend vermogen toegedicht. Meer dan vroeger wordt er daarom strafrechterlijk vooronderzoek ingezet en komt men tot strafrechterlijke vervolging.

De 'veramerikanisering van de maatschappij' is een tweede begrip dat veel omvat. Men doelt hiermee vooral op de toenemende aansprakelijkheidstelling door betrokkenen van de veroorzakers van crises. De nasleep van de vuurwerkramp en de cafébrand laten zien dat ook falend handelen op preventiegebied door (overheids)instanties reden is om die instanties daarvoor aansprakelijk te stellen.

Direct verbonden met de toenemende aansprakelijkheidsstelling is het belang dat aan normstelling wordt toegedicht als blijkt van professionaliteit. Ontoereikende normstelling in de preventieve en preparatieve fase is (steeds meer) een grond voor privaatrechterlijke aansprakelijkheidstelling. Anderzijds kan uitgebreide normstelling leiden tot een defensieve bureaucratie die de effectiviteit van preventie en preparatie juist belemmert.[18]

Complexificering

Bij crisis blijken steeds meer actoren een eigen rol, verantwoordelijkheid en bevoegdheid te hebben of op te eisen. De voorgaande trends betekenen voor betrokken actoren dat zij een crisis niet zomaar kunnen laten 'lopen'. Crisismanagement betekent daarmee steeds meer het betrekken van de juiste spelers in het complexe netwerk van betrokkenen. In de voorbereiding

[18] C.J.J.M. Stolker e.a. 'Defensieve bureaucratie? Rampen, de overheid en de preventieve rol van het aansprakelijkheidsrecht' in: 'Ramp en recht', red E.M. Muller en C.J.J.M. Stolker, Boom Juridische uitgevers, 2001

is daarom kennis van dit netwerk noodzakelijk en de competenties hoe in dit netwerk te opereren.

Internationalisering

Een bijzondere vorm van complexificering is de internationalisering van crises. Ook in het hoger onderwijs en het wetenschappelijk onderzoek wordt de internationale component steeds sterker. Studenten komen van over de hele wereld naar elke universiteit, onderzoeksprojecten worden steeds meer in internationaal verband uitgevoerd. Daarmee is ook de kwetsbaarheid voor (internationale) imagoschade toegenomen.

HOOFDSTUK 3
VEILIGHEIDS- EN CRISISMANAGEMENT

3.1 Inleiding

Overzicht over de risico's die instellingen binnen het hoger onderwijs en het wetenschappelijk onderzoek kennen, geeft het noodzakelijke inzicht in en duidelijkheid over kwetsbaarheden. Evenzo is een inzicht in crisistrends nodig om het ontstaan van crises tijdig te kunnen onderkennen. Inzicht en overzicht zijn echter niet voldoende voor het effectief voorkomen en beheersen van risico's. Een consequente, consistente en integrale inzet op veiligheids- en crisismanagement is daarvoor noodzakelijk.

Meer en meer ontdekken organisaties in het bedrijfsleven en binnen de overheid dat een veiligheidsbeleid een even normaal onderdeel dient te zijn van het gehele organisatiebeleid als bijvoorbeeld pr- of arbobeleid. Voorbereiding op crisisbeheersing is daarmee een soort gelijke investering als die op andere beleidsterreinen.

Dat consequente aandacht voor inzicht in en voorbereiding op kwetsbaarheden van groot belang is voor continuïteit van bedrijfsvoering, blijkt bijvoorbeeld uit recent onderzoek van Les Coleman dat gepubliceerd is in het Journal of Contingencies and Crisismanagement[19]. Coleman bestudeerde de gevolgen van crisis van verschillende oorsprong in het Australische bedrijfsleven. Meer dan een kwart van de door crises getroffen (internationale) bedrijven overleefde de crises niet. Veel van deze crises ontstonden of verergerden door afwezig veiligheidsbeleid of onvoldoende voorbereiding op crisismanagement.

Het doel van het veiligheidsbeleid van een organisatie is om zoveel mogelijk risico's te reduceren door het nemen van adequate maatregelen. Daarmee kan het totale risico nooit worden weggenomen, er zijn immers realistische grenzen aan de mogelijke en gewenste investeringen in veiligheid. Er blijven daarmee onvermijdelijk risico's aanwezig. Een goed

[19] L. Coleman, 'Costs of corporate crisis', Journal of Contingencies en Crisis Management, volume 1, 2004.

ingerichte crisismanagementorganisatie dient ertoe om manifesterende risico's te kunnen beheersen.

Dit hoofdstuk geeft in de eerste plaats een conceptueel kader voor een samenhangend beleid gericht op veiligheids- en crisismanagement (de 'veiligheidsketen'). Vervolgens wordt ingegaan op aspecten van veiligheidsmanagement. Daarna zal aandacht worden besteed aan crisismanagement.

3.2 De veiligheidsketen

De veiligheidsketen is een in de praktijk beproefde systematiek om veiligheids- en crisismanagement te structureren. Deze door de Amerikaanse Federal Emergency Management Agency ontwikkelde structuur is in de jaren negentig in Nederland door het ministerie van Binnenlandse Zaken en Koninkrijkdsrelaties geïntroduceerd.[20] De keten bestrijkt de volle cirkel die gerelateerd is aan veiligheids- en crisismanagement: van voorkomen via voorbereiden en daadwerkelijke respons tot herstelwerkzaamheden en nazorg.

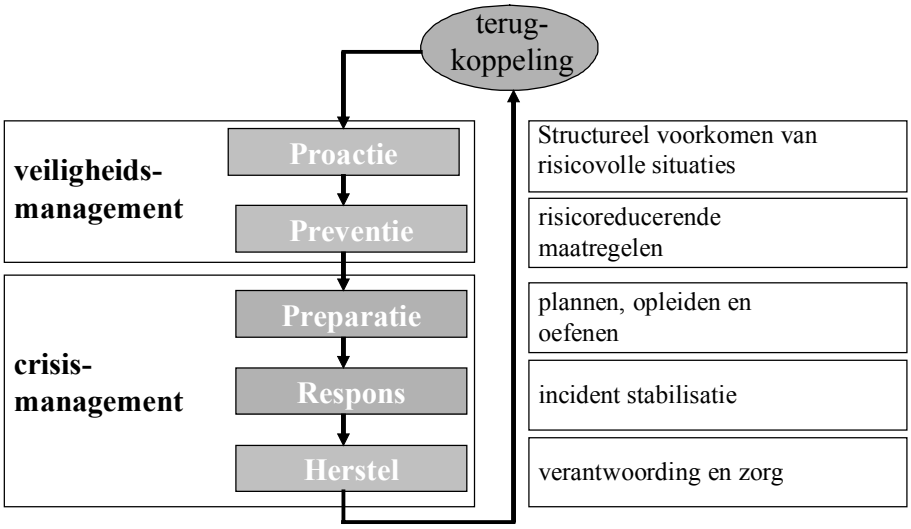
De veiligheidsketen bestaat uit de schakels pro-actie, preventie, preparatie, respons en herstel[21].

Puntsgewijs betekenen de onderdelen van de veiligheidsketen:

- Pro-actie kan gedefinieerd worden als het wegnemen van structurele oorzaken van incidenten ter voorkoming van het ontstaan ervan.
- Preventie kan gedefinieerd worden als het nemen van maatregelen vooraf ter voorkoming van het ontstaan van incidenten en beperken van de gevolgen indien zij zich toch voordoen. Te denken valt aan wettelijke kaders, voorlichting en toezicht.
- Preparatie omvat al datgene dat moet worden voorbereid om incidenten te kunnen bestrijden. In dit verband moet men denken aan het opstellen van plannen en procedures, het opleiden van personeel, etc.

[20] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Integrale Veiligheidsrapportage 1993; 15

- Respons is de daadwerkelijke bestrijding van incidenten gericht op stabilisering van de gevolgen van het incident.
- Herstel omvat al hetgeen nodig is om zo snel mogelijk de gevolgen te beperken en in de 'normale' situatie en verhoudingen terug te keren. Hieronder valt continuering van de zorg, verantwoording afleggen en evaluatie ter verbetering van het veiligheids- en crisismanagement.



Figuur: Veiligheidsketen

Uit de definities hierboven wordt meteen al duidelijk dat er sprake is van een zekere overlap tussen pro-actie en preventie evenals tussen respons en herstel.

3.3 Veiligheidsmanagement

In de veiligheidsketen wordt onderscheid gemaakt tussen pro-actie (het structureel voorkomen van risico's) en preventie (het beperken van risico's).

[21] Klassiek wordt de herstelfase wel als nazorgfase betiteld. Dit geeft echter de onjuiste indruk dat de crisis al beheerst is en 'slechts' enige nazorg benodigd is.

3.3.1 Pro-actie

Gezien de dominantie van de anticipatiestrategie (zie hoofdstuk 2) binnen onze maatschappij is het niet verrassend dat in veel beleidsstukken die aan veiligheidsproblematiek raken als voornemen wordt vermeld dat organisaties het accent moeten leggen op de pro-actieve en preventieve kant van de veiligheidsketen. Hoe 'Pro-actiever' hoe beter, lijkt daarbij het devies.

Pro-actie - in de context van het hoger onderwijs en het wetenschappelijk onderzoek - betekent in de praktijk met name de (beleidsmatige) overweging of risicovolle activiteiten wel binnen de instelling op een bepaalde plaats of tijd ondernomen moeten worden: bepaalde experimenten kunnen zo risicovol zijn dat besloten moet worden deze (nog) maar niet uit voeren binnen de instelling. Het risico kan dan fysiek zijn (giftigheid, explosiviteit, besmettelijkheid, etc), maar evengoed betrekking hebben op imagoschade of voorzienbare protestacties (zoals bij experimenten met genetisch gemodificeerde organismen).

Een essentieel kenmerk van pro-actie is dat het gedachten over de toekomst van activiteiten betreft. Dergelijke gedachten zijn aan weinig regelgeving gebonden. Daarmee kan voor sturing ervan bijvoorbeeld veelal weinig beroep worden gedaan op een wettelijk kader. Een ander kenmerk van structurele veiligheidsplanning is dat er beleidsconcurrentie plaatsvindt met andere beleidsterreinen als economie, ICT, transport, facilitaire zaken, huisvesting, etc. Beïnvloeding vergt dan onderkenning van het krachtenveld en gericht procesmanagement.

Voor instellingen betekenen beide aspecten van pro-actie dat de inzet en het ingezet personeel om essentieel andere kernkwalificaties vragen dan de inzet en het ingezette personeel voor de meer uitvoerende taken op het gebied van 'preventie', 'preparatie' of 'respons. Structurele veiligheidsplanning is niet een taak die 'erbij' kan worden genomen. Pro-actie vraagt om specifiek beleid en personeel met de juiste kwalificaties. Bestuurlijke betrokkenheid is een eerste vereiste.

3.3.2 Preventie

De preventieschakel kent een aantal klassieke activiteiten: uitvoering van (wettelijke) voorschriften, voorlichting en toezicht.

Uitvoering van (wettelijke) voorschriften

In tegenstelling tot pro-actie zijn veel preventieactiviteiten gebaseerd op een bestaande (wettelijke) normen. De meest bekende wettelijke regelingen die preventieve eisen met zich meebrengen zijn:

- Woningwet/ Bouwbesluit (brandveilig bouwen)
- Gemeentelijke bouwverordening (brandveilig gebruik van bouwwerken)
- Wet milieubeheer (zorg voor milieuaspecten)
- Arbeidsomstandighedenwet (zorg voor veilige en gezonde arbeidsomstandigheden).

Deze wettelijke gronden behoren de basis te zijn voor preventieve beleidsuitgangspunten binnen onderwijs- en onderzoeksinstellingen.

Voor instellingen geldt daarnaast dat zij zelf de mogelijkheid en verantwoordelijkheid hebben om preventief beleid en preventieve regels vast te stellen voor activiteiten binnen de instellingen zelf. Op veel gebieden gebeurt dit welhaast als vanzelfsprekend, maar gedragsregels in brede zin blijven toch nog (te) vaak impliciet. Een belangrijk voorbeeld is het gebruik van ‘overeenkomsten’ tussen instelling en studenten/medewerkers voor computergebruik.

Voorlichting

Voorlichting is een van drie aspecten die onderdeel uitmaakt van de klassieke preventieschakel vormen. Het belang dat aan voorlichting wordt gehecht en de plaats die het inneemt in het preventiebeleid hangt sterk af van het betrokken beleidsterrein. Op het gebied van bijvoorbeeld klassieke volksgezondheid (zoals SOA’s) en van inbraakpreventie bestaat een sterke traditie van voorlichting. Op het beleidsterrein van de fysieke veiligheid, zoals brand, is die traditie nog beperkt, maar wel in ontwikkeling met projecten als de Brandpreventieweek en de activiteiten van de Brandwondenstichting en

Stichting Consument en Veiligheid.

Ook vanuit het oogpunt van toezicht is voorlichting van belang. Zo is in een beoordelingskader dat door de toenmalige Inspectie Rechtshandhaving is ontwikkeld (de T11-methodiek) voorlichting expliciet een van de elf onderscheiden dimensies die de handhaafbaarheid van regels bepalen.[22]

Dat er geen noodzakelijk verband zit tussen het belang dat aan voorlichting wordt gehecht en de daadwerkelijke plaats die het heeft in het staand preventiebeleid wees bijvoorbeeld de quick-scan brandveiligheid uit die door de commissie Alders na de cafébrand in Volendam werd uitgevoerd[23] uit: voorlichting op het gebied van brandveiligheid werd door vele betrokkenen als belangrijk ingeschat, maar in de praktijk kwam voorlichting toch op een laatste budgettaire plaats.

Toezicht

Een derde aspect van preventie is toezicht. Met toezicht wordt hier gedoeld op 'het verzamelen van informatie over de vraag of een handeling of zaak voldoet aan de daaraan gestelde eisen, het zich daarna vormen van een oordeel daarover en het eventueel naar aanleiding daarvan interveniëren' (definitie uit het Eindrapport Ambtelijke Commissie Toezicht, Ministerie van Justitie, 2001).

Instellingen ondergaan toezicht op de naleving van wettelijke regelingen door verschillende toezichthouders als gemeentelijke diensten, de Arbeidsinspectie en de VROM-inspectie. Instellingen dienen zelf toezicht uit te voeren op de naleving van eigen voorschriften.

Een bijzondere vorm van toezicht is het organiseren van de vroegtijdige signalering van dreigingen. Een kritische succesfactor in het voorkomen van incidenten en crises is de vroegtijdige herkenning en melding van signalen die kunnen wijzen op een dreigende crisis. In dit kader spreekt men ook wel van *early warning*. Een definitie van *early warning* volgens

[22] Expertisecentrum Rechtshandhaving, Ministerie van Justitite, De Tafel van Elf, beknopte toets voor de handhaafbaarheid van regels, 2002

[23] NIBRA, Vergunningverlening, controle en handhaving brandveiligheid; eindrapportage van de quickscan, 2001

Cuny[24] is: 'The indentification, interpretation and recognition of events that indicate a potential emergency'. Het doel hiervan is het creëren van informatie voor actie; het leidt tot maatregelen die gepercipieerde dreigingen moeten voorkomen of beperken. Aan de meeste rampen (zo niet alle rampen) gaan signalen vooraf die potentieel gevaar aanduiden. Het is de kunst om dergelijke signalen te herkennen en ervoor te zorgen dat de juiste personen tijdige worden geïnformeerd, zodat na een risicoanalyse eventueel maatregelen kunnen worden genomen om te dreiging te voorkomen of de gevolgen te beperken. Het middel vroegtijdige signalering vindt in vele instituties en beleidsvelden toepassing, zoals in het leger, binnen de infectieziektebestrijding, maar ook bij (grotere) bedrijven.

Uit de enquête die ten behoeve van dit onderzoek is gehouden onder alle instellingen binnen het hoger onderwijs komt het volgende beeld naar voren over het huidige veiligheidsbeleid binnen het hoger onderwijs (voor een volledige weergave van de enquêteresultaten zie bijlage IV):

- De meeste instellingen kennen beleidsuitgangspunten op het gebied van organisatieveiligheid. Daarentegen kent vrijwel geen instelling beleid gericht op sociale veiligheid of kennisveiligheid. Aspecten van organisatieveiligheid komen bij de meerderheid van de instellingen dan ook als enige met regelmaat aan de orde in bestuursvergaderingen. Op langere termijn verwacht een meerderheid echter veiligheidsbeleid en meer benodigde middelen daarvoor.
- De klassieke RI&E uitgevoerd door de arbodiensten is bij het overgrote deel van de instellingen de enige vorm van kwetsbaarheidanalyse waarover aan het bestuur wordt gerapporteerd. Er blijkt bij doorvragen echter een breed scala aan risico's te worden onderkend. Slechts een minderheid van de hogescholen ziet geen grote veiligheidsrisico's.
- Personeel en studenten worden bij een minderheid van de instellingen betrokken bij het opstellen van veiligheidsbeleid.

3.4. Crisismanagement

Crisismanagement correspondeert zoals al aangegeven, met de volgende aspecten van de veiligheidsketen: preparatie, respons en herstel.

[24] Cuny, F.C., Disasters and Development. Oxford University Press, New York, 1983

Een crisismanagementorganisatie zal voor deze schakels in de keten in staat moeten zijn om adequaat te kunnen optreden om de negatieve gevolgen van een incident zoveel al mogelijk te reduceren.

3.4.1 Preparatie op de respons

Bij de voorbereiding op crises kan onderscheid gemaakt tussen de wettelijk verplichte voorbereiding gericht op de veiligheid van aanwezigen en de bovenwettelijke voorbereiding gericht op de continuïteit van bedrijfsvoering van de instelling.

De wettelijke verplichte BHV-organisatie gericht op veiligheid aanwezigen

Instellingen hebben een wettelijke verplichting zich op 'normale' bedrijfsongevallen voor te bereiden. De Arbeidsomstandighedenwet geeft aan dat instellingen een verantwoordelijkheid hebben om bij bedrijfsongevallen, zoals tenminste brand, de veiligheid van eigen personeel en derden te waarborgen. Elk bedrijf moet daatoe een bedrijfshulpverleningsorganisatie bezitten die naar behoren 'bijstand' kan verlenen bij een ongeval. Onder het verlenen van 'bijstand' valt:

- het verlenen van eerste hulp bij ongevallen
- het beperken en bestrijden van brand en het voorkomen en beperken van ongevallen
- het in noodsituaties alarmeren en evacueren van alle werknemers en andere personen
- het alarmeren van en samenwerken met hulpverleningsorganisaties waar het bovenstaande 'bijstand' betreft.

In het verplichte bedrijfsnoodplan wordt de bedrijfshulpverleningsorganisatie en de wijze waarop zij hulp verleent, beschreven. Het bedrijfsnoodplan moet onder meer voldoen aan de volgende vereisten.

- Ten eerste moeten alle bouwkundige voorzieningen (o.a. vluchtwegen, toegangen), technische voorzieningen (o.a. omroep- en ontruimingsinstallatie, verlichting, verwarming, liften) en brandblusvoorzieningen in het bedrijf in termen van functie, locatie, en capaciteit beschreven staan.
- Verder moet uit het noodplan blijken wat de capaciteit en organisatiestructuur van de bedrijfshulpverlening is.

- Daarnaast moet het bedrijfsnoodplan een calamiteitenplan (dat wil zeggen een draaiboek voor noodsituaties) bevatten. Essentieel onderdeel van dit calamiteitenplan is een alarmeringsschema. Het is van belang dat het calamiteitenplan in samenspraak met de overheid is opgesteld en beoefend. Het spreekt voor zich dat het bedrijfsnoodplan geïntegreerd moet zijn met het aanvalsplan/rampenbestrijdingsplan voor de instelling, als dat is vastgesteld door de overheid.

Voorbereiding op integraal crisismanagement

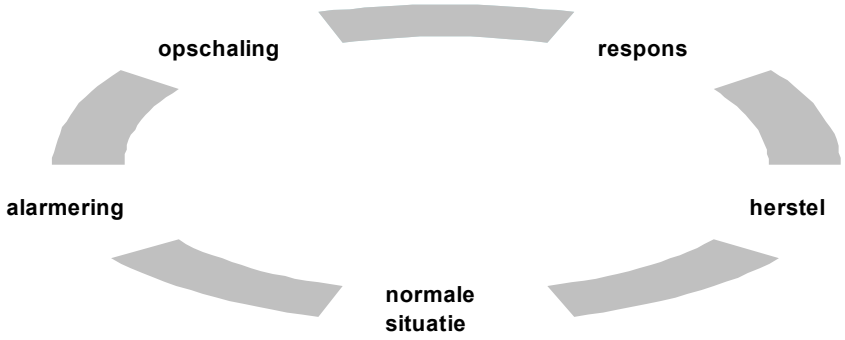
Integraal crisismanagement vergt beleid, planning, opleiding, oefening en toetsing.

Het *beleid* ten aanzien van het crisismanagement ligt vast in basisdocumenten waarin is tenminste aandacht is voor:

- De doelstellingen van crisisbeheersing; bijvoorbeeld als een beschrijving van risico's waarvan de effecten beheerst moeten worden en risico's waarvan geen of beperkte beheersing van de effecten geaccepteerd wordt.
- Het gealloceerde budget voor de voorbereiding op crisismanagement.
- De continue verbetering van de voorbereiding op crisisbeheersing door middel van evaluatie en rapportage.

In *crisisplanning* wordt onder andere aan de volgende aspecten aandacht besteed:

- alarmering
- opschaling
- middelen, taken en bevoegdheden voor de crisisbeheersingsorganisatie
- coördinatiemechanismen
- een beschrijving van netwerkpartners en hun taken bij crisismanagement.



Figuur: Levensloop van een crisis

Opleiding en oefening is noodzakelijk om de leden van de crisismanagementorganisatie op hun taak voor te bereiden.

Voor instellingen binnen het hoger onderwijs is het van belang om te onderkennen dat studenten ook een vorm van instructie moeten ontvangen over het handelen in noodsituaties.

Toetsing van de crisismanagementorganisatie dient om inzicht te krijgen in het functioneren van de crisismanagementorganisatie (en op die wijze tot verdere verbetering te komen) en om het kunnen afleggen van verantwoording over de bestede middelen.

3.4.2 Respons

Wanneer een risico zich materialiseert, blijkt in de responsfase de waarde van alle voorbereidingen. De gevolgen van het incident moeten zodanig beheerst worden dat er weer van een stabiele situatie kan worden gesproken.

In de responsfase dient er bij de besluitvorming continue aandacht te zijn voor de volgende drie aspecten:

- *Proces.* Crisisbesluitvorming vraagt, feitelijk als elk besluitvormingsproces, om bewuste aandacht voor tijdigheid en kwaliteit van informatievoorziening naar de besluitvormers, bewaking van de inbreng van alle betrokkenen, tijdigheid van besluitvorming en controle op de uitvoering van beslissingen.
- *Inhoud.* Om een crisissituatie te ‘beheersen’ is het evenzeer noodzakelijk in de

crisisorganisatie te beschikking over voldoende inhoudelijke deskundigheid. Dat kan door hen in het coördinerende crisisteam een rol te geven. Deze deskundigheid kan liggen in expertise, maar ook in lijnverantwoordelijkheid voor een bepaalde sector binnen de organisatie.

- *Communicatie.* Communicatie intern richting de eigen organisatie (personeel en studenten) is even belangrijk als externe communicatie naar pers, publiek en netwerkpartners. Beeldvorming is een belangrijke factor in de bepaling van de effectiviteit van besluiten en maatregelen.

In de responsfase gaat het niet altijd om het met krachtige maatregelen beheersen van een al exploderende crisis. Wanneer microtrends en andere 'early warning' signalen tijdig genoeg worden onderkend, kunnen in de responsfase soms subtiele maatregelen genoeg zijn om een crisis in wording te smoren.

> De politie in New York had zich in de jaren negentig van de vorige eeuw tot doel gesteld om de metro veilig te maken. Metrostations waren inmiddels een bijna onbegaanbaar terrein geworden. De politie koos voor een onorthodoxe methode. Er werd geen grote politiemacht op de stations en in de metrostellen ingezet om de criminaliteit de kop in te drukken, maar men koos voor twee andere bestrijdingswijzen. Op de eerste plaats werd graffiti structureel van de treinstellen verwijderd. Op de tweede plaats werd zwartrijden hard aangepakt. De achterliggende filosofie was dat graffiti en zwartrijden symbolen van normoverschrijdend gedrag waren. Het aanpakken van deze 'randverschijnselen' leidde tot succes. Graffitispuiters stopten met hun acties, omdat het zinloos was als elke trein die zij onder handen namen direct werd schoongemaakt. Het gevolg van de gecombineerde aanpak was een sterke afname van de criminaliteit in de metro en een corresponderende toename van de veiligheidsbeleving.[25]

3.4.3 Herstelfase

De zinsnede 'de ramp na de ramp' of 'crisis na de crisis' heeft vooral betekenis gekregen in relatie tot de aanzwellende mediakritiek die de speurtocht naar schuldigen of suboptimaal handelen tijdens de bestrijding vergezelt. Feit is dat de hoeveelheid activiteiten die noodzakelijk zijn voordat men vanuit de gestabiliseerde toestand weer terug bij normaal is,

[25] Zie: '*The Tipping Point',* Malcom Gladwell, 2002, hoofdstuk 4

veel groter is dan de activiteiten die nodig zijn om de toestand te stabiliseren. Feit is ook dat handelingen in de herstelfase de beeldvorming over de bestrijding van de crisis en meer in het bijzonder de prestatie van de verantwoordelijken zwaar kunnen beïnvloeden.

De les die uit de casuïstiek kan worden getrokken is dat het waardevol is de activiteiten in de herstelfase projectmatig te organiseren. De zin van het bewust aanbrengen van onderstaande driedeling is dat ongelijksoortige activiteiten elkaar niet verstoren. Projectverantwoordelijken voor elk van de drie aspecten hebben daarmee geen conflicterende doelstellingen. Alledrie de deelprojecten hebben behoefte aan specifieke specialistische ondersteuning die de beschikbare capaciteit 'in huis' meestal te boven gaat.

In deze paragraaf hanteren we een driedeling van de activiteiten in de herstelfase:

- publieke verantwoording
- de daadwerkelijke herstelactiviteiten
- juridisch verhaal door derden of op derden.

Publieke verantwoording

Zodra de eerste acute fase van de rampenbestrijding is afgelopen zal de aandacht van bevolking en media sterk gericht zijn op de schuldvraag. Recente crisis laten zien dat de druk van bevolking en media zo groot is dat die niet kan worden genegeerd. Wie bijvoorbeeld te snel de eigen onschuld proclameert, krijgt voorspelbaar te maken met het vergrootglas van de media. Evenals in de responsfase kan de effectiviteit van activiteiten gericht op herstel ernstig beperkt worden door negatieve beeldvorming.

Een eerste stap in het afleggen van publieke verantwoording is veelal het laten verrichten van een onafhankelijk extern onderzoek. Een langzamerhand gangbare wijze om op onafhankelijke wijze externe deskundigen aan te sturen, is door middel van een constructie waarbij een onafhankelijke begeleidingscommissie onder voorzitterschap van een bestuurlijk zwaargewicht het mandaat krijgt om de betrokken externen aan te sturen.

Crisiscommunicatie-experts wijzen allen op het belang van transparantie, eerlijkheid en

snelheid in het proces van publieke verantwoording. Een eenmaal ontstaan negatief beeld bij media en publiek leidt al snel tot noodgedwongen defensieve reacties waardoor een negatieve spiraal kan ontstaan die lastig is te doorbreken.

De daadwerkelijke herstelactiviteiten

Onder de daadwerkelijke herstelactiviteiten valt het geheel aan feitelijke herstelwerkzaamheden dat varieert van zorg voor slachtoffers (als die er zijn) tot het fysieke herstel van schade.

Juridisch schadeverhaal door derden en op derden

Recente crises laten nadrukkelijk zien dat de eerder genoemde crisistrend 'juridisering' sterk doorzet. Daarbij kan onderscheid gemaakt worden tussen twee typen van juridisch verhaal:
de eerste type is strafrechterlijke en civiele aansprakelijkheidstelling van de instelling en haar personeel
het tweede type is het verhaal dat de instelling zelf zou willen halen bij derden voor de kosten van hulpverlening.

Beide vormen van juridisch verhaal vragen om bewuste overweging van de betekenis van besluiten vanuit juridisch perspectief. Daarvoor is juridische bijstand bij voorkeur snel beschikbaar.

Binnen het hoger onderwijs wordt de verdergaande juridisering ook gevoeld. Verschillende instellingen spraken in dit verband bijvoorbeeld hun zorg uit voor aansprakelijkheidsstelling bij RSI-klachten van studenten. Aantoonbaar preventief beleid ter voorkoming ervan moet in de visie van deze instellingen invulling geven aan hun verantwoordelijkheid voor de gezondheid van studenten en daarmee de kans op succesvolle aansprakelijkheidstelling verminderen.

Uit de enquête die ten behoeve van dit onderzoek is gehouden onder alle instellingen binnen het hoger onderwijs komt het volgende beeld naar voren over de huidige beleidsmatige voorbereiding op crisismanagement binnen het hoger onderwijs (voor een overzicht van de enquêteresultaten zie bijlage IV):

- De meeste instellingen geven aan planvorming te hebben voorbereid voor crisismanagement. Dit gaat dan in het overgrote deel om BHV-plannen. Slechts een minderheid geeft aan ook planvorming voor coördinatie van het crisismanagement te hebben. Planvorming voor bijvoorbeeld crisiscommunicatie is niet aangetroffen. Evenzo wordt bij de overgrote meerderheid van de instellingen alleen op BHV en ontruiming geoefend.

HOOFDSTUK 4
HOGER ONDERWIJS ALS SPIEGEL VAN DE MAATSCHAPPIJ

4.1 Inleiding

De instellingen binnen het hoger onderwijs en wetenschappelijk onderzoek willen een omgeving bieden, waar studenten en medewerkers op plezierige en veilige wijze kunnen studeren en werken. Zoals vele andere instellingen met een publieke functie worden ook de onderwijsinstellingen geconfronteerd met normoverschrijdend gedrag. Op vele manieren kan dit gedrag leiden tot vormen van sociale onveiligheid binnen de instelling.

> Het ministerie stelt 'Op een veilige school voelen leerlingen zich thuis. Ze komen graag naar school en voelen zich serieus genomen door de leraren. [.] De school tolereert geen discriminatie en seksuele intimidatie. [.] Ook werken scholen vaak samen met politie, justitie en jeugdzorg. De school gaat bestaand sociaal onveilig gedrag tegen, maar voorkomt dat gedrag ook door een actieve, positieve stimulering van sociaal gedrag.' [26] Mutatis mutandis geldt ditzelfde ook voor instellingen in het hoger onderwijs.

Dit hoofdstuk gaat in op de risico's die in hoofdstuk 2 zijn genoemd onder de noemer van *'het hoger onderwijs als spiegel van de maatschappij'*. Deze risico's worden in dit hoofdstuk onderverdeeld naar primair intern en primair extern effect. Aan de hand van de methodiek van de veiligheidsketen zal worden ingegaan op de mogelijkheden die de onderwijsinstellingen hebben om risico's en incidenten op het gebied van de sociale veiligheid te beheersen. In het hoofdstuk zullen verder ervaringen van instellingen binnen het hoger onderwijsinstellingen worden gepresenteerd.

Hieronder zullen als eerste enkele algemene conclusies vanuit de enquête en interviews worden gepresenteerd.

Huidige stand van zaken

De mate waarin het aspect sociale veiligheid leeft, verschilt sterk van instelling tot instelling. Het merendeel van de instellingen geeft aan dat de aandacht voor sociale veiligheid is toegenomen. Toch ziet de helft van de instellingen geen grote risico's op sociaal vlak die het nodig maken om nieuwe initiatieven op dit vlak te ondernemen. De andere helft van de instellingen geeft daarentegen aan dat het vraagstuk van de sociale veiligheid binnen hun instelling een hoge of de hoogste prioriteit heeft. Deze groep bestaat vooral uit universiteiten die zich in de grote steden bevinden. Deze instellingen nemen wel de nodige initiatieven om risico's op het gebied van sociale veiligheid te verkleinen.

Risicoperceptie instellingen en ontwikkelingen

Uit de respons van de enquête blijkt dat veel risico's op het gebied van sociale veiligheid niet of nauwelijks door de instellingen worden gevoeld. Alleen de bekende risico's zoals diefstal, seksuele intimidatie en geweldpleging worden als risico's ervaren. Slechts een enkele instelling ervaart meer diffuse dreigingen als extremisme of terrorisme ook als risico, waartegen in meer of mindere mate maatregelen moeten worden genomen.

Instellingen is gevraagd naar de gepercipieerde ontwikkelingen op sociaal veiligheidsgebied. Genoemd wordt in dat verband de een meer intensieve samenwerking tussen universiteiten en hogescholen gericht op een integrale aanpak van veiligheidsvraagstukken. In het algemeen wordt onderkend dat vanwege maatschappelijke ontwikkelingen het belang van een adequaat veiligheidsbeleid toeneemt. Zo wordt er gesproken over een omslag in het denken over veiligheid; van *loss control* naar de zorg voor een veilige omgeving. Onderdeel van die omslag is het benadrukken van de juiste waarden en normen die de kaders van de sociale omgang binnen de organisatie bepalen. Dit is noodzakelijk juist omdat schaalvergroting en efficiëntieoperaties tot een afnemende sociale controle leiden.

[26] 'Dossier veilige school' op www.minocw.nl

Melden en registreren van incidenten

Vrijwel elke instelling meldt incidenten centraal bij het bestuur[27], een klachtencommissie of bij de beveiliging. De meeste instellingen hebben procedures voor melding door bijvoorbeeld te werken met klachtenformulieren. De rapportagefrequentie varieert per instelling van dagelijks tot jaarlijks. Bepaalde instellingen melden alleen zeer ernstige incidenten bij de politie.

Risicoscan

In de helft van de gevallen maakt sociale veiligheid onderdeel uit van de risico-inventarisaties die de instelling. Ongeveer een kwart van de respondenten geeft aan niets op dit gebied te doen. Verreweg de meeste instellingen geven aan geen concrete plannen te hebben gemaakt om de sociale veiligheid te bevorderen.

Het betrekken van interne en externe partijen

Meer dan de helft van de instellingen zegt opmerkingen en suggesties op het gebied van het sociale veiligheidsbeleid door werknemers te stimuleren. In veel van deze instellingen wordt de medewerker – al dan niet actief - op de hoogte gehouden van (wijzigingen in) het veiligheidsbeleid. Dit gebeurt door persoonlijk contact, folders, de website, publicaties in werknemerskranten en het versturen van e-mails. Sommige instellingen trainen hun medewerkers op omgang met “lastige personen” of geven assertiviteitstrainingen.

Op het gebied van sociale veiligheid worden weinig initiatieven ontplooid richting studenten. Incidenten zijn vaak wel een aanleiding om op ad hoc basis voorlichtingsinitiatieven richting studenten te starten. Een beperkt aantal instellingen reikt folders uit waarin wordt gewezen op de gehanteerde klachtenprocedure en de aanwezigheid van vertrouwenspersonen. Slechts een enkele instelling betrekt de studenten actief bij het vormgeven van veiligheidsbeleid.

Het overleg met relevante externe partijen (zoals de politie) is nog beperkt. Verschillende instellingen hebben juist met de samenwerking met de politie minder goede ervaringen vanwege formele belemmeringen. Een enkele andere instelling heeft daarentegen juist de

[27] Op het merendeel van de universiteiten en hogescholen wordt het bestuur aangeduid als ´College van Bestuur (CvB)´. In het vervolg van dit rapport zal naar het bestuur worden verwezen als ´CvB´.

laatste jaren door intensieve samenwerking met de politie een slag kunnen maken op het gebied van de sociale veiligheid.

4.2 Sociale risico's met een primair intern effect

In deze paragraaf worden de sociale risico's met een primair intern effect beschouwd zoals die in het onderzoek naar boven zijn gekomen.

Diefstal
Uit de ingevulde vragenlijsten blijkt dat diefstal een van de meest frequent voorkomende type incidenten is.

Veel instellingen geven aan last te hebben van niet met de instelling verbonden personen die diefstal of inbraak plegen. De instellingen onderkennen dat zij over het algemeen zeer toegankelijk zijn en daarmee een aantrekkelijk doel zijn voor dit soort kwaadwillenden. Instellingen hebben in het algemeen geen beeld van het percentage van de diefstallen dat door eigen personeel of studenten wordt gepleegd. Een veiligheidsmanager van een universiteit schat echter dat 75% van de diefstallen door studenten of medewerkers wordt gepleegd (de zogenaamde gelegenheidsdieven).

> Twee onbekende figuren kwamen bij een universiteit binnen en deden zich voor als medewerkers van een technisch bedrijf. Op hun verzoek hielpen twee medewerkers mee om twee televisietoestellen naar de auto te brengen. Pas later bleek dat de mannen dieven waren.

Werknemers worden zelden gescreend, ook niet als zij in een beheersmatige functie toegang hebben tot nagenoeg alle faciliteiten van de instelling. Ook elementaire screening als het opvragen van een bewijs van goed gedrag of het opnemen van contact op met vorige werkgevers is niet standaard. Bevraagde beveiligingsmedewerkers zijn van mening dat het aangekondigde gebruik van een dergelijke screeningselementen een zekere filterende werking

met zich meebrengen; iemand die kwaad wil, zal minder snel solliciteren op een functie waarbij een bewijs van goed gedrag moet worden overlegd.

Bij constatering dat een persoon diefstal pleegt, is het beleid in veel gevallen om de politie in te schakelen. In ernstige gevallen wordt ook het College van Bestuur op de hoogte gebracht. Van een aanzienlijk deel van de geconstateerde diefstallen wordt echter geen aangifte gedaan. Apparatuur wordt dan bijvoorbeeld als defect opgegeven. Hierbij wordt als deelverklaring gewezen op schaamte bij medewerkers door het besef dat zij de diefstal door naïviteit of gebrek aan toezicht min of meer mogelijk hebben gemaakt.

(Seksuele) intimidatie en geweld

Uit een onderzoek van de Open Universiteit blijkt dat (seksuele) intimidatie niet alleen op het lager- en middelbaar onderwijs voorkomt. Uit enquêtes bij een tweetal hogescholen bleek 16% van de studenten in de eigen perceptie wel eens 'gepest', seksueel geïntimideerd, buitengesloten of gediscrimineerd te worden.[28] In het kader van dit onderzoek bleek dat er overigens weinig informatie over dit onderwerp bekend is, mede doordat het onderwerp in de taboesfeer ligt.[29] Betrouwbare cijfers over geweldpleging, seksuele intimidatie en vergelijkbare voorvallen zijn daarom voor het hoger-onderwijs niet aanwezig. Naar aanleiding van het aangehaalde onderzoek van de Open Universiteit zijn kamervragen gesteld aan de toenmalige minister van OCW. De minister merkte op dat het onderzoek geen representatieve steekproef bevat van het Nederlandse hoger onderwijs. Wel vindt de minister het beeld dat is ontstaan naar aanleiding van incidenten binnen enkele faculteiten 'zorgwekkend': 'Instellingen van onderwijs dienen leerlingen en studenten een veilige leeromgeving te garanderen. Dit is een essentiële voorwaarde voor elke vorm van onderwijs'.[30]

Medewerkers van instellingen in het hoger onderwijs ervaren een toenemende intimidatie en agressie vanuit studenten. Als verklaring wordt gewezen op de toenemende veeleisendheid van studenten (een ontwikkeling die past binnen de bredere ontwikkeling die wel een ontwikkeling van de *the demanding society* wordt genoemd). Als een student in de eigen

[28] HBO-Journaal 30 mei 2001

[29] Dit in tegenstelling tot de BVE-sector waar intimidatie een actueel onderwerp is. Zie bijvoorbeeld Dorien van Zundert, Agressie en geweld in het onderwijs, bijdrage in het kader van de vierde werkconferentie, georganiseerd door het platform Veiligheid en Geweld in de BVE-sector d.d. 6 juni 2002.

perceptie niet snel genoeg wordt geholpen, vindt zo nu en dan bedreiging en verbale intimidatie plaats. Onder de respondenten aan dit onderzoek zijn voorbeelden bekend van werknemers van dienstverlenende onderdelen binnen de instelling, zoals de audiovisuele dienst, die zich met regelmaat ernstig bedreigd voelen.

Ongeveer een derde van de in het kader van dit onderzoek bevraagde instellingen noemt intimidatie en geweldpleging als een van de grotere risico's binnen onderwijsinstellingen.

Net als vormen van agressie valt (seksuele) intimidatie onder de werkingssfeer van de Arbowet uit 1998. Dit betekent dat de werkgever de plicht heeft preventieve maatregelen te nemen die de werknemer en student beschermen. Daarnaast dient een instelling maatregelen te treffen die de gevolgen van een incident beperken, bijvoorbeeld door het aanstellen van vertrouwenspersonen of psychologen die slachtoffers kunnen bijstaan. De instelling bepaalt ook hier zelf hoe ze beleid terzake vormgeeft. Wel is de instelling verplicht een risicoinventarisatie en -evaluatie te maken.

Toenemend wapenbezit

In combinatie met het voorgaande risico wordt een potentieel gevaar gevormd door het vuurwapenbezit op scholen. Tot op dit moment zijn er geen gevallen bekend van incidenten binnen hoger onderwijsinstellingen die samenhangen met vuurwapenbezit van studenten. Echter daar waar op middelbare scholen een toenemend wapenbezit wordt gesignaleerd, lijkt aandacht voor dit potentiële probleem gewenst binnen het hoger onderwijs.

> In Rotterdam is een speciaal project gelanceerd om het wapenbezit op middelbare scholen terug te dringen. "Wapenbezit is een probleem; 31% van de Rotterdamse scholieren geeft aan wel een wapen bij zich te hebben". Het gaat in de meeste gevallen om messen of traangas. De samenwerking met de politie bij incidenten blijkt op scholen te verschillen.[31]

Er zijn geen cijfers bekend over wapenbezit binnen instellingen in het hoger onderwijs of over incidenten waarbij wapens werden gebruikt binnen het hoger onderwijs (ook in het

[30] TK 2000111510

buitenland). De meeste instellingen zien wapenbezit daarom niet als een groot risico. Er worden dan ook nauwelijks maatregelen genomen door de instellingen om wapens op te sporen of om te voorkomen dat iemand met een wapen het gebouw of terrein betreedt.

Onverdraagzaamheid resulterend in discriminatie of geweld

De multi-etniciteit van de Nederlandse maatschappij wordt ook, hoewel veelal nog in mindere mate, weerspiegeld binnen het hoger onderwijs. Met name in de grote steden kennen instellingen een kleurrijk palet aan verschillende culturen. Mede onder invloed van gebeurtenissen in andere delen van de wereld kunnen spanningen ontstaan tussen personen van verschillende culturele of religieuze afkomst. Evenals voor een risico als het toenemend wapenbezit geldt dat hoewel hoger onderwijs instellingen in Nederland tot nu toe van ernstige problemen op dit vlak zijn gespaard, er geen garantie bestaat dat de problemen die nu (al) op middelbare scholen spelen zich niet ook zullen manifesteren in het hoger onderwijs.

Het Regionaal Opleidingscentrum ROC Oost-Nederland in Hengelo (3.000 leerlingen) meldde eind november 2003 dat de spanningen tussen groepen moslim Turken en christelijke Suryoye (Armeniërs en Syriërs) zo hoog waren opgelopen, dat de schoolleiding de politie en gemeente Hengelo heeft gevraagd te bemiddelen. Spanningen tussen bevolkingsgroepen sloegen als het ware over van buiten de school naar groepen leerlingen die zich binnen de schoolmuren bevonden.

Volgens een woordvoerder van dat opleidingscentrum broeit het al geruime tijd tussen de twee bevolkingsgroepen. Op een gegeven moment verzamelden zich ongeveer 150 jongeren bij het ROC. De politie en het personeel wisten een confrontatie te voorkomen. Volgens het ROC is er geen directe aanleiding voor de onderlinge spanningen en is het meer een kwestie dat beide groeperingen elkaar niet goed liggen. De politie Twente heeft vervolgens enkele jeugdagenten vrijgemaakt om de gemoederen te bedaren. Er zijn gesprekken gevoerd met leerlingen, ouders en de geestelijk leiders. De gemeente Hengelo is ingeschakeld om een coördinerende rol te vervullen. Het ROC heeft de situatie tijdens de lessen met de leerlingen besproken. De woordvoerder reageert: "Maar we zijn natuurlijk geen politie. Onze primaire taak is het geven van onderwijs."

[31] Zie: BOOM, Op onze school zijn alle wapens verboden; Een evaluatie van de campagne tegen wapenbezit op Rotterdamse middelbare scholen, 2000

Verschillende instellingen hebben aangegeven dit risico te onderkennen en daar alert op te zijn. Zo is bijvoorbeeld naar aanleiding van de oorlog in Irak het Crisismanagementteam (CMT) van de Universiteit van Amsterdam enkele malen bijeen gekomen om een risicoanalyse te maken van de situatie.

4.3 Sociale risico's met een primair extern effect

In deze paragraaf worden de risico's met een primair extern effect beschouwd zoals die in dit onderzoek naar boven zijn gekomen. Deze risico's hebben daarmee geen direct gevolg voor de veiligheid binnen de instellingen, maar zijn er wel nauw mee verbonden.

Individuele problemen van studenten die leiden tot incidenten buiten de instelling
Het aantal studenten dat zich went tot een studentenpsycholoog neemt de laatste jaren fors toe. Hieraan liggen verschillende oorzaken ten grondslag, zoals eenzaamheid, depressie, faalangst, relationele problemen en een hoge studiedruk.[32] Dit kan leiden tot alcohol- en drugsgebruik, afnemende studieresultaten en zelfs zelfdoding.

> Naar aanleiding van een elftal zelfmoorden binnen twee academiejaren besloot de KU Leuven een onderzoek in te stellen naar de oorzaken van de zelfmoorden. Van de elf personen die zichzelf van het leven beroofden, waren negen van het mannelijk geslacht. Zelfdoding onder studenten is een probleem waar weinig cijfers over bekend zijn, ook niet bij universiteiten in de rest van Europa. In de VS wordt naar dit probleem meer studie verricht. De drie uitlokkende factoren voor zelfdoding zijn volgens het onderzoek van de universiteit: relationele problemen, studiegerichte problemen en geldnood.[33]

Het merendeel van de bevraagde instellingen in Nederland geeft aan dat zeer ernstige incidenten gerelateerd aan individuele problemen van studenten, zoals zelfdoding, binnen hun

[32] Zie bijvoorbeeld: H. Smit, 'Studentenpsycholoog krijgt steeds meer klachten, Drank, depressie en discipline', in: NRC Handelsblad, 14 april 2001 en 'Voer voor psychologen', in: Delta, jaargang 35, nr. 27
[33] Zie: Vandendriessche, D. en K. Raskin, 'Zelfmoord aan de KU Leuven: onderzoek en beleidsimplicaties, Studeren aan de universiteit: levensgevaarlijk?', Studentenweekblad van de Leuvense Overkoepeldende Kringorganisatie, nummer 16, 17 januari 2000

instelling niet of nauwelijks voorkomen. De instellingen kennen een systeem van studieadviseurs, vertrouwenspersonen en psychologen waar studenten met problemen zich toe kunnen wenden. Bij zeer schrijnende gevallen wordt doorverwezen naar professionele hulpverleningsorganisaties. Toch wordt het risico wel onderkend: de Universiteit Twente heeft bijvoorbeeld maatregelen genomen, zodat het niet langer mogelijk is om van hoge gebouwen af te springen.

Incidenten veroorzaakt door stagiairs of afstudeerders bij een andere instelling

Het komt voor dat een stagiair of student-assistent op zijn stageplaats op de een of andere manier de fout ingaat, bijvoorbeeld door gevoelige, vertrouwelijke informatie te verspreiden of door schade te veroorzaken. De instelling in het hoger onderwijs die de stagiair uitzend heeft een zekere verantwoordelijkheid voor het gedrag van de stagiair. In hoeverre deze verantwoordelijkheid ook aansprakelijkheid met zich meebrengt, hangt onder andere af van het stagecontract en de voorbereiding cq begeleiding van de student. Bij een van de instellingen die in het kader van dit onderzoek zijn bevraagd, zijn naar aanleiding van enkele ernstige incidenten geheel vernieuwde stagecontracten ontworpen met het oog op het beperken van de aansprakelijkheid van de instelling voor eventuele schade.

Ontoelaatbaar gedrag gerelateerd aan studentenverenigingen

Binnen de studentenverenigingen hebben zich in het verleden verschillende incidenten voorgedaan waarbij gewonden en zelfs doden zijn gevallen, met name in het kader van de ontgroening. Bij veel van die incidenten was sprake van excessief alcoholgebruik.

> Waarschijnlijk het bekendste incident deed zich in 1965 voor bij een elitaire subvereniging van het Utrechts Studenten Corps; Tres. Van deze subvereniging konden alleen leden van adellijke komaf lid worden. Tres had een eigen ontgroening. Een onderdeel van deze ontgroening bestond uit het plaatsen van een roetkap over het hoofd van het aspirant-lid. Dit werd uiteindelijk een aspirant-lid fataal. Zijn dood maakte een golf van maatschappelijke kritiek los en leidde uiteindelijk tot de opheffing van Tres.[34]

[34] Zie; Heijnen, A., 'Redactioneel, Très', Ublad, 10 december 1998

Op zichzelf heeft de instelling geen directe verantwoordelijkheid over wat er zich afspeelt binnen of buiten de muren van de studentenvereniging. Wel voelt elke instelling een vanzelfsprekend zorgplicht voor haar studenten. Daarnaast kunnen incidenten schade veroorzaken aan het imago van de instellingen. Recente incidenten laten dan ook een actieve reactie van het bestuur van de betrokken instellingen zien:

- Bij de corpsontgroening van het Delfts Studenten Corps (DSC) doet zich in 1999 een ernstig incident voor. Een 19-jarige student die deelneemt aan de kennismakingstijd wordt ernstig mishandeld door twee ouderejaars. De student moet worden opgenomen in het Bronovoziekenhuis met scheurtjes in zijn botten. De daders zijn door de politie gearresteerd. De collegevoorzitter van de Technische Universiteit Delft is van mening dat dergelijke incidenten ook schade veroorzaken aan de goede naam van de universiteit. De TU heeft echter geen maatregelen genomen omdat het bestuur van DSC kordaat heeft opgetreden in de afwikkeling van het incident.[35]
- In 2000 verbreekt de Erasmus Universiteit voor een jaar de banden met het Rotterdams Studenten Corps (RSC). Dit doen zij nadat is gebleken dat er zich onoorbare praktijken hadden afgespeeld bij de ontgroening, waarbij aspirant-leden met honkbalknuppels zouden zijn geslagen. 'Het besluit om de erkenning in te trekken is bedoeld als strafmaatregel omdat door gedragingen binnen het RSC de goede naam van de Erasmus Universiteit opnieuw in diskrediet is gebracht'.[36]
- De Utrechtse verenigingen Veritas en Unitas worden in 2001 gesanctioneerd nadat blijkt dat zich binnen de verenigingsontgroeningen incidenten hadden voorgedaan. De Universiteit Utrecht en de Hogeschool Utrecht verbreken de banden met Veritas. De reden was dat een ontgroener een sigarettenpeuk op de arm van een aspirant-lid heeft uitgedrukt. Unitas wordt minder zwaar gestraft met een voorwaardelijke schorsing en intrekking van subsidies.[37]

Alcohol- en drugsgebruik onder studenten

De Onderwijsraad signaleert dat, in tegenstelling tot roken en overgewicht, alcoholconsumptie hoger ligt bij hoger opgeleiden (HBO, WO) dan bij lager opgeleiden.38

[35] Zie: 'Corpsleden bekennen mishandeling nuldejaars', in: Delta, jaargang 31, nummer 27
[36] 'Erasmus straft studentencorps voor wangedrag', in: NRC Handelsblad, 17 oktober 2000
[37] 'Erasmus straft studentencorps voor wangedrag', in: NRC Handelsblad, 17 oktober 2000
[38] Onderwijsraad, Samen leren leven, Verkenning, 2002, p. 44

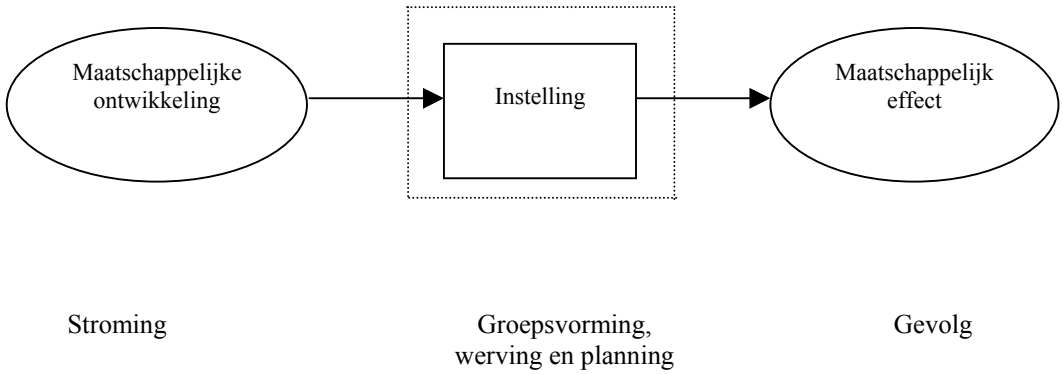
Daarnaast is het gebruik van verdovende of stimulerende middelen onder studenten in het hoger onderwijs aanzienlijk. Volgens een onderzoek onder 750 studenten van de Universiteit van Amsterdam door het universiteitsblad Folia blijkt dat één op de drie studenten wel eens een joint rookt.[39] Eén op de tien studenten geeft aan wel eens cocaïne te gebruiken. De top vijf van populaire verdovende middelen uit het Folia- onderzoek is cannabis, XTC, cocaïne, paddestoelen en speed. De respondenten van het Folia-onderzoek geven aan vooral in de weekenden en 's avonds te gebruiken.

Het gebruik van alcohol en drugs vindt met name plaats buiten de muren van de instelling. De instelling is hiervoor niet primair verantwoordelijk, maar sommige instellingen trekken zich de problematiek wel aan: In 1997 gaf de rector magnificus van de Technische Universiteit Delft aan dat hij wil dat studenten anders met drank omgaan. Dit doet hij vlak na excessief drankmisbruik bij een corpsontgroening in Groningen, waarbij een dode en een zwaargewonde vielen nadat beiden een liter jenever hadden gedronken. De rector magnificus kondigt aan over deze problematiek in gesprek te willen raken met de verschillende Delftse studentenverenigingen. De rector magnificus wil geen regels of verboden opleggen, maar een attitudeverandering bewerkstelligen. 'Het is misschien niet onze rechtstreekse verantwoordelijkheid, maar de TU voelt zich wel verantwoordelijk'.[40]

Extremisme binnen het hoger onderwijs

Traditioneel zijn studenten als hoog opgeleide burgers kritisch. Belangengroeperingen en andere issuepartijen vinden dikwijls voedingsbodem binnen instellingen in het hoger onderwijs. De meeste van deze verbanden uitten hun kritiek op vreedzame, ludieke wijze, maar er zijn ook voorbeelden waarbij groeperingen geweld gebruikten om hun standpunten kracht bij te zetten. Op het gebied van antiglobalisme, milieu en dierenrechten zijn er ook groepen en individuen actief in Nederland die zich bereid hebben getoond geweld of vernieling als middel niet te schuwen. De instellingen binnen het hoger onderwijs kunnen derhalve gezien hun aard ongewild fungeren als een katalysator van maatschappelijke onvrede.

[39] Zie: http://www.foliacivitatis.nl
[40] 'Rector wil beraad over drankgebruik', in: Delta, jaargang 29, nr. 28



Figuur: de instelling als katalysator van onvrede over maatschappelijke ontwikkelingen.

Terrorisme

Evenals voor extremisme geldt dat instellingen binnen het hoger onderwijs gezien hun aard voor terroristen aantrekkelijk kunnen zijn. Het gaat dan niet om het hoger onderwijs als doelwit voor aanslagen, maar als wel als doelwit voor recrutering of als schuilhaven. In het hoger onderwijs leeft dit vraagstuk en de risico's ervan vooralsnog nauwelijks.[41]

Een van de zwartste scenario's is dat een terroristische cel zich bevindt binnen de instelling. Mohammed Atta en andere kapers van vliegtuigen studeerden aan de Technische Universiteit Hamburg-Harburg en hadden aldaar informele meetings.[42] De daadwerkelijke werving vond overigens plaats in Hamburgse moskeeën. Ook in Nederland hebben fundamentalistische moslimgroeperingen aanhang. Zij werven ook studenten om zich in te zetten voor gewelddadige acties. Volgens de AIVD gaat het met name om leden van de Marokkaanse gemeenschap. 'Op het oog goed geïntegreerd, blijken sommigen van hen een dusdanig radicaal, anti-Nederlands en antiwesters gedachtegoed te hebben, dat zij bereid zijn deel te nemen aan gewelddadige terroristische activiteiten'.[43]

[41] COT, Aandachtspunten OCenW dreiging oorlog Irak (concept), 2003; 4
[42] Zie: Peter Finn, 'Sept. 11 plot came together in Germany', in: The Washington Post, 11 september 2002
[43] AIVD, Jaarverslag 2002; 39

Twee studenten uit Eindhoven worden in Nederland gerekruteerd voor de Jihad. In januari 2003 worden zij in Kasjmir doodgeschoten door de Indiase grenspolitie. 'Het zijn vooral Marokkaanse jongeren [die worden gerekruteerd, COT], geen hangjeugd maar juist goed opgeleide jongens van universitair of hbo-niveau die kampen met een ernstige identiteitscrisis en een uitweg zoeken in radicalisering en het martelaarschap voor God. De gevestigde islamitische NGO's zoals moskeestichtingen, scholen en welzijnsorganisaties spelen daarbij niet direct een rol. Die rekruteren niet zelf, maar dragen bij aan het creëren van de voedingsbodem'.[44]

Onveiligheid buiten het terrein van de instelling

Verscheidene instellingen zijn gevestigd op locaties met een hoger sociaal risico. Het gaat hier om gebieden die met name 's nachts onveilig zijn of als onveilig worden ervaren. Studenten en medewerkers van instellingen kunnen worden lastig gevallen, beroofd of worden geconfronteerd met verbale of fysieke agressie of zelfs aanranding.

De Haagse Hogeschool is gevestigd in een dergelijke risicobuurt. Om naar de hogeschool te komen vanaf station Hollands Spoor moet men door de voetgangers- en fietsertunnel: 'En daar gaat het vaak mis. Drugsgebruik en berovingen zijn schering en inslag. De medezeggenschapsraad eist maatregelen'. Op zich heeft de Haagse Hogeschool geen directe verantwoordelijkheid voor de situatie buiten de schoolmuren, maar zij trekt zich de situatie wel aan; 'Het is natuurlijk ook onze plicht om de veiligheid van leerlingen, leraren en andere medewerkers zoveel mogelijk te garanderen. De school ergert zich al langere tijd aan de verloedering rond het station waar vooral 's avonds drugsdealers en junks het straatbeeld bepalen'.[45] Volgens de politie is vooral het gevoel van onveiligheid een probleem. Statistisch gezien bestaat er geen reden om aan te nemen dat de situatie veel onveiliger is geworden. Toch vindt 80% van de studenten van de hogeschool het station een 'enge boel', aldus het studentenblad Atrium.[46] Naar aanleiding van het toegenomen gevoel van onbehagen heeft overleg plaatsgevonden tussen de politie en de hogeschool. Hierop heeft de politie de

[44] A. Brouwer, 'De Algerijnse connectie', in: De Groene Amsterdammer, 16 november 2002
[45] 'Hogeschool wil af van onveilige tunnel', in: De Posthoorn, 2 mei 2001
[46] Zie: 'Het onveilige gevoel rond Hollands Spoor', in: de Haagse Courant, 19 april 2002

surveillance afgestemd op de lesrooster van de hogeschool. Daarnaast wordt het cameratoezicht op het station geïntensiveerd.

4.4 De veiligheidsketen toegepast op sociale veiligheid

De voornaamste risico op het gebied van sociale veiligheid die door de geënqueteerde hogescholen en universiteiten zijn genoemd, zijn in de voorgaande paragrafen de revue gepasseerd. In deze paragraaf zullen aan de hand van de veiligheidsketen verschillende aandachtspunten voor sociaal risico- en crisismanagement worden gepresenteerd. Deze aandachtspunten zijn deels afgeleid van 'best practices' die de instellingen zelf via de enquêtes hebben teruggekoppeld. In de Hoger Onderwijs Veiligheidsaudit in bijlage I zijn de aandachtspunten weergegeven per benoemd risico binnen dit domein.

Pro-actie en preventie

- Maatschappelijke trends die ook voor de instelling risico's met zich mee kunnen brengen worden gevolgd door de instelling;
- De instelling heeft een monitoringsysteem (melding en analyse) van sociale spanningen en gevoelens van onveiligheid dat inzicht geeft in microtrends binnen de instelling;
- De instelling is consequent in gesprek met vertegenwoordigers van verschillende groepen binnen de studentenpopulatie;
- De instelling geeft grenzen aan met betrekking tot toelaatbaar gedrag en handhaaft deze grenzen;
- De instelling bevordert bij werknemers en studenten erkenning dat een sociaal veilige werk- en studieomgeving van groot belang is;
- De instelling besteedt zorg aan gebouwen en terreinen vanuit de onderkenning van de voorbeeldfunctie daarvan;
- De instelling bevordert draagvlak onder studenten en medewerkers voor het sociaal veiligheidsbeleid, waardoor excessen als intimidatie, racisme en bedreigingen ook door hen niet worden getolereerd;

- De instelling deelt kennis over pro-actie/preventie met collega-instellingen;
- De instelling rapporteert periodiek over de sociale veiligheid binnen de instelling;
- De instelling betrekt vertrouwenspersonen, studiebegeleiders, decanen en studentenpsychologen bij het sociaal veiligheidsbeleid;
- De instelling initieert overleg tussen instelling en vertegenwoordigers van studentenpopulatie, medewerkers en partners buiten de instelling, om samen oplossingen te zoeken voor sociale onveiligheid binnen en buiten de instelling;

Preparatie

- De instelling draagt zorg voor een adequaat opleidingsniveau (zoals cursussen conflictbeheersing) van vertrouwenspersonen, psychologen, decanen en studiebegeleiders;
- Door de instelling zijn draaiboeken ontwikkeld voor bijvoorbeeld seksuele intimidatie en agressie;
- De instelling kent een bij medewerkers en studenten bekende meldingsprocedure voor sociale incidenten;
- De instelling deelt kennis over preparatie met collega-instellingen;
- De instelling initieert structureel overleg De instelling deelt kennis over pro-actie/preventie met collega-instellingen en afstemming met relevante externe partijen – zoals de politie – die een rol spelen bij incidenten;

Respons

- De instelling zet eigen studentendecanen, vertrouwenspersonen en studentenpsychologen in;
- De instelling vormt een tactisch en strategisch coördinatieteam voor interne en externe afstemming van de activiteiten in deze fase;
- De instelling informeert studenten, medewerkers en relaties over het incident en de genomen maatregelen;
- De instelling betrekt waar mogelijk (vertegenwoordigers van) de studentenpopulatie en medewerkers bij besluitvorming in de responsfase.

Herstel

- De instelling doet aangifte bij ernstige incidenten;
- De instelling evalueert ernstige voorvallen, met als doel van het incident te leren opdat dergelijke voorvallen in de toekomst binnen de eigen of andere instellingen kunnen worden voorkomen;
- De instelling coördineert de activiteiten in de herstelfase op tactisch en strategisch niveau;
- Evaluaties leiden derhalve binnen de instelling tot het bijstellen van de risicoanalyses en het sociaal veiligheidsbeleid;.
- De instelling draagt zorg voor begeleiding of doorverwijzing van medewerkers of medestudenten die nadere (psychosociale) zorg behoeven. Hiertoe wordt samenwerking met externe partijen gezocht.

HOOFDSTUK 5
HOGER ONDERWIJS ALS ORGANISATIE

5.1 Inleiding

Dit hoofdstuk gaat in op organisatieveiligheidsrisico's voor het hoger onderwijs. Dit zijn de risico's die ook van toepassing zijn voor andere organisaties buiten het hoger onderwijs en wetenschappelijk onderzoek met een vergelijkbare omvang.

> 'Ieder bedrijf of instelling kan te maken krijgen met incidenten. Naast de min of meer bekende incidenten als ongevallen en branden moet daarbij ook gedacht worden aan bijvoorbeeld uitval van telefoon- en datavoorzieningen, overstroming, negatieve persberichten etc'.[47]

Een belangrijk deel van de risico's heeft betrekking op de fysieke veiligheid; het gaat daarbij om bedreigingen van de gebouwen, terreinen en goederen van de instellingen. Voorbeelden van dergelijke risico's zijn brand en inbraak. Andere risico's die in dit hoofdstuk aan de orde komen zijn van een heel ander karakter: fraude, reguliere arbeidsrisico's, bedreigingen van het interne werkmilieu, ed.

In dit hoofdstuk zullen de risico's verder worden onderverdeeld naar risico's met een primair interne oorzaak en risico's met een primair externe oorzaak.

Aan de hand van de methodiek van de veiligheidsketen zal worden ingegaan op de mogelijkheden die de onderwijsinstellingen hebben om risico's en incidenten op het gebied van organisatieveiligheid te beheersen. In het hoofdstuk zullen verder ervaringen van instellingen binnen het hoger onderwijsinstellingen worden gepresenteerd.

[47] Zie: Dienst Facilitaire Zaken, Hanzehogeschool Groningen, Bedrijfsnoodplan Faculteit Economie en Bestuur & Stafbureaus, 2003

Hieronder zullen als eerste enkele algemene conclusies vanuit de enquête en interviews worden gepresenteerd.

Algemeen

Instellingen geven aan dat er recent een toenemende aandacht is voor het thema 'organisatieveiligheid' binnen hun organisaties. Veiligheid komt meer en meer op de agenda van de colleges van bestuur komen te staan en binnen veel colleges zijn portefeuillehouders 'veiligheid' aangewezen.

De instellingen zijn van mening dat de alertheid op en het bewustzijn van risico's bij medewerkers en studenten betrekkelijk laag zijn. Daarnaast zijn instellingen van mening dat technische oplossingen vaker kunnen worden toegepast dan op dit moment het geval is. Sprinklerinstallaties, automatische alarmsystemen en inbraakbeveiligingen kunnen de organisatieveiligheid verder verhogen.

Risicoperceptie instellingen en ontwikkelingen

Instellingen zien inbraak en brand als het grootste risico binnen de organisatieveiligheid. Andere mogelijke incidenten worden door de meeste instellingen nog nauwelijks als een reëel risico herkend.

Na de vuurwerkramp in Enschede en de cafébrand in Volendam wordt door de instellingen een stringentere handhaving van wet- en regelgeving op het gebied van fysieke veiligheidsrisico's ervaren. Ook verzekeraars stellen hogere eisen aan de instellingen. Een onverwachte consequentie daarvan is dat bij een gelijkblijvend budget de noodzakelijke investeringen in veiligheid leiden tot een mindere investering in het primaire proces (onderwijs of onderzoek).

Melden en registreren van incidenten

Vrijwel alle instellingen registreren en analyseren incidenten rond organisatieveiligheid. De mate waarin instellingen een systeem hebben om incidenten te melden, wisselt echter per organisatie. Een aantal hoger onderwijsinstellingen is ook begonnen met het nauwkeurig vastleggen van bijna-ongevallen. In een aantal gevallen worden ook jaarlijkse cycli van risico-inventarisaties en evaluaties gehouden. De leerpunten worden in die gevallen meegenomen in de planvorming en het aanscherpen van de BHV-organisatie.

Risicoscan

Uit de enquête is gebleken dat ongeveer tweederde van de instellingen een risico-inventarisatie en -evaluatie (RIE) maakt, en daarbij veelal gebruikmaken van advies van externen. Deze RI&E heeft dan in het algemeen het klassieke 'arbo'-karakter.

Een enkele instellingen geeft aan principes van de lerende organisatie binnen haar organisatie te hebben geïncorporeerd. Veiligheidsmedewerkers van de verschillende faculteiten houden elkaar scherp. Huismeesters lopen van tijd tot tijd elkaars gebouwen na, om zodoende goede zaken van elkaar over te nemen en fouten te elimineren. In een andere instelling wordt eenmaal per kwartaal een onaangekondigde controleronde gelopen door de facilitair manager en een directielid. Daarbij wordt steekproefsgewijs ook naar basale dingen als stopcontacten, trapjes en dergelijke gekeken.

Samenwerking met interne en externe partijen

De totstandkoming van het preventieve beleid op het terrein van de organisatieveiligheid vindt vrijwel nergens plaats in overleg met medewerkers en studenten. Wel geldt op dit terrein in de preparatie en de responsfase klassiek een sterke betrokkenheid van medewerkers en studenten voor de fysieke veiligheidsrisico's: medewerkers vormen de BHV-organisatie, studenten en medewerkers nemen deel aan ontruimingsoefeningen.

De meeste instellingen maken gebruik van gespecialiseerde externe partijen bij het vormgeven en uitvoeren van het organisatieveiligheidsbeleid. Een gevolg hiervan lijkt te zijn dat veel instellingen geen eigen en integraal beeld hebben op dit terrein. Zo is er bij veel

instellingen een goed overleg met de brandweer voor het aspect brandveiligheid. Instellingen dreigen dan licht te vergeten dat de zorg voor de bedrijfscontinuïteit een andere is dan de zorg voor de persoonlijke veiligheid die primair is voor de brandweer.

5.2 Organisatieveiligheidsrisico's met een primair interne oorzaak

Brand

Brand is een van de meest in het oog springende risico's. Instellingen besteden in BHV-plannen en calamiteitenplannen aandacht aan de brandpreventieve voorzieningen die zijn aangelegd om brand in de gebouwen te voorkomen. Met regelmaat worden binnen de meeste instellingen brandalarmoefeningen en ontruimingsoefeningen gehouden, die beoogd bijdragen aan een grotere bewustwording bij studenten en medewerkers.

De effecten van de grote brand op de Technische Universiteit in Enschede waren echter voor instellingen en verzekeraars een eye-opener. Brand bleek een erger doemscenario voor veel instellingen dan gedacht was. Dit heeft vanuit de zijde van de verzekeraars tot aanvullende eisen geleid. Bij nadere beschouwing bleken instellingen kwetsbaarder dan gedacht. Slechts een enkele instelling heeft bijvoorbeeld back-ups en (vervangende) rekencentra buiten de eigen complexen ondergebracht. Veel instellingen zijn gehuisvest in oudere panden (sommige met historische waarde) met beperktere brandveiligheid. Instellingen hebben verder vaak unieke collecties die door brand verloren kunnen gaan.

Brandstichting

Brandstichting verdient een aparte vermelding als risico omdat brandpreventieve voorzieningen in het algemeen niet ontworpen zijn op de snelle brandontwikkeling die vaak het gevolg is van brandstichting. De al aangehaalde brand op het terrein van de Universiteit Twente is bijvoorbeeld ontstaan door brandstichting.

Het is niet eenvoudig om brandstichting te voorkomen. Uit de ervaring van verzekeraars blijkt dat symptomen in veel gevallen niet als *early warning indicators* van grotere brandstichtingen worden geïnterpreteerd. Een brandende papierbak wordt niet gezien als een (mislukte)

poging tot brandstichting, maar slechts geïnterpreteerd als een daad van vandalisme gericht op de desbetreffende papierbak.

Een belangrijk motief voor brandstichting kan wraak zijn door bijvoorbeeld (ex)werknemers, actiegroepen en (ontspoorde) studenten. Actiegroepen zullen het vooral gemunt hebben op specifieke laboratoria waar dierproeven of andere maatschappelijk gevoelige proeven worden gehouden. De plaats van brandstichting hangt af van de motieven en zal in die gevallen doorgaans met zorg gekozen worden. Pogingen tot brandstichting die binnen de gebouwen worden ondernomen zullen met name via toezicht moeten worden voorkomen. Samenvattend is een belangrijke factor in de bestrijding van brandstichtingen a) het vergroten van de alertheid onder studenten en medewerkers en b) het implementeren of verbeteren van *early warning systemen* binnen de instelling in het hoger onderwijs.

Arbeidsveiligheid algemeen

Instellingen hebben als werkgever een verantwoordelijkheid voor de gezondheid van werknemers en studenten. Bepaalde opleidingen zijn vanzelfsprekend gevoeliger voor lichamelijke ongelukken dan andere. Het risico op verwondingen bij studenten is hoger voor een studie lichamelijke opvoeding dan voor accountancy. De met deze studies gepaard gaande risico's vragen een specifieke aanpak. Ook werkzaamheden in werkplaatsen of laboratoria vergen extra veiligheidsmaatregelen.

Instellingen zetten in verschillende mate in op bewustwording bij medewerkers en studenten van de risico's die zij lopen. Verschillende instellingen hebben aangegeven dat het risicobewustzijn binnen die instellingen bij met name studenten gering is. Enkele instellingen hebben op dit gebied beleid ontwikkeld mede uit angst voor aansprakelijkheid bij ongevallen. Een aangetroffen best-pratice is bijvoorbeeld veiligheidsinstructie gevolgd door het laten tekenen voor ontvangst van een handleiding voor laboratoriumveiligheid.

Naar aanleiding van een onderzoek op de Universiteit Utrecht bleek dat 40% van de studenten RSI-klachten heeft. Het CvB van de universiteit geeft aan ergonomische maatregelen in de computerlokalen te zullen nemen, maar dat RSI tegelijkertijd ook een verantwoordelijkheid is

van de individuele student. ‘Studenten dienen ook hun eigen grenzen in acht te nemen als het gaat om RSI preventie met de hulp van computerprogramma's als Workpace’.[48]

Arbeidsveiligheid specifiek: bedreiging van het interne milieu door gevaarlijke stoffen (waaronder asbest)

Verschillende instellingen zijn geconfronteerd met bedreiging van het interne milieu binnen de instelling. In de meeste gevallen gaat het hier om ontdekking van asbest, maar in enkele gevallen ook om het vrijkomen van gevaarlijke stoffen die voor onderwijs- of onderzoeksdoeleinden worden gebruikt. Zo leidde het lekken van formaline bij een instelling tot inzet van de brandweer die de lekkende opslagcontainer moest afvoeren.[49] Overigens kunnen bij renovaties ook andere gevaarlijke bouwstoffen vrijkomen, zoals oude verfresten.

Op de faculteit Lucht- en Ruimtevaarttechniek van de Technische Universiteit Delft werd asbest aangetroffen in een werkruimte en een ventilatieschacht. Het gebouw werd daarop geheel ontruimd. De verwijdering van het asbest kostte enkele weken. Het primair proces heeft door het realiseren van uitwijkvoorzieningen nauwelijks te lijden gehad.[50]

Verscheidene instellingen maken zich specifiek zorgen over de veiligheid in en rond de laboratoria. Hierbij is het opvallend dat de instellingen van mening zijn dat de veiligheid in hun eigen laboratoria voldoende is geregeld. Men verwacht juist bij de laboratoria van collega-instellingen grotere veiligheidsrisico’s. Een veelgenoemd risico is inbraak in laboratoria waarbij door ondeskundige of vandalistische handelingen gevaarlijke stoffen of organismen vrijkomen. Een van de instituten heeft een specifieke risicobeperkende maatregel doorgevoerd: door op de begane grond geen *flatscreens* te installeren en geen laptops voor het personeel beschikbaar te stellen, is de inbraakgevoeligheid van het pand gedaald.

Sommige instellingen werken met microbiologische ziekteverwekkers[51]. De veiligheidsmaatregelen omtrent de beveiliging van laboratoria die met dergelijke ziekteverwekkers is ingedeeld in een viertal niveaus die mondiaal gelden: de *biosafety level-*

[48] Zie bijvoorbeeld: http://www.edusite.nl/edusite/nieuws/10699
[49] Zie: ‘Giflek bij Ziekenhuis’, Provinciale Zeeuwse courant. 10 juni 2004
[50] Zie: ‘Asbest ontdekt bij elektrotechniek’, Delta, nummer 14, jaargang 28
[51] Ook wel pathogenen. Onderscheiden worden: virussen, bacterieën, prionen, schimmels en parasiteiten.

schaal (BSL). Geïnterviewde operationeel verantwoordelijken hebben zorgen over de beveiliging van deze laboratoria. Dit heeft mede te maken met de afweging tussen budget beschikbaar voor beveiligingsmaatregelen en budget beschikbaar voor het primaire onderzoeksproces.

Fraude

Fraude is een veelvormig fenomeen ook binnen instellingen van het hoger onderwijs. In de eerste plaats gaat het dan, als bij elke organisatie, om het nemen van maatregelen zodat eigen werknemers niet in verleiding worden gebracht.

Een recent voorbeeld waar op grote schaal fraude werd gepleegd door studenten betreft de betaalpasfraude op de Hogescholen van Fontys. De hogeschool kwam er begin 2003 achter dat studenten op grote schaal hun chippassen illegaal hebben opgewaardeerd. Het bestuur houdt rekening met een schade die 50.000 euro kan bedragen, maar mogelijk is dit meer. Via een apparaat dat bij postorderbedrijven te koop is, bleek het eenvoudig om het saldo van de pas op te waarderen. Men had in een eerder stadium al gemerkt dat op kleine schaal illegaal passen werden opgewaardeerd, maar toen dit een grote vlucht nam, besloot het bestuur in te grijpen. De hogeschool heeft alle studenten een brief gestuurd met de mededeling dat bij vrijwillige melding af zal worden gezien van justitiële vervolging, tenzij de student zich heeft verrijkt door handel te drijven in het illegaal opwaarderen van passen.[52] Na het verstrijken van de deadline van melden, hadden 120 studenten zich gemeld bij de beveiliging. De berichtgeving over deze fraude in de regionale media is een illustratie van de in hoofdstuk 2 genoemde crisistrends: ‘Typisch een voorbeeld waaruit blijkt dat centralisatie van diensten leidt tot een te grote afstand tussen werkvloer en dienstverleners. De dienstverleners zitten in hun ivoren torens en negeren signalen dat het fout gaat. En als het fout gaat dan gaat het ook meteen Fontysbreed fout en mag je uit de krant lezen wat beleidsmakers nu weer gedaan hebben met geld dat eigenlijk bestemd is voor onderwijs’.[53]

[52] Zie: http://www.fontys.nl/nieuws/nieuws_artikel.asp?docid=1905
[53] Honderdtwintig studenten melden fraude bij Fontys, In: Branbants Dagblad, 26 februari 2003

Naast dergelijke vormen van fraude is ook examenfraude door het plegen van plagiaat een vorm die met regelmaat voorkomt. In het volgende hoofdstuk over kennisveiligheid zal nader op dit onderwerp worden ingegaan.

> De faculteit Rechtsgeleerdheid van de Universiteit Utrecht constateerde een toename van het aantal gevallen van tentamenfraude en besloot daarop tot verscherping van de controles.[54]

Overigens komt fraude met studiefinanciering frequent voor. Deze vorm van fruade valt echter buiten de scope van dit onderzoek gezien het feit dat de instelling noch probleem- noch effecteigenaar is.

5.3 Organisatieveiligheidsrisico's met een primair externe oorzaak

Inbraak

Inbraak wordt door de meeste instellingen gezien als een groot risico. Hierbij speelt niet alleen het risico op het verlies van apparatuur, maar zeker ook het verlies van kostbare informatie. De beveiliging buiten kantooruren wordt over het algemeen als voldoende beschouwd; men werkt met toegangscontroles en pasjessystemen voor de verschillende gebouwen.

Hogescholen en universiteiten bieden in de dagsituatie een open omgeving, waarin kwaadwillende personen eenvoudig en anoniem hun slag kunnen slaan. Verzekeraars dringen aan op het instellen van een kliklijn, om de drempel om opvallende zaken te melden, zo laag mogelijk te maken.

Extreme weersomstandigheden

Extreme weersomstandigheden worden binnen het onderwijs nauwelijks als risico gezien. Toch kunnen extreme weersomstandigheden tot grote schade en overlast leiden. Zo zorgden twee wolkbreuken op de Universiteit Twente in 2002 voor flinke wateroverlast. De brandweer moest eraan te pas komen om de kelders leeg te pompen. Het is raadzaam om vooraf na te

[54] Zie: 'Nieuws, rechten pakt fraude stevig aan', in: Ublad, 24 januari 2002

gaan welke locaties binnen de instellingen zich in kelders bevinden en in hoeverre hier kwetsbare situaties ontstaan bij wolkbreuken, extreme en langdurige regenval of sneeuwoverlast. Speciale aandacht is verder wenselijk voor kwetsbare locaties die bij zware storm kunnen instorten.

De Universiteitsbibliotheek van de Universiteit Maastricht heeft een calamiteitenplan (Collectie Hulpverlening), waarmee een (boeken)collectie in geval van bijvoorbeeld brand- en/of waterschade snel in veiligheid kan worden gebracht. Het plan is gebaseerd op het calamiteitenhandboek van het Overleg Kunst(historische) Bibliotheken Nederland (OKBN) een calamiteitenhandboek, dat instructies geeft ter voorkoming en beperking van schade als gevolg van brand, waterschade en schimmel. Daarnaast worden instructies gegeven voor het verpakken en de registratie van het te evacueren materiaal en eisen waaraan de droogruimte moet voldoen.

Een bijzondere weersomstandigheid die in menige verzekeringspolis wordt uitgesloten, maar door de instellingen niet als risico wordt gepercipieerd, is blikseminslag die inductie veroorzaakt in elektronische apparatuur: bij het inslaan van bliksem ontstaan door magnetische velden op grote afstand van de inslag sterke inductiespanningen. Zonder de nodige beveiligingen kunnen elektronische apparaten (computers, televisietoestellen, gevoelige meetapparatuur) hierdoor volledig vernield worden. In moderne onderwijsomgevingen is het onmogelijk om alle apparatuur los te koppelen van het lichtnet. Servers staan doorgaans dag en nacht aan, net als faxapparatuur, telefooncentrales, alarminstallaties, etc. Zonder de nodige beveiligingen kan – letterlijk – in één klap niet alleen de apparatuur, maar ook de kennis die op het netwerk is vastgelegd, verloren gaan.

Infectieziekten

Binnen een instelling kan een uitbraak van een infectieziekte ontstaan. Op zich vormen studenten in het hoger onderwijs, in tegenstelling tot scholieren in het lager onderwijs (basisscholen, bepaalde internaten), geen bijzondere risicogroep. Toch is het mogelijk dat een student bijvoorbeeld een besmettelijke ziekte als open TBC of hepatitis A oploopt en medestudenten besmet.

Een specifieke infectieziekte is legionella. Het is mogelijk dat in de gebouwen van de instelling legionellabesmetting ontstaat in het leidingstelsel (of een andere vochtige plaats, zoals koeling of airconditioning). Bij verneveling van water ontstaan aërosolen: kleine druppeltjes die bij inademing besmetting kunnen veroorzaken. In Nederland vond in 1999 een grootschalige epidemie plaats van de veteranenziekte ofwel legionellose, waarbij ongeveer 300 mensen besmet raakten en 30 mensen overleden. De bron bleek een bubbelbad te zijn op een bloemententoonstelling. Naar aanleiding hiervan is aangescherpte regelgeving van kracht geworden.

De uitbraak van SARS toonde aan hoe makkelijk een infectieziekte zich kan verspreiden in ziekenhuizen. Veel besmettingen betroffen nosocomiale besmettingen; infecties die ontstonden in ziekenhuizen zelf. Deze instellingen kennen beleid en planvorming hiervoor.

De Hogeschool Zeeland onderkende het besmettingsgevaar van SARS gezien de ongeveer 250 Chinese studenten die een studie volgen binnen de instelling. De instelling heeft verschillende maatregelen genomen, zoals het benaderen van deze studenten per e-mail, waarin een negatief reisadvies naar hun vaderland wordt gegeven. Daarnaast hield de hogeschool risicogebieden nauwlettend in de gaten. Indien een leerling van de school relevante symptomen zou vertonen, zou onmiddellijk een arts worden ingeschakeld. Ook zijn zes studenten die uit Shanghai terugkeerden naar Vlissingen preventief in vrijwillige quarantaine geplaatst. [55]

Dreiging met aanslagen

In bedrijfsnoodplannen anticiperen veel instellingen op bommeldingen. Het wordt daarbij aan de beoordeling van de politie overgelaten of de bommelding serieus moet worden genomen. De brandweer is verder betrokken wanneer het gaat om dreiging van aanslagen met nucleaire, chemische of biologische stoffen. In beide gevallen worden de geldende ontruimingsprocedures gevolgd.

[55] 'Maatregelen SARS op Hogeschool Zeeland', in: De Telegraaf, 3 april 2003

Na de aanslagen in de VS in 2001 met anthraxpoeder in brieven is er ook in Nederland een grote hoeveelheid valse poederbrieven gestuurd. Vanzelfsprekend kan een dergelijke poederbrief minstens evenveel onrust, angst en onzekerheid losmaken als een bommelding.

> 'Tot 1 februari 2003 zijn door het Centraal Instituut voor Dierziekte Controle (CIDC) te Lelystad 992 monsters [poedersamples, COT] onderzocht; de piek lag in week 42 van 2001 maar het aantal nam vervolgens snel af. In week 52 was er weer een lichte stijging van onderzochte monsters, maar deze stijging kwam mede door het onderzoeken van kerstkaarten waar poedersneeuw vanaf kwam. Het jaar 2002 gaf een veel rustiger beeld van het aantal gemelde poederbrieven en pakjes. Dit leidde tot het afschalen van de mogelijkheid om 24 uur per dag materiaal voor onderzoek aan te leveren bij het CIDC. In 2003 wordt gemiddeld één monster per week onderzocht'. [56]

Een constante dreiging bestaat voor instellingen waar met proefdieren wordt gewerkt. Tot nu toe hebben zich verschillende incidenten voorgedaan, waarbij tegenstanders van een dergelijke proeven waren betrokken zoals een drietal bezettingen, bommeldingen, demonstraties, brandstichtingen en vernielingen. Ook voor instellingen waar met genetisch gemanipuleerde organismen wordt gewerkt, geldt een dergelijke dreiging. Instellingen proberen met voorlichting begrip te kweken voor de proeven, maar dit heeft voorspelbaar weinig effect op de meer radicale elementen die juist verantwoordelijk zijn voor harde acties.

> Een onderzoeksinstelling geeft aan dat pogingen tot infiltratie van de instelling door dierenactivisten worden ondernomen. Als gevaar van een dergelijke infiltratie wordt gezien dat bepaalde zaken in een laboratorium in scene worden gezet en dat hier vervolgens negatief over gepubliceerd wordt.[57]

5.4 De veiligheidsketen toegepast op organisatieveiligheid

De voornaamste risico op het gebied van organisatieveiligheid die door de geënquêteerde hogescholen en universiteiten zijn genoemd, zijn in de voorgaande paragrafen de revue

[56] A.J. Jacobi, 'Bioterrorisme in Nederland', in: Infectieziektenbulletin, jaargang 14, nr. 3
[57] Vertrouwelijk interview.

gepasseerd. In deze paragraaf zullen aan de hand van de veiligheidsketen verschillende aandachtspunten voor risico- en crisismanagement binnen het domein organisatieveiligheid worden gepresenteerd. Deze aandachtspunten zijn deels afgeleid van 'best practices' die de instellingen zelf via de enquêtes hebben teruggekoppeld. In de Hoger Onderwijs Veiligheidsaudit in bijlage I zijn de aandachtspunten weergegeven per benoemd risico binnen dit domein.

Pro-actie en preventie

- De instelling heeft de organisatierisico's geïnventariseerd en geanalyseerd in een RI&E die breder kijkt dan alleen de 'reguliere' arbo-risico's;
- De instelling heeft een (anoniem) meldingsysteem voor 'verdachte zaken' en incidenten, analyse dient om microtrends binnen de instelling te onderkennen;
- De instelling heeft een integriteitsbeleid en oefent toezicht uit op de naleving ervan (voorlichting aan medewerkers en studenten, controle en sanctionering);
- De instelling leeft bestaande regelgeving na (uitvoering, controle);
- De instelling bevordert het besef van normen en waarden door middel van voorlichting en discussie met medewerkers en studenten;
- De instelling gaat diefstal en fraude tegen door het invoeren van een brede vorm van 'clean desk policy': zorg voor de staat waarin de werkplek wordt achtergelaten verminderd risico's;
- De instelling neemt de nodige technische maatregelen (zoals cameratoezicht, sprinklerinstallaties en geschikte back-up systemen) om inbraak- en brandrisico's te verkleinen;
- De instelling initieert overleg met relevante externe partijen (zoals vergunningverleners en verzekeraars);
- De instelling wisselt kennis uit met collega-instellingen.

Preparatie

- De instelling draagt zorg van een adequaat opleidingsniveau van BHV'ers en EHBO'ers;
- De instelling organiseert regelmatig ontruimingsoefeningen met personeel en studenten om hen voor te bereiden op incidenten en tevens de alertheid te vergroten;

- De instelling test met regelmaat de backup-faciliteiten.
- De instelling heeft draaiboeken ontwikkeld voor veel voorkomende organisatierisico's als inbraak en brand;
- De instelling wisselt kennis uit met collega-instellingen;
- De instelling initieert overleg en afstemming met relevante externe partijen die een rol spelen bij incidenten;

Respons

- De instelling zet de eigen opgeleide BHV-ers en EHBO-ers in bij incidenten;
- De instelling vormt een tactisch en strategisch coördinatieteam voor interne en externe afstemming van de activiteiten in deze fase;
- De instelling informeert studenten, medewerkers en relaties over het incident en de genomen maatregelen;
- De instelling betrekt waar mogelijk en nuttig (vertegenwoordigers van) de studentenpopulatie en medewerkers bij besluitvorming in de responsfase.

Herstel

- De instelling doet aangifte bij ernstige incidenten;
- De instelling coördineert de activiteiten in de herstelfase op tactisch en strategisch niveau;
- De instelling evalueert ernstige voorvallen, met als doel van het incident te leren opdat dergelijke voorvallen in de toekomst binnen de eigen of andere instellingen kunnen worden voorkomen;
- Evaluaties leiden derhalve binnen de instelling tot het bijstellen van de risicoanalyses en het sociaal veiligheidsbeleid;
- De instelling draagt zorg voor begeleiding of doorverwijzing van medewerkers of medestudenten die na een incident (psychosociale) zorg behoeven. Hiertoe wordt samenwerking met externe partijen gezocht.

HOOFDSTUK 6
HOGER ONDERWIJS ALS KENNISBEHEERDER

6.1 Inleiding

De kerntaak van het hoger onderwijs en het wetenschappelijk onderzoek is het verwerven, beheren en verspreiden van kennis. Hiertoe is een scala aan verschillende faciliterende voorzieningen aanwezig voor studenten en docenten. Via onder andere toegang tot intranet, internet, beschikbare computerzalen, bibliotheken, colleges en werkgroepen kan kennis verzameld, geanalyseerd en toegepast worden.

Instellingen proberen laagdrempelig te zijn in het toegangsregime tot de aanwezige kennis voor studenten en docenten. Tegelijkertijd lopen instellingen het risico dat misbruik wordt gemaakt van aangeboden voorzieningen. Dit hoofdstuk gaat nader in op de risico's die de instellingen lopen in hun functie als kennisbeheerder. Het beleid rond kennisveiligheid heeft daarbij twee elementen: a) het misbruik van de systemen waar de kennis wordt ontwikkeld, opgeslagen en verwerkt (onder meer de computernetwerken) en b) het misbruik van kennis als 'product' waarmee de onderwijssector werkt.

Op voorhand is duidelijk dat de balans tussen ongehinderde kennisoverdracht en veiligheid een precaire is. Een te zware nadruk op beveiliging brengt de kerntaak van het hoger onderwijs en het wetenschappelijk onderzoek in het geding. Zo is bijvoorbeeld het ontoegankelijk maken van internet op instellingen ondenkbaar gezien de grote negatieve gevolgen daarvan voor het verspreiden en verzamelen van kennis. Andersom geldt echter ongeclausuleerde toegang tot faciliteiten ernstige veiligheidsrisico's oplevert. Het zonder beveiliging toegankelijk stellen van internet betekent eenvoudige toegang voor virussen, wormen en andere elektronisch overlast, maar biedt ongeautoriseerde personen ook de kans om misbruik van de beschikbare voorzieningen te maken.

In dit hoofdstuk zullen de risico's verder worden onderverdeeld naar risico's met een primair interne oorzaak en risico's met een primair externe oorzaak.

Aan de hand van de methodiek van de veiligheidsketen zal worden ingegaan op de mogelijkheden die de onderwijsinstellingen hebben om risico's en incidenten op het gebied van organisatieveiligheid te beheersen. In het hoofdstuk zullen verder ervaringen van instellingen binnen het hoger onderwijsinstellingen worden gepresenteerd.

Hieronder zullen als eerste enkele algemene conclusies vanuit de enquête en interviews worden gepresenteerd.

Algemeen

Instellingen melden zonder uitzondering een toegenomen aandacht in de afgelopen jaren voor beveiliging van de ICT-systemen. In Colleges van Bestuur is er bij veel instellingen een portefeuillehouder ICT die aandacht besteedt aan beveiligingsvraagstukken. Wel wordt door opgemerkt door operationeel verantwoordelijken voor deze beveiliging dat hoewel de aandacht is toegenomen, de problemen harder lijken te groeien. Waar voorheen ICT-incidenten relatief zeldzaam waren, zijn ze nu aan de orde van de dag. De mate waarin systemen beveiligd zijn varieert per instelling. Diverse instellingen hebben of werken aan een beleidsplan ICT-beveiliging. Zo heeft de KUN een aparte beveiligingscoördinator die onder meer tot taak heeft het ICT-beveiligingsbeleid gestalte te geven, het doen uitvoeren van security audits en het ontwikkelen van een beleidsplan voor ICT beveiliging. De UvA werkt momenteel aan het project 'Beveiligingsbeheer'. Dit richt zich op herziening van regelgeving, communicatie en voorlichting, uitvoeren van technische maatregelen en het uitvaardigen van technische beveiligingsrichtlijnen. Andere instellingen beperken zich nog voornamelijk tot het met enige regelmaat updaten of installeren van nieuwe technische systemen (met name firewalls, anti-virusssystemen en virusdetectiesystemen).

Risicoperceptie instellingen en ontwikkelingen

'ICT' dringt steeds verder door in het onderwijs. Elektronische leeromgevingen winnen aan populariteit en moeten het liefst wereldwijd toegankelijk zijn. Door deze toenemende penetratie van ICT-systemen neemt de kwetsbaarheid toe van instellingen toe. Dit legt een steeds grotere claim op beveiligingseisen rond autorisatie, authenticatie en

afscherming/versleuteling. Instellingen onderkennen dit toenemende risico in verschillende mate. Informatiebeveiliging vergt in ieder geval een steeds groter deel van het ICT-budget. Gebruikers en budgethouders van ICT-systemen zien echter geen meetbaar resultaat van deze toenemende kosten. Het feit dat er niet 'gehackt' wordt, is immers geen meetbare eenheid. Bij de afwezigheid van incidenten ontstaat er dan weer druk op het beschikbare budget.

Melding en registratie van incidenten
De registratie en analyse van ICT-incidenten wordt door de meeste instellingen ter hand genomen. Wel is een duidelijk verschil zichtbaar in de professionaliteit van de aanpak van verschillende instellingen. Voorlopers hebben centrale Computer Emergency Response Teams (CERT) die zijn ingericht om incidenten te verhelpen, registreren en analyseren.

Risicoscan
Een minderheid van de instellingen kent een systematische risicoanalyse van kennisveiligheidsrisico's (waaronder ICT-risico's). Eenderde van de bevraagde instellingen geeft aan hiermee net gestart te zijn of op korte termijn te starten.

Samenwerking met interne en externe partijen
Samenwerking met externe partijen lijkt voor de meerderheid van de instellingen niet aan de orde op het gebied van kennisveiligheid. Voor de hand liggende organisaties waar incidenten op het gebied van de kennisveiligheid kunnen worden gemeld of waar advies kan worden verkregen, kent men niet.

Studenten en docenten worden vooral betrokken bij kennisveiligheid door het stimuleren van het risicobewustzijn van deze eindgebruikers. Zij worden gewezen op het gebruik van toegangscodes en op gedragsregels. Enkele instellingen besteden actief aandacht aan risicobewustzijn via campagnes. Het meest bekende voorbeeld is de gezamenlijke campagne 'www.laatjenietpakken.nl'. Middels deze campagne worden gebruikers gewaarschuwd voor gevaren van internet en gemaand om beveiligingssoftware te gebruiken, back ups van bestanden te maken en wachtwoorden vertrouwelijk te behandelen.

Laat je niet pakken! is een campagne van SURFnet in samenwerking met hogescholen, universiteiten en onderzoeksinstellingen in Nederland. Doel van de campagne is het verhogen van het bewustzijn rondom het beveiligen van computers en netwerken. Veel schade is namelijk te voorkomen door bewust met een pc om te gaan. SURFnet is de internetprovider voor hoger onderwijs en onderzoek in Nederland. Ruim 500.000 studenten en onderzoekers maken dagelijks gebruik van het netwerk en de diensten van SURFnet.[58]

6.2 Kennisveiligheidsrisico's met een primair externe oorzaak

Vormen bedreigingen van de ICT-infrastructuur : digitaal activisme en hacktivisme
De verschillende vormen van bedreigingen van de ICT-infrastructuur van instellingen kunnen gecategoriseerd worden in 'digitaal activisme' en 'hacking':

Digitaal activisme: Digitaal activisme kenmerkt zich door gebruik van internet of intranet voor een bepaalde zaak. De volgende voorbeelden zijn relevant voor instellingen binnen het hoger onderwijs en het wetenschappelijk onderzoek:

- *Publicatiemedium*: Activisten gebruiken internet veelvuldig als publicatiemedium. Bekende voorbeelden zijn het opzetten van anti-websites die zich richten op specifieke bedrijven (bijv. microsoftsucks.com en nikewages.com) of industrieën (bijv. websites van anti-globalisten tegen gen-technologie). Duizenden websites en specialistische nieuws- of discussiegroepen stellen tips en gereedschap voor hacking beschikbaar. Instellingen kunnen onbewust dergelijke activisten 'hosten'.

- *Coördinatie van acties*: Via internet is het mogelijk een grote groep activisten aan te sturen en in korte tijd te mobiliseren. Hierin zijn 'online' en 'offline' acties te onderscheiden. In het geval van 'offline' acties geldt internet als communicatiemiddel en vindt de actie 'gewoon' op straat plaats. Zo werd bij de scholierendemonstratie van 6

[58] www.laatjenietpakken.nl

december 1999 in Den Haag via internetsites opgeroepen tot staking. Uiteindelijk hebben ongeveer 20.000 scholieren hieraan gehoor gegeven.[59] 'Online' acties worden volledig elektronisch uitgevoerd. De meest voorkomende actievorm betreft e-mailacties. Deze zijn gericht op het aanhoudend bestoken van instanties of personen met e-mailberichten om de besluitvorming te beïnvloeden. Regelmatig komt het voor dat traditionele acties, als demonstraties en protestmarsen, ondersteund worden door digitale acties.60

- *E-mailbommen*: Het automatisch tegelijk of kort na elkaar zenden van grote hoeveelheden (duizenden) e-mails zorgt voor een blokkade van het e-mailadres van de adressant. Wraakacties of protestacties liggen vaak ten grondslag aan deze vorm van hacktivisme. Eind maart 1999, gedurende het Kosovo-conflict, raakte de emailserver van de NAVO verzadigd doordat dagelijks 2000 e-mailberichten werden gestuurd naar deze server. Tegenwoordig gaat het bij dergelijke acties om honderduizenden mails per dag.

- *Web sit-ins, virtuele blokkades en Denial of Service (DoS)*: Door massaal bezoek van een bepaalde website of vraag om toegang tot een beveiligd deel daarvan kan een actiegroep andere personen verhinderen de site te bezoeken. Hierdoor ontstaat een virtuele blokkade.

  Op 21 december 1995 vond de eerste grootschalige websit-in plaats. De groep Strano Network riep deelnemers op om hun browsers op een vooraf afgesproken tijdstip een uur lang op bepaalde overheidssites te richten. Verschillende sites raken hierdoor onbereikbaar. In september 1998 ging de groep Electronic Disturbance Theater (EDT) verder op dit pad van elektronische burgerlijke ongehoorzaamheid. Ze organiseerden een serie van Web sit-ins tegen de website van onder meer de Mexicaanse president Zedillo, Clinton's White House website, het Pentagon, de Mexicaanse beurs en de beurs in Frankfurt. Het doel van de actie was een solidariteitsbetuiging aan de Mexicaanse Zapatistas. EDT zette ter ondersteuning speciale websites op waar men programmatuur kon downloaden om sites automatisch iedere paar seconden te bezoeken. EDT schat dat mondiaal 10.000 mensen mee hebben gedaan aan de sit-in op 9 september 1998. De sit-in

[59] M.J.A. Borgers-Roozen, T.J. Golder, M.J. Klaver, G.J. van Rossum, Informatieoorlog: over de schaduwkanten van de informatiemaatschappij, Stichting Maatschappij en Onderneming, Den Haag, 2000, p. 39
[60] M.J.A. Borgers-Roozen, T.J. Golder, M.J. Klaver, G.J. van Rossum, Informatieoorlog: over de schaduwkanten van de informatiemaatschappij, Stichting Maatschappij en Onderneming, Den Haag, 2000, p. 42

leverde 600.000 hits per minuut per doel op. Het is vooralsnog onduidelijk of Web sit-ins illegaal zijn.

Hacking: Het begrip 'hacking' duidt op handelingen waarbij een persoon probeert toegang te verkrijgen tot beveiligde delen van de ICT-infrastructuur of tot andere computers. Een hacking-actie hoeft daarmee niet per definitie te leiden tot schade, maar kan dat wel wanneer de hacker bestanden of functies van het ICT-systeem wijzigd. De afgelopen jaren zijn er opzienbarende pogingen van hackers geweest om kwetsbare (internationale) communicatienetwerken lam te leggen.[61]

- *Webhacks en computerinbraken*: Een 'webhack' is het kraken van een website en het plaatsen van alternatieve teksten en afbeeldingen. In sommige gevallen willen hackers enkel aantonen dat websites 'gekraakt' zijn, zonder moedwillig informatie te wijzigen. Een voorbeeld van deze vorm van webhacks zijn de websites waarop de zinsnede *'All your base are belong to us'* wordt achtergelaten. Deze zin, afkomstig uit het computerspel Zero Wing waarbij de Engelse vertaling was overgelaten aan een Aziatische firma, wordt door hackers met regelmaat als ludieke 'graffiti' achtergelaten. In Nederland viel de tekst onder meer te lezen op de sites van de Nederlandse Spoorwegen en postcode.nl.[62] Minder ludiek was een poging in juni 1998, waarbij een internationale groep hackers – genaamd Milw0rm – erin slaagde om de site van India's Bhabha Atomic Research Center te kraken en protestleuzen te plaatsen. De daders bleken zes hackers in de leeftijd van 15-18 jaar uit de VS, Engeland, Nederland en Nieuw Zeeland te zijn.[63]

- *Computervirussen, wormen en trojan-horses*: Zowel computervirussen als wormen en trojan-horses worden verspreid over netwerken en zijn kwaadwillende codes die computers infecteren. Een worm is een autonoom software-element dat zichzelf verspreidt. Een virus bevestigt zichzelf aan andere bestanden en wordt verspreid door de onwetende gebruiker. Een trojan-horse heft de beveiliging van computersystemen op. Het

[61] D.E. Denning, 'Activism, Hacktivism, and Cyberterrorism; The Internet as a Tool for Influencing Foreign Policy', in: J. Arquilla, D. Rohnfeldt, Networks and Netwars: the Future of Terror, Crime and Militancy, RAND, Santa Monica, 2001, p. 241

[62] De website voor de introductie van de Euro werd voorzien van de tekst 'All your euros are belong to us'.

[63] D.E. Denning, 'Activism, Hacktivism, and Cyberterrorism; The Internet as a Tool for Influencing Foreign Policy', in: J. Arquilla, D. Rohnfeldt, Networks and Netwars: the Future of Terror, Crime and Militancy, RAND, Santa Monica, 2001, p. 241

grensvlak tussen de drie verschillende vormen is niet altijd goed aan te geven. De specifieke kenmerken overlappen bij verschillende soorten wormen en virussen.[64]

Bekende voorbeelden van wormen en virussen zijn Sasser, Melissa en I Love You. Deze virussen zorgden voor miljarden euro's aan geleden schade. De schade voor de ontvanger van de worm of het virus is meestal verpakt in een bijlage (attachment). Deze kan bestaan uit onder meer platte tekst, figuren of foto's. De schade die wordt aangericht kan bestaan uit het volledig disfunctioneren van de computer, het vernietigen van bestanden of het onbereikbaar worden van de harde schijf. Het voorkomen van het ontvangen van virussen of wormen – of het tijdig detecteren – is zeer gecompliceerd, omdat telkens nieuwe virussen worden ontwikkeld, de systemen zeer intensief worden gebruikt en virusdetectiesystemen en de update- en upgrademogelijkheden van bijvoorbeeld WindowsUpdate niet altijd up-to-date worden gehouden.[65]

Kennisverzameling voor oneigenlijke doelen

Vrijwel alle onderwijsinstellingen hanteren een 'open-deur beleid'. Mensen die kennis willen opdoen zijn welkom deel te nemen aan het onderwijs. De selectiecriteria voor studenten zijn vooropleiding en voldoende financiële middelen. Van een screening op veiligheidsgebied is geen sprake. Hetzelfde geldt in algemene zin voor docenten en wetenschappelijke onderzoekers.

Voor veel opleidingen is hiertoe ook geen noodzaak omdat de gedoceerde kennis geen vertrouwelijk karakter heeft. Er zijn echter uitzonderingen. De faculteiten en onderzoeksinstellingen die op natuurkundig, scheikundig of medisch gebied onderwijs aanbieden en onderzoek laten verrichten, zijn interessant voor landen, groeperingen of bedrijven die kennis willen misbruiken of stelen.

[64] D.E. Denning, 'Activism, Hacktivism, and Cyberterrorism; The Internet as a Tool for Influencing Foreign Policy', in: J. Arquilla, D. Rohnfeldt, Networks and Netwars: the Future of Terror, Crime and Militancy, RAND, Santa Monica, 2001, p. 278

[65] D.E. Denning, 'Activism, Hacktivism, and Cyberterrorism; The Internet as a Tool for Influencing Foreign Policy', in: J. Arquilla, D. Rohnfeldt, Networks and Netwars: the Future of Terror, Crime and Militancy, RAND, Santa Monica, 2001, p. 283

Bij TNO is men constant beducht voor het weglekken van kennis die misbruikt zou kunnen worden voor commerciële doeleinden of het vervaardigen van massavernietigingswapens. Gezien de defensiehistorie is dit begrip voor een goede veiligheidscultuur niet verwonderlijk. TNO kent aangewezen veiligheidsmanagers met een controle- en instructiefunctie. Op universitaire onderzoeksinstellingen is het veiligheidsbesef nog veel minder aanwezig.

In Nederland (of Europa) is er nog geen wetgeving over de wijze waarop men geacht wordt om te gaan met gevoelige informatie en kennis. In de VS kent men wel dergelijke regelgeving voor bijvoorbeeld de omgang met biologische agentia zoals antrax.

'In de afgelopen jaren zijn in verschillende landen Chinese studenten en wetenschappers die (tijdelijk) in het westen studeren of werken, betrapt op inlichtingenactiviteiten. Zij verbleven meestal in het westen in het kader van officiële Chinese overheidsprogramma's voor kennisintensivering. Dit zijn openbare programma's die beogen een inhaalslag voor de Chinese kenniseconomie te realiseren. De deelname aan zulke programma's blijkt soms als cover te dienen. Zo slaagden bijvoorbeeld enkele jaren geleden twee Chinese studenten in de VS erin, tijdens hun studieverblijf informatie te verzamelen voor de productie van een chemische substantie die wordt gebruikt in sensoren en wapens. Het lukte hen de verworven informatie door te spelen naar China voor hun activiteiten ontdekt werden.' [66]

Een bekend Nederlands voorbeeld betreft Khan, de man die zichzelf de 'vader van de Pakistaanse atoombom' noemt. Hij deed zijn kennis grotendeels op via een studie en een stageproject in Almelo waar hij in de jaren zeventig bij een uranium-opwerkingsfabriek werkte. Hij sloot zijn stage af met de diefstal van de technologie van zijn stage-werkgever.[67]

[66] AIVD, Spionage en veiligheidsrisico's; actueel, onzichtbaar en divers, 2004, p. 10.
[67] AIVD, Profileratie van massavernietigingswapens; Risico's voor bedrijven en wetenschappelijke instellingen, 2003, p. 9.

6.3 Kennisveiligheidrisico's met een primair interne oorzaak

Misbruik van ICT-faciliteiten

In de perceptie van instellingen is het grootste risico's voor informatie-communicatie technologie misbruik door studenten en medewerkers. Onder misbruik wordt verstaan het gebruiken van ICT-systemen op een andere wijze dan door de instelling bedoeld. Dit kan het verspreiden van opruiende berichten of aanstootgevende foto's zijn, maar ook het bewust vernietigen of vervuilen van bestanden, het onbereikbaar maken van systemen en het ongeautoriseerd gebruiken van toegangscodes. De mogelijkheden tot misbruik hangen sterk samen met de beveiliging.

> Een bijzonder risico is de mogelijkheid van ongeautoriseerde toegang tot de ICT-systemen. Met name het werken op afstand en de ontwikkeling naar steeds meer draadloze verbindingen maken een sluitende beveiliging steeds moeilijker. Uit de reacties van respondenten wordt duidelijk dat het belang van afdoende beveiliging niet gelijk oploopt met de ontwikkelingen en eisen op het gebied van gebruikersgemak. In de praktijk blijkt overigens dat diverse bedrijven en instellingen zelfs de minimale encryptiebeveiligingen voor WiFi-toepassingen niet doorvoeren, waardoor externen zonder autorisatie eenvoudig draadloos toegang kunnen krijgen tot computernetwerken.[68]

Operationeel verantwoordelijken voor de beveiliging van ICT-systemen binnen de instellingen waarschuwen voor een beperkt veiligheidsbewustzijn bij de eindgebruiker; gebruiksgemak wint het van veiligheid. Hoewel de ICT-afdelingen in de meeste gevallen informatie over beveiliging geven (algemene voorwaarden voor gebruik e.d.), wordt dat door gebruikers eerder als lastig en onnodig ervaren dan als welkome informatie.

> Een ander bijzonder risico is de illegale verspreiding van software via instellingsnetwerken. Zogenaamde 'warez-groepen' verspreiden op grootschalige en georganiseerde wijze de zogenaamde 'cracks' of 'crackz', waarmee de auteursrechtelijke bescherming van software wordt omzeild. Via peer-to-peernetwerken als Bittorrent en Kazaa wordt auteursrechtelijk beschermd materiaal zoals software, muziek en films uitgewisseld. Universiteitsnetwerken zijn

– vanwege de snelle verbindingen – bij computergebruikers zeer geliefd om illegaal te down- en uploaden. Op 21 april 2004 viel de FIOD-ECD bij diverse studentenhuizen in Utrecht, Enschede en Delft binnen om onderzoek te doen naar het grootschalig verspreiden van illegale software. Het onderzoek werd op verzoek van de afdeling Cybercrime van het Amerikaanse ministerie van Justitie gedaan. Ook in zeven andere landen werden tegelijkertijd huiszoekingen verricht. In verschillende studentenwoningen zijn apparatuur en documenten in beslag genomen.

De Twentse universiteit heeft een van de snelste computernetwerken van Nederland en is daarmee aantrekkelijk voor computerliefhebbers van goede, maar ook van kwade wil. Dat blijkt – behalve in bovenstaande geval – ook eind 2001. De TU Twente raakt in opspraak als blijkt dat het netwerk van de universiteit de Europese spil in de warez-handel is. In november 2001 worden enkele personen bij invallen op de campus aangehouden en hun computerapparatuur in beslag genomen. Ze worden verdacht van georganiseerde criminaliteit

Kennisverlies door calamiteiten

De gevolgen van brand in (delen van) het complex heeft veel te maken met het fysieke veiligheidsaspect van organisatieveiligheid. Het voorbereid zijn op brandontwikkeling is een vereiste om tot adequate bestrijding over te kunnen gaan. Brandblussers, rookmelders, brandvertragende materialen zijn hierbij van groot belang. Voor kennisveiligheid is brand – of een ander risico dat fysieke schade oplevert – een een grote bedreiging. De vernietiging van computers, databases en/of bibliotheken betekent een soms niet te herstellen schadepost als de opgeslagen kennis verdwenen is.

De al eerder aangehaalde grote brand in het rekencentrum van de TU Twente in november 2003 leidde tot een geschatte materiële schade van 40 tot 50 miljoen euro. Immaterieel was de schade nauwelijks te bevatten; personeel raakte van het ene op het andere moment uniek onderzoeksmateriaal op hun eigen werkkamers kwijt, promovendi verloren onderzoekresultaten en ingeleverde verslagen en tentamens waren verbrand.

[68] Zie onder meer Zembla-uitzending 3 juni 2004 (gearchiveerd op http://www.zembla.tv)

Een zeer belangrijk onderdeel van het onderwijs en onderzoek op hogescholen en universiteiten wordt gevormd door diegenen die kennis ontwikkelen en overbrengen; de docenten, hoogleraren en wetenschappelijk medewerkers. Indien een dergelijke medewerker voor de instelling wegvalt door ziekte of overlijden, kan ervaring en kennis verloren gaan die niet (op korte termijn) te vervangen is, zodat continuïteitsproblemen kunnen ontstaan binnen onderzoek en opleidingen.

Kennisfraude
Kennisfraude door medewerkers of studenten is een bedreiging van de reputatie van instellingen.

Er zijn in Nederland de afgelopen jaren enkele gevallen van mogelijke plagiaat door medewerkers in de media gekomen. De zaak 'Diekstra' leidde in 1996 in Nederland tot veel commotie. Uiteindelijk bleek, na onder zware druk ontslag te hebben genomen, Diekstra onschuldig, maar zijn reputatie en de reputatie van de betreffende universiteit waren wel beschadigd door deze affaire. De affaire leidde tot discussie over de noodzaak van aandacht voor dit risico. 'Het aan de kaak stellen van wangedrag is nuttig en niet laakbaar, lijkt me. Als je wangedrag wilt voorkomen, moet iedereen op vergrijpen verdacht zijn en ze bespreekbaar maken'.[69]

Behalve door medewerkers, kan plagiaat ook door studenten worden gepleegd in essays, werkstukken of scripties.

Een Amerikaans onderzoek wees uit dat bij 122 van de 1500 onderzochte scripties sprake is van plagiaat. Dit werd vastgesteld door middel van een eenvoudig computerprogramma dat zinsneden uit verschillende scripties met elkaar kan vergelijken.[70]

In Nederland vraagt in 2002 de hoofdinspecteur hoger onderwijs naar aanleiding van een onderzoek van zijn Inspectie aandacht voor de grote schaal waarop binnen het hoger onderwijs dergelijke kennisfraude plaatsvindt. Instellingen worden erop gewezen

[69] P. Zandbergen, 'Zaak-Diekstra is testcase', in: UT Nieuws, weekblad van de universiteit Twente, 5 september 1996, jaargang 31, nr. 25

onvoldoende alert te zijn op scriptiefraude.[71] Instellingen in het hoger onderwijs onderschrijven daarop het belang van hard optreden tegen deze vorm van kennisfraude Omdat 'deze vorm van gedrag [..] het wezen van de wetenschapsbeoefening aantast'.[72]

Verschillende instellingen nemen sindsdien maatregelen om scriptiefraude op het spoor te komen. De fraudecontrole valt of staat echter met het aantal beschikbare bestanden waarmee scripties vergeleken kunnen worden en daarom is samenwerking met andere faculteiten noodzakelijk.[73] Deze samenwerking tussen verschillende universiteiten is echter nog niet tot stand gekomen. Evenzeer bestaat er nog geen uniform sanctiebeleid. Wel worden door individuele instellingen zware straffen aangekondigd, zoals uiteindelijk verwijdering van de universiteit of zelfs strafrechtelijke vervolging. Enkele instellingen hebben een gedragscode ontwikkeld met betrekking tot plagiaat.[74]

6.4 De veiligheidsketen toegepast op kennisveiligheid

De voornaamste risico op het gebied van kennisveiligheid die door de geënquêteerde hogescholen en universiteiten zijn genoemd, zijn in de voorgaande paragrafen de revue gepasseerd. In deze paragraaf zullen aan de hand van de veiligheidsketen verschillende aandachtspunten voor risico- en crisismanagement binnen het domein kennisveiligheid worden gepresenteerd. Deze aandachtspunten zijn deels afgeleid van 'best practices' die de instellingen zelf via de enquêtes hebben teruggekoppeld. In de Hoger Onderwijs Veiligheidsaudit in bijlage I zijn de aandachtspunten weergegeven per benoemd risico binnen dit domein.

Preventie en proactie

- De instelling heeft de organisatierisico's geïnventariseerd en geanalyseerd;

[70] Zie: 'De bedrieger bedrogen', op: http://www.edusite.nl/edusite/nieuws/1475 (bron: The Washington Post)
[71] Zie: http://docenten.nrc.nl/nieuwsbrief/archief/2002/10.html
[72] Citaat van de rector magnificus van de Universiteit van Tilburg in:'Plagiaat en spieken strafrechtelijk vervolgen', op Univers Online (http://www.uvt.nl/univers/nieuws/0203/08/fraude.html) , 17 oktober 2002
[73] http://www.uvt.nl/faculteiten/frw/trom-l/j4n11/
[74] Zie: http://e-learning.surf.nl/e-learning/artikelen/773

- De instelling heeft een (anoniem) meldingsysteem voor ‘verdachte zaken’ en incidenten, analyse dient om microtrends binnen de instelling te onderkennen;
- De instelling heeft een kennisintegriteitsbeleid, en oefent toezicht uit op de naleving ervan (voorlichting aan medewerkers en studenten, controle en sanctionering);
- De instelling bevordert het besef van normen en waarden bij medewerkers en studenten middels voorlichting en discussie;
- De instelling gaat kennisdiefstal en -fraude tegen door het invoeren van een brede vorm van ‘clean desk policy’: zorg voor de staat waarin de werkplek wordt achtergelaten verminderd risico’s;
- De instelling neemt de nodige technische en organisatorische maatregelen (zoals cameratoezicht, geschikte back-up systemen en screening van personeel) om de kans op en het effect van kennisdiefstal en kennisverlies te verkleinen;
- De instelling neemt de nodige technische en organisatorische maatregelen (zoals legitimatieplicht) om de kans op kennisfraude (onder studenten) te verkleinen;
- De instelling wisselt kennis uit met collega-instellingen;
- De gebruikte ICT-systemen voldoen aan vastgestelde veiligheidseisen, virusdetectie, anti-virusprogramma’s en software-updates worden regelmatig aangepast;
- Informeren (verplicht) van eindgebruikers over het veilig gebruik van de systemen, waarbij gebruik wordt gemaakt van de informatie uit het project KWINT (Kwetsbaarheid op Internet) van het Ministerie van Economische Zaken;
- Ontwikkelen van sanctiebeleid voor gebruikers die zich niet aan veiligheidsvoorschriften houden op basis van de Code voor Informatiebeveiliging (ISO 17799) van het ministerie van Economische Zaken, ministerie van Verkeer en Waterstaat en NNI; [75] [76]
- Ontwikkelen van een ‘vertrouwelijkheidsverklaring’ ter ondertekening voor medewerkers en studenten voor instellingen die met gevoelige informatie werken;
- De instelling wijst medewerkers binnen relevante delen van de instelling op de risico’s van het misbruik van kennis, bijvoorbeeld op basis van de brochures over ongewenste inlichtingenactiviteiten in Nederland ‘Spionage en veiligheidsrisico’s’ (ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2004) en over de proliferatie van

[75] Zie het initiatief http://www.informatiebeveiliging.nl van het NPC (Nationaal Platform Criminaliteitsbeheersing) en ECP.nl (Platform voor eNederland)
[76] Een herziening van de code is volgens het Nederlands Normalisatie Instituut gepland voor 2004/2005

massavernietigingswapens (ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2003) ;

- De instelling ontwikkelt selectiecriteria voor de toelating van (buitenlandse) studenten en wetenschappelijk medewerkers tot relevante opleidingen en delen van de instelling op basis van het Handboek Integriteitsonderzoek (ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2003). [77] Hiertoe kan overleg met de AIVD worden gezocht.

Preparatie

- De instelling oefent met regelmaat backup-faciliteiten en personeel.
- De instelling heeft draaiboeken ontwikkeld voor veel voorkomende kennisveiligheidsrisico's als kennisfraude en ICT-problemen;
- De instelling wisselt kennis uit met collega-instellingen;
- De instelling initieert overleg en afstemming met relevante externe partijen die een rol spelen bij incidenten;
- De instelling heeft een ICT- servicedesk met voldoende capaciteit om ICT-risico's te beheersen en met afspraken met specialisten op het gebied van ICT-ondersteuning;
- De instelling initieert overleg en afstemming met relevante externe partijen (zoals de politie) over de voorbereiding op kennisveiligheidsincidenten.

Respons

- De instelling activeert haar servicedesk bij ICT-incidenten;
- De instelling vormt een tactisch en strategisch coördinatieteam voor interne en externe afstemming van de activiteiten (zoals persvoorlichting) in deze fase;
- De instelling informeert studenten en medewerkers over het incident en de genomen maatregelen;
- De instelling betrekt waar mogelijk en nuttig (vertegenwoordigers van) de studentenpopulatie en medewerkers bij besluitvorming in de responsfase;
- De instelling kan bij incidenten besluiten de politie in te schakelen, deze kan op haar beurt besluiten tot het inschakelen van de AIVD.

[77] Zie ook http://www.minbzk.nl/contents/pages/2056/Deel1.pdf

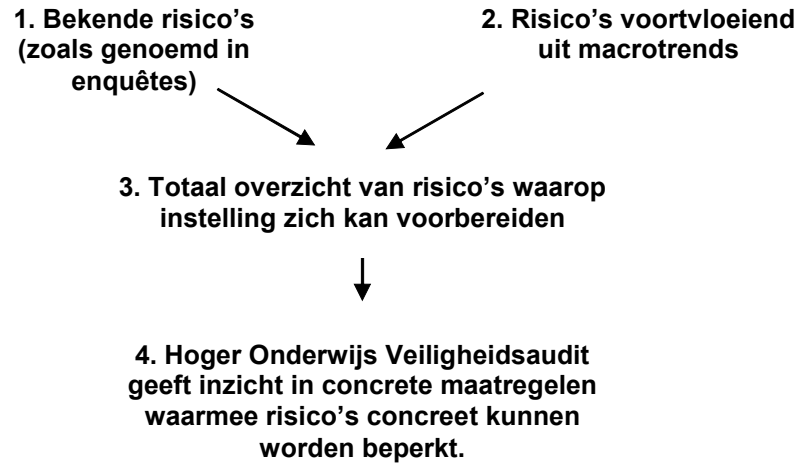
Herstel

- De instelling doet aangifte bij ernstige incidenten;
- De instelling coördineert de activiteiten in de herstelfase op tactisch en strategisch niveau;
- De instelling evalueert ernstige voorvallen, met als doel van het incident te leren opdat dergelijke voorvallen in de toekomst binnen de eigen of andere instellingen kunnen worden voorkomen;
- Evaluaties leiden derhalve binnen de instelling tot het bijstellen van de risicoanalyses en het kennisveiligheidsbeleid;

BIJLAGE I
HOGER ONDERWIJS VEILIGHEIDSAUDIT

Als handreiking voor de instellingen in het hoger onderwijs en het wetenschappelijk onderzoek is in dit onderzoek een auditkader ontwikkeld waaraan de instellingen hun eigen veiligheidsbeleid kunnen ijken.

Het auditkader is gevormd door de bekende risico's te combineren met de risico's die volgen uit de onderscheiden macrotrends. Deze combinatie geeft een totaal overzicht van de risico's waarmee instellingen geconfronteerd worden. Aan de risico's zijn vervolgens concrete maatregelen gekoppeld die instellingen kunnen nemen om deze risico's te beheersen.



Zoals in de gehele rapportage wordt ook in het auditkader onderscheid gemaakt tussen de drie risicodomeinen sociale veiligheid, organisatieveiligheid en kennisveiligheid. Het auditkader kent verder twee delen: het eerste deel is gericht op de bestuurlijk verantwoordelijken voor het veiligheidsbeleid van de instelling, het tweede deel op de operationeel verantwoordelijken voor de verschillende risicodomeinen.

I. Auditkader voor het bestuur

1. Veiligheidsbeleid op gebied van sociale veiligheid

Onderwerp 1:	***Sociale veiligheid***
Norm 1:	*De instelling heeft beleid voor sociale veiligheid geformuleerd. Voor dit sociale veiligheidsbeleid is een beleidscyclus ingericht.*

Aspecten 1:

- Er is vastgesteld sociaal veiligheidsbeleid voor de instelling
- Er is een portefeuillehouder binnen het bestuur voor het onderwerp sociale veiligheid (deze onderhoudt onder andere het contact over dit onderwerp met koepelorganisaties)
- Er is budget voor sociaal veiligheidsbeleid
- Jaarlijks wordt een sociale risico-analyse gemaakt waaraan het sociale veiligheidsbeleid wordt getoetst
- Jaarlijks worden te nemen maatregelen op het gebied van sociale veiligheid geprioriteerd
- Over de uitvoering van het beleid wordt jaarlijks gerapporteerd aan het bestuur
- Met medewerkers en studenten (bijvoorbeeld via Faculteitsraden) wordt het beleid jaarlijks geëvalueerd
- Het sociale veiligheidsbeleid is bekend binnen de instelling en afgestemd met externe partners (politie, gemeente, psycho-sociale hulpverlening e.d.)

2. Veiligheidsbeleid op gebied van organisatieveiligheid

Onderwerp 2:	***Organisatieveiligheid***
Norm 2:	*Het bestuur heeft beleid voor organisatieveiligheid geformuleerd. Een uitgangspunt is daarbij dat de instelling aan de eisen voldoet van de vergunningen die omtrent organisatieveiligheid aan de instellingen worden gesteld. Het beleid heeft een beleidscyclus.*

Aspecten 2:

- Er is vastgesteld organisatieveiligheidsbeleid voor de instelling
- Er is een portefeuillehouder binnen het bestuur voor het onderwerp organisatieveiligheid (deze onderhoudt onder andere het contact over dit onderwerp met koepelorganisaties)
- Er is budget voor organisatieveiligheidsbeleid
- Jaarlijks wordt een risico-analyse gemaakt waaraan het organisatieveiligheidsbeleid wordt getoetst
- Jaarlijks worden te nemen maatregelen op het gebied van organisatieveiligheid geprioriteerd
- Over de uitvoering van het organisatiebeleid wordt jaarlijks gerapporteerd aan het bestuur
- Met medewerkers en studenten (bijvoorbeeld via Faculteitsraden) wordt het beleid jaarlijks geëvalueerd
- Het organisatieveiligheidsbeleid is bekend binnen de instelling en afgestemd met externe partners (vergunningverleners, verzekeraars e.d.)

3. Veiligheidsbeleid op gebied van kennisveiligheid

Onderwerp 3:	***Kennisveiligheid***
Norm 3:	*Het bestuur heeft beleid voor kennisveiligheid geformuleerd. Men voldoet aan de eisen van ISO-17799. Het beleid heeft een beleidscyclus.*

Aspecten 3:

- Er is vastgesteld kennisveiligheidsbeleid voor de instelling
- Er is een portefeuillehouder binnen het bestuur voor het onderwerp kennisveiligheid (deze onderhoudt onder andere het contact over dit onderwerp met koepelorganisaties)
- Er is budget voor kennisveiligheidsbeleid
- Jaarlijks wordt een risico-analyse gemaakt waaraan het kennisveiligheidsbeleid wordt getoetst
- Jaarlijks worden te nemen maatregelen op het gebied van kennisveiligheid geprioriteerd
- Over de uitvoering van het kennisveiligheidsbeleid wordt jaarlijks gerapporteerd aan het bestuur
- Met medewerkers en studenten (bijvoorbeeld via Faculteitsraden) wordt het beleid jaarlijks geëvalueerd
- Het kennisveiligheidsbeleid is bekend binnen de instelling en afgestemd met externe partners

II. Auditkader voor operationeel verantwoordelijken

1. Operationeel auditkader op het gebied van sociale veiligheid

Onderwerp 1A:	**Algemeen**
Norm 1A:	*Het sociaal veiligheidsbeleid is uitgewerkt in een concreet uitvoeringsplan. Hierin is de uitvoering van maatregelen geprioriteerd en van budget voorzien. Een veiligheidsmanager is verantwoordelijk voor de uitvoering van de maatregelen. Incidenten op het gebied van sociale veiligheid worden centraal binnen de instelling geregistreerd en geanalyseerd. Analyses leiden tot aanbevelingen voor het verder terugdringen van sociaal onveilige situaties.*

Aspecten 1A:

- Er is een concrete uitwerking van het sociaal veiligheidsbeleid
- Maatregelen op gebied van sociale veiligheid zijn geprioriteerd en van budget voorzien
- Incidenten op gebied van sociale veiligheid worden geregistreerd en geanalyseerd
- Over uitvoering van maatregelen wordt gerapporteerd aan het bestuur
- Een tactisch en strategisch coördinatieteam coördineert tijdens ernstige incidenten de interne en externe afstemming van de activiteiten
- De instelling wisselt kennis uit met collega-instellingen

Onderwerp 1B:	**Sociale macrotrend 'toenemende agressie en geweldpleging'**
Norm 1B:	*Uitgangspunt: er wordt geen geweld getolereerd binnen de eigen instelling. Binnen de instelling worden daartoe passende maatregelen genomen om geweld te voorkomen. In het bijzonder zijn noodzaak en wenselijkheid van maatregelen gericht op het voorkomen en tegengaan van (vuur)wapenbezit binnen de eigen instelling onderzocht en worden gedragen door medewerkers en studenten..*

Aspecten 1B:

- Er is een vastgesteld zero-tolerance beleid met betrekking tot agressie en geweldpleging
- Medewerkers en studenten worden geïnformeerd over dit zero-tolerance beleid
- De instelling controleert indien nodig op wapenbezit
- De instelling neemt preventieve maatregelen om agressie te voorkomen

Onderwerp 1C:	**Sociale macrotrend 'multiculturalisering samenleving'**
Norm 1C:	*Men is zich bewust van de verschillende culturen binnen de eigen instelling. Er is beleid ontwikkeld om spanningen tussen subculturen in de instelling vroegtijdig te herkennen. Er is tevens beleid ontwikkeld om maatwerk te kunnen leveren op basis van actualiteit (bijv. spanningen in Midden-Oosten) om agressie tussen subculturen te voorkomen. Voor elk van de subculturen zijn contactpersonen in kaart gebracht (bijv. contacten binnen de studentenpopulatie of bij studentenverenigingen).*

Aspecten 1C:

- In kaart brengen van het netwerk van subculturen binnen de instelling
- Onderhouden van contacten met personen binnen de verschillende subculturen
- Inschatten van (potentiële) spanningen op basis van actualiteit
- De instelling is consequent in gesprek met vertegenwoordigers van verschillende groepen binnen de studentenpopulatie
- De instelling besteedt zorg aan gebouwen en terreinen vanuit de onderkenning van de voorbeeldfunctie daarvan;
- Organiseren van bijeenkomsten om potentiële spanningen op basis van actualiteit weg te nemen

Onderwerp 1D:	**Alcohol- en drugsmisbruik onder studenten**
Norm 1D:	*Er is beleid om alcohol- en drugsgebruik binnen de instellingen en/of activiteiten van de instelling tegen te gaan. Er is beleid om met studentenverenigingen in contact te treden om een attitudeverandering te bewerkstelligen en excessief gebruik van alcohol en drugs tegen te gaan.*

Aspecten 1D:

- In contact treden met studentenverenigingen en benadrukken dat excessief gebruik een gezamenlijk probleem is
- Uitvaardigen van duidelijke richtlijnen over het verstrekken van alcohol op festiviteiten die door de instelling (mede-)georganiseerd worden

Onderwerp 1E:	**Probleemstudenten door eenzaamheid, slechte studieresultaten, (seksuele) intimidatie, racisme en andere sociale factoren**
Norm 1E:	*Er bestaat binnen de instelling een meldingsstructuur voor studenten met psychische problemen. Medewerkers en studenten worden bewust gemaakt van het bestaan van deze meldingsstructuur en de aanwezigheid van vertrouwenspersonen binnen de instelling.*

Aspecten 1E:

- Vergroten bekendheid van de vertrouwenspersonen binnen de instelling
- Stimuleren dat studenten zichzelf of anderen in contact brengen met vetrouwenspersonen, om langs die weg te werken aan het wegnemen van psychische problemen
- Signaleren van studenten met slechte studieresultaten
- Opstellen van vaste procedures om in gesprek te komen met studenten met slechte resultaten, bijv. via studentendecanen
- Opstellen van procedure om studenten met psychische problemen door te verwijzen naar vertrouwenspersonen, studentenpsychologen of externe hulpverleners
- Benadrukken van ‘zero tolerance’ beleid ten aanzien van (seksuele) intimidatie en racisme
- Stimuleren dat studenten zichzelf of anderen in contact brengen met vetrouwenspersonen in geval van (seksuele) intimidatie
- Ontwikkelen van maatregelen voor situaties waarin racisme zich uit (grafitti, drukwerk)
- Opstellen van procedure om studenten die het slachtoffer zijn van (seksuele) intimidatie door te verwijzen naar vertrouwenspersonen, studentenpsychologen of externe hulpverleners

Onderwerp 1F	**Dreiging radicalisering binnen de instelling**
Norm 1F	*Er bestaat binnen de instelling een meldingsstructuur voor verdachte zaken. Medewerkers en studenten worden bewust gemaakt van het bestaan van deze meldingsstructuur.*

Aspecten 1F:

- Opstellen van meldingsprocedure naar managementniveau
- Opstellen van beoordelingskader voor managementniveau voor het op waarde schatten van meldingen
- Onderhouden van contacten met politie voor het doorgeven van verdachte zaken
- Informeren van medewerkers en studenten over het bestaan en de werkwijze van de meldingsstructuur

Onderwerp 1G:	**Incidenten door stagairs**
Norm 1G:	*In stagecontracten wordt het beleid van de instelling vastgelegd en worden afspraken gemaakt over het omgaan met gevoelige, vertrouwelijke informatie en de aansprakelijkheid van de instelling. Stagebegeleiders worden bewust gemaakt van het bestaan van deze regelingen.*

Aspecten 1G:

- Opstellen van gestandaardiseerde stagecontracten met heldere afspraken over taken, bevoegdheden en verantwoordelijkheden van student, stagebegeleider en bedrijf/instelling waar de stage wordt volbracht
- Ondertekenen van stagecontracten door stagebegeleiders, student en het bedrijf/instelling waar de stage wordt volbracht
- Informeren van medewerkers en studenten over de te hanteren stagecontracten

Onderwerp 1H:	**Ontoelaatbaar gedrag gerelateerd aan studentenverenigingen en/of verenigingen betrokken bij de introductie van aspirant-studenten**
Norm 1H:	*Er bestaan duidelijke richtlijnen waaraan studentenverenigingen dienen te voldoen, willen zij door universiteiten / hogescholen worden erkend.*

Aspecten 1H:

- Accorderen van de door de studentenverenigingen op te stellen richtlijnen voor ontgroeningen en festiviteiten die onder de verantwoordelijkheid van studentenverenigingen worden gehouden
- Waar mogelijk in overleg met collega-universiteiten en hogescholen opstellen van passende sanctiemaatregelen (schorsing, intrekken subsidie, intrekken van erkenning) bij overtreding van de vastgestelde regels

Onderwerp 1I	**Onveiligheid op terrein van de instelling**
Norm 1I:	*De instelling verzamelt meldingen van medewerkers en studenten over onveilige situaties op het terrein van de instelling. Met externe partijen wordt contact gezocht om de veiligheid op het eigen terrein van de instelling te verbeteren.*

Aspecten 1I:

- Opstellen van procedure waar onveilige situaties cq situaties die als ‘onveilig’ worden gevoeld kunnen worden gemeld
- Analyseren van de gemelde situaties
- Vaststellen van prioritering om de onveilige situaties te verbeteren
- Initiëren van overleg met externen (gemeente, politie, openbaar vervoerbedrijven e.d.) om gezamenlijke oplossingen voor de onveilige situaties te zoeken (cameratoezicht, surveillance, aanpassen sluitingstijden etc.)

Onderwerp 1J:	**Onveiligheid buiten terrein van de instelling**
Norm 1J:	*De instelling verzamelt meldingen van medewerkers en studenten over onveilige situaties buiten het terrein van de instelling. Met externen wordt contact gezocht om de veiligheid buiten de instelling te verbeteren.*

Aspecten 1J:

- Opstellen van procedure waar onveilige situaties cq situaties die als ‘onveilig’ worden gevoeld kunnen worden gemeld
- Initiëren van overleg met externen (gemeente, politie, openbaar vervoerbedrijven e.d.) om prioritering in onveilige situaties vast te stellen
- Aandragen van oplossingen om - met beperkte kosten - de onveilige situaties weer veilig te maken

2. Operationeel auditkader voor organisatieveiligheid

Onderwerp 2A:	**Algemeen**
Norm 2A:	*Het organisatieveiligheidsbeleid is uitgewerkt in een concreet uitvoeringsplan. Hierin is de uitvoering van maatregelen geprioriteerd en van budget voorzien. Een veiligheidsmanager is verantwoordelijk voor de uitvoering van de maatregelen. Incidenten op het gebied van organisatieveiligheid worden centraal binnen de instelling geregistreerd en geanalyseerd. Analyses leiden tot aanbevelingen voor het verder terugdringen van onveilige situaties.*

Aspecten 2A:

- Er is een concrete uitwerking van het organisatieveiligheidsbeleid
- Maatregelen op gebied van organisatieveiligheid zijn geprioriteerd en van budget voorzien
- Incidenten op gebied van organisatieveiligheid worden geregistreerd en geanalyseerd
- Over uitvoering van maatregelen wordt gerapporteerd aan het bestuur
- Een tactisch en strategisch coördinatieteam coördineert tijdens ernstige incidenten de interne en externe afstemming van de activiteiten
- De instelling wisselt kennis uit met collega-instellingen

Onderwerp 2B:	**Macrotrend op gebied van organisatieveiligheid: 'Gedogen is uit'; vergunningen worden nageleefd**
Norm 2B:	*De instelling voldoet aan alle bestaande regelgeving. De instelling ziet toe op naleving van de eisen op het gebied van brandveiligheid, arboveiligheid en milieuveiligheid door medewerkers en studenten.*

Aspecten 2B:

- Initiëren van overleg met externen (gemeente, hulpverleningsdiensten) om prioritering in het opheffen van onveilige situaties vast te stellen
- Initiëren van overleg met brandweer en gemeente om vergunningsplichtige locaties in kaart te brengen
- Jaarlijkse analyse van de veiligheid van de gebouwen
- Analyse van veiligheid gebouwen bij wijziging van het gebruik
- Uitrusten van BHV- en EHBO-ploegen en verzorgen van regelmatige trainingen voor deze ploegen
- Organiseren van jaarlijkse ontruimingsoefeningen in alle gebouwen van de instelling voor medewerkers én studenten door de BHV-organisatie
- Betrekken van medewerkers en studenten bij het bedenken van oplossingen om de onveilige situaties veiliger te maken
- Afstemmen van de (ontruimings)plannen van BHV met aanvalsplannen van brandweer
- Vergroten van begrip van medewerkers en studenten voor het handhaven van veiligheidsregels (branddeuren, omgaan met gevaarlijke stoffen)
- Betrekken van buitenlandse studenten en medewerkers die de Nederlandse taal niet machtig zijn bij ontruimingsoefeningen en in de communicatie over het veiligheidsbeleid

Onderwerp 2C:	**De risico-inventarisatie en evaluatie**
Norm 2C:	*De instelling stelt een conform de Arbeidsomstandighedenwet een risico-inventarisatie en evaluatie op, die jaarlijks als basis dient voor het organisatieveiligheidsbeleid. De knelpunten die uit de RI&E naar voren komen worden geprioriteerd en in volgorde opgelost.*

Aspecten 2C:

- Initiëren van overleg met Arbodienst voor het eisenpakket van een RI&E voor de eigen instelling
- Prioriteren van onveilige situaties en de mogelijke effecten voor de continuïteit van de processen binnen de instelling
- Vaststellen van een RI&E alsmede een plan van aanpak
- Laten toetsen van de RI&E van instelling door de Arbodienst

Onderwerp 2D:	**Registratie en doormelden van incidenten**
Norm 2D:	*Er bestaat binnen de instelling een meldingsstructuur voor organisatieveiligheidsproblemen. Medewerkers en studenten worden bewust gemaakt van het bestaan van deze meldingsstructuur en aangemoedigd om problemen te melden.*

Aspecten 2D:

- Registreren van incidenten opstellen en analyseren op samenhang
- Aanstellen van persoon voor registratie en verwerking van meldingen van incidenten
- Vergroten van bekendheid van de meldingsregeling binnen de instelling
- Stimuleren dat studenten en medewerkers problemen op het gebied van organisatieveiligheid melden
- Vergroten van bekendheid van eigen calamiteitenorganisatie bij de relevante autoriteiten waar de calamiteiten moeten worden doorgemeld

Onderwerp 2E:	**Bedreiging vitale objecten binnen de instellingen**
Norm 2E:	*Binnen de instellingen zijn specifieke vitale objecten in kaart gebracht. Specifieke aandacht wordt geschonken aan brand- en inbraakbeveiliging van laboratoria. Medewerkers en studenten zijn op de hoogte van de procedures voor het werken met gevaarlijke stoffen en microbiologische ziekteverwekkers en wat te doen bij een bedreiging van deze vitale objecten (onder meer bij bommeldingen).*

Aspecten 2E:

- Bewijs van goed gedrag en andere 'screening' toepassen op beheerders en medewerkers in kwetsbare functies
- Doorvoeren van specifieke risicobeperkende maatregelen op plaatsen waar wordt gewerkt met gevaarlijke en/of brandbare stoffen en microbiologische ziekteverwekkers.
- Geven van specifieke aandacht voor brand- en inbraakbeveiliging op vitale plaatsen
- Opzetten van back-up systemen die garanderen de dat vitale kennis niet verloren gaat
- Testen van back-up systemen
- Geven van aparte voorlichting aan medewerkers, studenten en derden (schoonmakers, onderhoudswerkers e.d.) die op plaatsen met gevaarlijke stoffen werken, over nut-en-noodzaak van de veiligheidsregels ter plaatse
- Registreren van calamiteiten en regelmatig herzien van risico-analyses op basis van de geregistreerde calamiteiten en incidenten
- Doen van aangifte van ernstige calamiteiten (zonder uitzondering)
- Ondertekenen van veiligheidsregels door studenten en medewerkers
- Voorrang geven aan meldingen van calamiteiten op deze locaties - waaronder bommeldingen - en evalueren binnen de registratieprocedure (2B)

Onderwerp 2F:	**Controversiële experimenten**
Norm 2F:	*De instelling verzamelt meldingen over bezettingen, bommeldingen, demonstraties, brandstichtingen en vernielingen in of nabij gebouwen waarin controversiële experimenten (met proefdieren, genetisch gemodificeerde organismen etc.) worden gehouden. Bedreigingen van het personeel worden gemeld.*

Aspecten 2F:

- Bewijs van goed gedrag en andere 'screening' toepassen op beheerders en medewerkers in kwetsbare functies
- Opstellen van procedure waarbij de veiligheidsrisico's rond proefdierenlaboratoria in kaart worden gebracht
- Initiëren van overleg met externen (gemeente, politie, collega-instellingen e.d.) om onveilige situaties vast te stellen, te anticiperen op maatschappelijk gesproken 'gevoelige proeven'
- Rapporteren van incidenten op management niveau
- Aandragen van oplossingen om de onveilige situaties rond proefdierenlaboratoria weer veilig te maken

Onderwerp 2G:	**Bijzondere collecties en historische panden**
Norm 2G:	*Collectiebeherende instellingen en beheerders van historische panden stellen specifieke brandveiligheids- en inbraakbeveiligingsplannen op, die rekening houden met de specifieke omstandigheden van deze instellingen.*

Aspecten 2G:

- Opstellen van brandveiligheidsplannen voor historische panden en collecties
- Opstellen van inbraakbeveiligingsplannen voor historische panden en collecties
- Aandragen van maatwerkoplossingen om collecties tegen zowel brand als diefstal te beveiligen
- Initiëren van overleg met gemeente en hulpdiensten (brandweer, politie) om oplossingen te zoeken voor tegenstrijdige regelgeving

Onderwerp 2H:	**Brandstichting**
Norm 2H:	*De instelling verzamelt meldingen van medewerkers en studenten over brandstichtingen en analyseert deze.*

Aspecten 2H:

- Opstellen van kwetsbaarhedenanalyse voor brandstichting, waarbij de zwakke plekken binnen de instelling in kaart worden gebracht (openbaar toegankelijke plaatsen met weinig toezicht e.d.)
- Opstellen van procedure waar brandstichtingen worden gemeld en geanalyseerd
- Betrekken van medewerkers en scholieren door de instelling in het melden van verdachte gedragingen die mogelijk samen kunnen hangen met brandstichtingen
- Instelling stelt alleen of in samenspraak met verzekeraars en vergunningverleners ‘early warning indicatoren’ vast waarmee brandstichtingen vroegtijdig kunnen worden ontdekt
- Opstellen van procedure voor het verscherpen van toezicht na brandstichtingen, om nieuwe brandstichtingen te voorkomen.

Onderwerp 2I:	**Inbraak en diefstal**
Norm 2I:	*De instelling stelt beleid op om diefstal van goederen te voorkomen. De instelling verzamelt meldingen van medewerkers en studenten over inbraak en diefstal en analyseert deze*

Aspecten 2I:

- Opstellen van kwetsbaarhedenanalyse voor inbraak en diefstal, waarbij de zwakke plekken binnen de instelling in kaart worden gebracht (weinig toezicht, computer-, video- en audioapparatuur, gevaarlijke stoffen e.d.)
- Bewijs van goed gedrag en andere ‘screening’ toepassen op beheerders en medewerkers in kwetsbare functies
- Opstellen van procedure waar inbraken en diefstal worden gemeld en geanalyseerd
- Betrekken van medewerkers en scholieren door de instelling, in het melden van verdachte gedragingen die mogelijk samen kunnen hangen met inbraken en diefstal
- Instelling stelt alleen of in samenspraak met verzekeraars en vergunningverleners procedures vast waarmee inbraak en diefstal worden voorkomen
- Betrekken van medewerkers en studenten om de alertheid voor inbraak en diefstal te vergroten

Onderwerp 2J:	**Extreme weersomstandigheden, waaronder onweer**
Norm 2J:	*De instelling maakt kwetsbaarhedenanalyse voor verschillende extreme weerstypen, waaronder onweer (met inductie tot gevolg).*

Aspecten 2J:

- Opstellen van kwetsbaarhedenanalyse voor verschillende weertypen (extreme regenval, storm, onweer, extreme droogte) en de gevolgen daarvan voor de continuïteit van de processen binnen de instelling
- Prioriteren van kwetsbaarheden (brand, waterschade, vorstschade, inductie) en treffen van maatregelen om grootste risico's te beperken

Onderwerp 2K:	**Voorbereiding op en signaleren van infectieziekten**
Norm 2K:	*De instelling stelt procedure op om bij opvallend hoog aantal ziektemeldingen de plaatselijke GGD in te schakelen*

Aspecten 2K:

- Instellingen hebben geen bijzondere taak in het signaleren van infectieziekten
- Desalniettemin worden instellingen aangeraden contact te leggen met de plaatselijke GGD, indien een opvallend hoog aantal ziektemeldingen plaatsvindt bij personen die werkzaam zijn danwel een opleiding volgen binnen de instelling
- Na raadplegen van GGD worden zonodig maatregelen afgekondigd die verspreiding van infectieziekte binnen de instelling tegengaan en geïnfecteerde personen in contact brengen met de GGD

Onderwerp 2L:	**Bedreiging intern milieu door gevaarlijke stoffen zoals asbest**
Norm 2L:	*De instelling is zich bewust van de aanwezigheid van gevaarlijke stoffen (zoals asbest) en weet wat te doen wanneer deze vrijkomen. Maatregelen zijn afgestemd met externe partijen.*

Aspecten 2L:

- Inventarisatie van aanwezige gevaarlijke stoffen
- Aanmelden en registreren van renovatiewerkzaamheden ivm asbest
- Voorbereiden maatregelen wanneer gevaarlijke stoffen vrijkomen

Onderwerp 2M:	**Risico's bij reguliere arbeidsomstandigheden**
Norm 2M:	*Studenten en medewerkers worden op de hoogte gebracht van de maatregelen die zijzelf kunnen treffen om hun werkzaamheden conform de Arbeidsomstandighedenwet en Arboregels uit te voeren.*

Aspecten 2M:

- Instelling past Arboregels onverkort toe binnen de eigen organisatie
- Wijzen van studenten en medewerkers op hun eigen verantwoordelijkheid ten aanzien van het naleven de Arbo-regels
- Informeren van studenten en medewerkers over het gevaar van RSI en de maatregelen die zijzelf kunnen treffen om klachten als RSI te voorkomen
- Stimuleren van studenten en medewerkers om maatregelen te treffen die klachten als RSI kunnen voorkomen

Onderwerp 2N:	**Fraude en diefstal**
Norm 2N:	*Er bestaat binnen de instelling een meldingsstructuur voor fraude en diefstal. Medewerkers en studenten worden bewust gemaakt van het bestaan van deze meldingsstructuur.*

Aspecten 2N:

- Opstellen van meldingsprocedure voor diefstal
- Faciliteren van het doen van aangifte voor diefstal
- Registreren van diefstallen naar soort en frequentie
- Opstellen van interne meldingsprocedure naar managementniveau en/of CvB-niveau bij diefstal door eigen medewerkers en/of studenten
- Opstellen van aangiftebeleid bij diefstal van het eigendom van de eigen instelling
- Opstellen van eisen voor het toetsen van de integriteit van medewerkers, zoals een verplichting tot een ‘verklaring van goed gedrag’
- Inwinnen van informatie bij voorgaande werkgevers, om achtergronden van nieuwe medewerkers na te gaan
- Onderhouden van contacten met politie voor het doorgeven van diefstallen
- Bewijs van goed gedrag en andere ‘screening’ toepassen op beheerders en medewerkers in kwetsbare functies
- Informeren van medewerkers en studenten over het bestaan en de werkwijze van de meldingsstructuur bij fraude en diefstallen

3. Audit op gebied van kennisveiligheid

Onderwerp 3A:	**Algemeen**
Norm 3A:	*Het kennisveiligheidsbeleid is uitgewerkt in een concreet uitvoeringsplan. Hierin is de uitvoering van maatregelen geprioriteerd en van budget voorzien. Een veiligheidsmanager is verantwoordelijk voor de uitvoering van de maatregelen. Incidenten op het gebied van kennisveiligheid worden centraal binnen de instelling geregistreerd en geanalyseerd. Analyses leiden tot aanbevelingen voor het verder terugdringen van onveilige situaties*

Aspecten 3A:

- Er is een concrete uitwerking van het kennisveiligheidsbeleid
- Maatregelen op gebied van kennisveiligheid zijn geprioriteerd en van budget voorzien
- Incidenten op gebied van kennisveiligheid worden geregistreerd en geanalyseerd
- Over uitvoering van maatregelen wordt gerapporteerd aan het bestuur
- Een tactisch en strategisch coördinatieteam coördineert tijdens ernstige incidenten de interne en externe afstemming van de activiteiten
- De instelling wisselt kennis uit met collega-instellingen

Onderwerp 3B:	**Macrotrend op gebied van kennisveiligheid** **'Toenemend gebruik van ICT'**
Norm 3B:	*Men is zich bewust van de toenemende afhankelijkheid van de ICT-infrastructuur binnen de instelling en kwetsbaarheid voor virussen, hackers, stroomuitval etc..*

Aspecten 3B:

- Informeren van medewerkers en studenten over ICT-beleid
- Centrale registratie van virusaanvallen en/of hackpogingen
- Opstellen van 'policy' of kennisintegriteitsbeleid voor het gebruik van internet en het computernetwerk van de instelling, waarin expliciet ongewenst gedrag staat beschreven
- Opstellen van kwetsbaarhedenanalyse en een overzicht van de effecten van een uitval van ICT-netwerken op de continuïteit van de processen van de instelling
- Stimuleren van risicobewustzijn bij eindgebruiker

Onderwerp 3C:	**Risicomanagement**
Norm 3C:	*Hoofden van ICT-afdelingen zijn bekend met de laatste stand van zaken op ICT-gebied en hebben actuele kennis van risico's.*

Aspecten 3C:

- De instelling gaat diefstal en fraude van kennis tegen door het invoeren van een brede vorm van *'clean desk policy'*: zorg voor de staat waarin de werkplek wordt achtergelaten verminderd risico's
- Doorlopend actualiseren van ICT-kennis en kennis over beveiliging van computernetwerken
- Legaliseren van de software die op het universiteitsnetwerk aanwezig is
- Software wordt met regelmaat geupdate om hackpogingen te voorkomen
- Centrale registratie van virusaanvallen en/of hackpogingen
- Nemen van passende maatregelen om virusaanvallen en/of hackpogingen via het vaste netwerk danwel via WiFi-;access points te voorkomen
- Eindgebruikers worden geïnformeerd over een veilig gebruik van systemen en kennis
- Ontwikkelen van een 'vertrouwelijkheidsverklaring' ter ondertekening voor medewerkers en studenten voor instellingen die met gevoelige informatie werken
- Ontwikkelen van selectiecriteria voor de toelating van (buitenlandse) studenten en wetenschappelijk medewerkers tot relevante opleidingen en delen van de instelling op basis van het Handboek Integriteitsonderzoek (ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2003).

Onderwerp 3D:	**Alertheid bij studenten en medewerkers**
Norm 3D:	*Studenten en medewerkers zijn bekend met de risico's van computergebruik en melden verdachte zaken.*

Aspecten 3D:

- Aanstellen van aanspreekpunten binnen de ICT-afdeling waar verdachte zaken (anoniem) gemeld kunnen worden
- Conformeren van studenten en medewerkers aan een policy waarin het gebruik van het computernetwerk en internet binnen de instelling is beschreven
- Informeren (verplicht) van eindgebruikers over het veilig gebruik van de systemen en kennis, waarbij gebruik wordt gemaakt van de informatie uit het project KWINT (Kwetsbaarheid op Internet) van het Ministerie van Economische Zaken
- Informeren van eindgebruikers in geval van calamiteiten of incidenten over de maatregelen die moeten worden getroffen om herhaling te voorkomen

Onderwerp 3E:	**Kennisveiligheid bij calamiteiten**
Norm 3E:	*De instelling treft voorzieningen om bij calamiteiten de kennis veilig te stellen.*

Aspecten 3E:

- Back-up faciliteiten worden opgezet waarop kennis die digitaal aanwezig is wordt vastgelegd
- Back-up faciliteiten worden buiten de instelling ondergebracht
- Vermelden - in ontruimingsplannen - hoe de aanwezige kennis van de instelling die niet digitaal beschikbaar is in veiligheid kan worden gebracht tijdens calamiteiten (brand, aanslagen, ontruimingen,bezettingen)

Onderwerp 3F:	**Beheer van kennis**
Norm 3F:	*De instelling maakt zonodig classificaties en stelt vast welke studenten, medewerkers en promovendi toegang hebben tot welke kennis.*

Aspecten 3F:

- Bewijs van goed gedrag en andere ‘screening’ toepassen op beheerders en medewerkers in kwetsbare functies
- Vaststellen welke kennis binnen de instelling aanwezig is
- Classificeren van kennis, waarna wordt vastgesteld welke studenten, medewerkers en promovendi toegang hebben tot welke kennis
- Beveiligen van kennis die niet algemeen toegankelijk wordt geacht
- Op de hoogte brengen van medewerkers en studenten omtrent het nut en de noodzaak om zorgvuldig om te gaan met de kennis die binnen de instelling aanwezig is
- Binnen instellingen wordt ondersteunend personeel (schoonmakers, onderhoudmedewerkers) gescreend alvorens zij aan het werk kunnen op afdelingen met gevoelige informatie
- Informeren van eindgebruikers over een veilig gebruik van systemen en kennis
- De verantwoordelijke voor integriteit van personeel en studenten beschikt over procedures om politie te informeren omtrent (vermeend) misbruik van kennis

BIJLAGE II
LITERATUURLIJST

Boeken en rapporten

- AIVD, Jaarverslag 2002
- AIVD, *Proliferatie van massavernietigingswapens; Risico's voor bedrijven en wetenschappelijke instellingen*, 2003
- AIVD, *Spionage en veiligheidsrisico's: actueel, onzichtbaar en divers*, 2004
- Ambtelijke Commissie Toezicht, *Vertrouwen in onafhankelijkheid*, 2000
- Benschop, A., *Cyberterrorisme: dodelijk geweld vanaf het toetsenbord*, Universiteit van Amsterdam, Amsterdam, 2001
- Borgers-Roozen, M.J.A., T.J. Golder, M.J. Klaver, G.J. van Rossum, *Informatieoorlog: over de schaduwkanten van de informatiemaatschappij*, Stichting Maatschappij en Onderneming, Den Haag, 2000
- Bruin, J.A. de, en E.F. Ten Heuvelhof, *Management in netwerken*, Lemma, Utrecht, 1999
- COT, Aandachtspunten *OCW dreiging oorlog Irak*, 2003
- COT, *Crisis. Oorzaken, gevolgen en kansen*, Leiden, 1998
- Cuny, F.C., *Disasters and Developmen*t. Oxford University Press, New York, 1983
- Denning, D.E., '*Activism, Hacktivism, and Cyberterrorism*; *The Internet as a Tool for Influencing Foreign Policy*', in: J. Arquilla, D. Rohnfeldt, Networks and Netwars: the Future of Terror, Crime and Militancy, RAND, Santa Monica, 2001
- Dienst Facilitaire Zaken, Hanzehogeschool Groningen, *Bedrijfsnoodplan Faculteit Economie en Bestuur & Stafbureaus*, 2003
- Expertisecentrum Rechtshandhaving, Ministerie van Justitie, *De Tafel van Elf, beknopte toets voor de handhaafbaarheid van regels*, 2002
- Gezondheidsraad: Commissie Risicomaten en risicobeoordeling, *Niet alle risico's zijn gelijk. Kanttekeningen bij de grondslagen van de risicobenadering in het milieubeleid*, Den Haag, advies 1995/06, 1995
- Gladwell, M., *The Tipping Point*, 2002
- Helsloot, I. en P. Verhallen (red.), *Zicht op rampenbestrijding*, 2003
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, *Integrale Veiligheidsrapportage*, 1993
- Ministerie van OC&W, *Risicoanalyse normale bedrijfsvoering*, 2004
- Muller, E.R., R.F.J. Spaaij, A.G.W. Ruitenberg, *Trends in terrorisme*, 2003
- NIBRA, *Vergunningverlening, controle en handhaving brandveiligheid; eindrapportage van de quickscan,* 2001, In opdracht van de Onderzoek Cafébrand Nieuwjaarsnacht 2001
- Onderwijsraad, *Samen leren leven*, Verkenning, 2002
- RIVM, *Nuchter omgaan met Risico's*, Milieu- en Natuurplanbureau (MNP), rapport 251701047/2003, 2003
- Rosenthal, U., *Veiligheidsniveaus: over menselijke fouten, het systeem en nieuwe zondebokken*, in *Ramp en Recht*, Boom Juridische Uitgevers, 2001
- Slovic, P, en E.U. Weber, *Perception of Risk* Posed by Extreme Events, discussionpaper at the conference '*Risk Management Strategies in an Uncertain World'*, New York, 2002
- Slovic, P., The perception of risk, Earthscan, Londen, 2000
- Stolker, C.J.J.M., e.a., "*Defensieve bureaucratie? Rampen, de overheid en de preventieve rol van het aansprakelijkheidsrecht*" in "ramp en recht", red E.M. Muller en C.J.J.M. Stolker, Boom Juridische uitgevers, 2001
- Thomas, W.J. en D.S. Thomas, *The child in America*, New York, 1928
- TNO, Kiwa en NIBRA, Emergos, *Checklist voor de inrichting van bedrijfsnoodorganisaties*, 2002

- Wendrich, L., Op *onze school zijn alle wapens verboden*; Een evaluatie van de campagne tegen wapenbezit op Rotterdamse middelbare scholen, 2000
- Wildawsky, A., *Searching for Safety*, New Brunswick, 1988

Artikelen in dagbladen en tijdschriften

- Anoniem, *Amsterdamse studenten flink aan de drugs*, Folia jaargang 56, 1 maart 2003
- Anoniem, '*Asbest ontdekt bij elektrotechniek'*, Delta, nummer 14, jaargang 28
- Anoniem, *Erasmus straft studentencorps voor wangedrag*, in: NRC Handelsblad, 17 oktober 2000
- Anoniem, *Friese docenten sturen directie een poederbrief*, in: De Telegraaf 29 oktober 2001
- Anoniem, *Honderdtwintig studenten melden fraude bij Fontys*, In: Branbants Dagblad, 26 februari 2003
- Anoniem, '*Maatregelen SARS op Hogeschool Zeeland'*, in De Telegraaf, 3 april 2003
- Anoniem, '*Minister vreest 'veel rampspoed',* in: Folia 28 – Weekblad Universiteit van Amsterdam, jaargang 56, 17 maart 2003
- Anoniem, '*Nieuws, rechten pakt fraude stevig aan'*, in: Ublad, 24 januari 2002
- Anoniem, '*Plagiaat en spieken strafrechtelijk vervolgen'*, op Univers Online (http://www.uvt.nl/univers/nieuws/0203/08/fraude.html) , 17 oktober 2002
- Anoniem, '*Veertig procent van Utrechtse studenten heeft RSI'*, op site: http://www.edusite.nl/edusite/nieuws/10699
- Brouwer, A., *De Algerijnse connectie*, in: De Groene Amsterdammer, 16 november 2002
- Coleman, L., *Costs of corporate crisis*, Journal of Contingencies en Crisis Management, volume 1, 2004
- Finn, P., *Sept. 11 plot came together in Germany*, in: The Washington Post, 11 september 2002
- Fokkinga, P., *De bedrieger bedrogen*, op: http://www.edusite.nl/edusite/nieuws/1475 (bron: The Washington Post)
- Heijnen, A., '*Redactioneel, Très'*, Ublad, 10 december 1998
- Holtgrave, D., en E.U. Weber, *Dimensions of risk perception for financial and health risks*, in: Risk Analysis, no. 13, 1993
- IJssel, G. van den, *Hogeschool wil af van onveilige tunnel*, in: De Posthoorn, 2 mei 2001
- Jacobi, A.J., *Bioterrorisme in Nederland,* in: Infectieziektenbulletin, jaargang 14, nr. 3
- Ruis, P., '*Pronken met andermans veren'*, op site: http://e-learning.surf.nl/e-learning/artikelen/773
- Sing-Sit, K., *Het onveilige gevoel rond Hollands Spoor*, in: de Haagse Courant, 19 april 2002
- Sjöberg, L., *Are received risk models alive and well?*, in: Risk Analysis, 2002
- Smit, H., *Studentenpsycholoog krijgt steeds meer klachten*, Drank, depressie en discipline, in: NRC Handelsblad, 14 april 2001
- Starr, C., *Social benefits versus technological risk*, in: Science, 1969, pp. 1232-1238
- Vandendriessche, D. en K. Raskin, 'Zelfmoord aan de KU Leuven: onderzoek en beleidsimplikaties, *Studeren aan de universiteit: levensgevaarlijk?*', Studentenweekblad van de Leuvense Overkoepeldende Kringorganisatie, nummer 16, 17 januari 2000
- Vlek, C.A.J. en P.J.M. Stallen, *Persoonlijke beoordeling van risico's*, Instituut voor Experimentele Psychologie, Groningen, 1979; A multi-level, multi-stage, multi-attribute perspective on risk assesment, decision making and risk control, in: Risk Decision Policy, 1996, pp. 9-31
- Vries, L. de, *Corpsleden bekennen mishandeling nuldejaars*, in: Delta, jaargang 31, nummer 27
- Vries, L. de, *Rector wil beraad over drankgebruik*, in: Delta, jaargang 29, nr. 28
- Wijnands, K, *Voer voor psychologen,* in: Delta, jaargang 35, nr. 27
- Zandbergen, P., '*Zaak-Diektra is testcase'*, in: UT Nieuws, weekblad van de universiteit Twente, 5 september 1996, jaargang 31, nr. 25

Tweede Kamerstukken
- TK 21761, *Schriftelijk overleg inzake de monitor Sociale veiligheid*, 24 juni 2003
- TK 2000111510, *Vragen PvdA over pesten*, 19 juni 2001
- TK HBO/SB/01/25136, *Antwoord op de vragen van de leden Kortram en Hamer van uw Kamer inzake het onderzoek naar ongewenst gedrag op de Hogeschool Zuyd*, 19 juni 2001

Lezingen
- *Machiavelli-lezing* 19 november 2001, uitgesproken door minister Korthals van Justitie
- Zundert, D. van, Lezing "*Agressie en geweld in het onderwijs*", in het kader van de vierde werkconferentie, georganiseerd door het platform Veiligheid en Geweld in de BVE-sector d.d. 6 juni 2002

Websites
- http://www.aob.nl/hobarchief/resultaat/0,ArtikelIID,2939,Marker,geweld,00.asp
- http://www.cdc.gov/od/ohs/biosfty/bmbl4/bmbl4s2.htm
- http://docenten.nrc.nl/nieuwsbrief/archief/2002/10.html
- http://www.edusite.nl/edusite/nieuws/10699
- http://www.edusite.nl/edusite/nieuws/1475
- http://www.foliacivitatis.nl
- http://www.fontys.nl/nieuws/nieuws_artikel.asp?docid=1905
- http://www.minbzk.nl/contents/pages/2056/Deel1.pdf
- http://www.uvt.nl/faculteiten/frw/trom-l/j4n11/
- http://www.zembla.tv
- http://www.laatjenietpakken.nl

BIJLAGE III
RESPONS INSTELLINGEN HOGER ONDERWIJS

In deze bijlage wordt de repons op de enquêtes die onder alle onderwijsinstellingen zijn verspreid weergegeven.

	Bestuur	Organisatie	Sociaal	Kennis
Universiteit van Amsterdam	X	X	X	X
Vrije Universiteit Amsterdam				
Technische Universiteit Delft		X	X	X
Technische Universiteit Eindhoven	X	X	X	X
Rijksuniversiteit Groningen	X	X		X
Universiteit Leiden	X	X	X	X
Universiteit Maastricht	X			X
Katholieke (Radboud per 1/9/04) Universiteit Nijmegen	X	X	X	X
Erasmus Universiteit Rotterdam	X	X	X	X
Universiteit Twente	X	X	X	X
Universiteit van Tilburg	X	X	X	X
Universiteit Utrecht				
Wageningen Universiteit	X	X	X	X
Hogeschool IPABO Amsterdam/Alkmaar				
Hogeschool van Amsterdam				
Dr. Gerrit TFh. Rietveld Academie				
Hogeschool van Arnhem en Nijmegen	X			X
Hogeschool Brabant				
NHTV, Internationale Hogeschool Breda	X	X	X	X
Iselinge Educatieve faculteit	X	X	X	X
Christelijke Hogeschool Ede		X	X	X
The Design Academy				
Christelijke Hogeschool De Driestar	X	X	X	X
Hogeschool Edith Stein/Onderwijscentrum Twente		X	X	X
Hogeschool Zuyd	X	X	X	X
Noordelijke Hogeschool Leeuwarden				
Gereformeerde Hogeschool Zwolle	X			
Christelijke Hogeschool Nederland				
Stichting Hogeschool Leiden				
Hogescholen INHOLLAND				X
Christelijke Agrarische Hogeschool Dronten	X	X		
Internationale Agrarische Hogeschool Larenstein				
Hogeschool voor Muziek en Dans Rotterdam	X	X		X
Marnix Academie PC hogeschool Lerarenopleiding basisonderwijs	X	X	X	X
Hogeschool van Utrecht		X	X	X
Hogeschool 's-Hertogenbosch				
RK Technische Hogeschool Rijswijk				X
Hogeschool Diedenoort				
Amsterdamse hogeschool voor de Kunsten				
Hogeschool voor Economische Studies	X			X

ArteZ Hogeschool voor Kunsten		X	X	X
Saxion Hogescholen	X	X		
Hogeschool Helicon		X	X	
Fontys Hogescholen	X	X	X	X
Hogeschool De Horst				
Christelijke Hogeschool Windesheim				
Hogeschool Drenthe	X	X	X	X
Haagse Hogeschool				X
Hotelschool Den Haag, Internationale Hogeschool voor Hotelmanagement		X		X
Hogeschool van Beeldende Kunsten, Muziek en Dans				
Hanzehogeschool Groningen		X		X
Pedagogische Hogeschool De Kempel				
Katholieke PABO Zwolle	X	X		
Van Hall Instituut				
Hogeschool Rotterdam				
Hogeschool Zeeland				
Hogeschool voor de Kunsten Utrecht				
Hogeschool Domstad, Kath lerarenopleiding basisonderwijs		X	X	X
HAS 's-Hertogenbosch				

BIJLAGE IV
UITWERKING RESPONS ENQUÊTES

In deze bijlage is de respons op de enquêtes voor de besturen en de respons op de vragenlijsten voor sociale veiligheid, organisatieveiligheid en kennisveiligheid verwerkt. De vragenlijsten zijn naar de instellingen binnen het hoger onderwijs verstuurd. De antwoorden op de vragen met betrekking tot de functies en taken, en de inrichting van de organisatie van de respondent zijn niet verwerkt in deze bijlage.

Uitleg symbolen
U= universiteit
H= hogeschool

VRAGENLIJST BESTUUR

Vraag 1.	***Vragenlijst Bestuur***
	Kunt u (zo mogelijk in een organogram) aangeven waaronder de verschillende vormen van veiligheid binnen uw instelling vallen (bestuurlijk en operationeel)?

Vraag 2.	***Vragenlijst Bestuur***
	Hoe zijn de bevoegdheden en verantwoordelijkheden voor veiligheids- en crisismanagement verdeeld binnen uw instelling?

Vraag 3.	***Vragenlijst Bestuur***
	Hoe wordt over veiligheid binnen uw instelling gerapporteerd aan het (college van) bestuur?

Antwoord:
- Via het arbo-jaarverslag, 7x (6U,1H)
- Periodiek, 11x (6U,5H)
- Incidenteel, 7x (3U,4H)
- Niet, 1x (1H)

Vraag 4.	***Vragenlijst Bestuur***
	Heeft uw instelling beleidsuitgangspunten geformuleerd aangaande een of meerdere vormen van veiligheid?

Antwoord:
- Ja, op gebied fysieke veiligheid, 13x (8U,5H)
- Ja, op gebied sociale veiligheid, 3x (2U,1H)
- Ja, op gebied kennis/ICT veiligheid, 1x (1U)
- Nee, 4x (4H)

Vraag 5.	***Vragenlijst Bestuur***
	Heeft uw instelling in het bijzonder beleidsmatige voorzieningen getroffen voor crisismanagement in de acute fase van een crisis (bv. strategisch plan, risicocommunicatieplan)?

Antwoord:
- Vorming Crisismanagementteam (CMT), 3x (2U,1H)
- Planvorming, 16x (6U,10H)
- Geen voorzieningen, 1x (1H)

Vraag 6.	***Vragenlijst Bestuur***
	Welke risico- of kwetsbaarheidanalyses worden er binnen uw instelling uitgevoerd waarover aan het bestuur wordt gerapporteerd?

Antwoord:
- Risico-inventarisatie –en evaluatie, 16x (6U,12H)
- Geen, 2x (2H)

Vraag 7.	***Vragenlijst Bestuur***
	Heeft uw instelling specifiek budget gealloceerd in haar begroting voor de verschillende vormen van veiligheid? Zo ja, wat is ontwikkeling hiervan in de afgelopen jaren?

Antwoord:
- Het budget is gestegen, 4x (2U,2H)
- Het budget is gelijk gebleven, 9x (4U,5H)
- Nee, 5x (5H)

Vraag 8.	***Vragenlijst Bestuur***
	Wordt er in jaarrapportages aandacht besteed aan de verschillende vormen van veiligheid?

Antwoord:
- Ja, 13x (6U,7H)
- Nee, 5x (5H)

Vraag 9.	***Vragenlijst Bestuur***
	Welke vormen van veiligheid komen met regelmaat aan de orde in het College van Bestuur? Kunt u voorbeelden aangeven?

Antwoord:
- Fysiek, 11x (5U,6H)
- Sociaal, 5 (3U,2H)
- Kennis/ICT, 1x (1H)
- Crisismanagement, 3x (2U,1H)
- Geen, 5x (1U,4H)

Vraag 10.	***Vragenlijst Bestuur***
	Kunt u een voorbeeld geven van een (bestuurlijke) *best practice* ten aanzien van een of meerdere vormen van veiligheid binnen uw instelling? *

* Antwoorden op deze vraag zijn in het rapport verwerkt.

Vraag 11.	***Vragenlijst Bestuur***
	Worden studenten betrokken bij veiligheidsaspecten? Zo ja, hoe? Heeft u daarover beleid geformuleerd?

Antwoord:
- Via medezeggenschapsraden, 5x (3U,2H)
- Via training of oefening, 3x (3H)
- Via klachtenregeling, 1x (1U)
- In de opleiding, 3x (1U, 2 H)
- Door voorlichting, 2x (2U)
- Niet betrokken, 5x (5H)

Vraag 12.	***Vragenlijst Bestuur***
	Wordt het personeel betrokken bij veiligheidsaspecten? Zo ja, hoe? Heeft u daarover beleid geformuleerd?

Antwoord:
- Via medezeggenschapsraden, 5x (3U,2H)
- Via training of oefening, 7x (3U,4H)
- Via contactpersoon, 2x (2U)
- Via huisregels 1x (1H)
- In de opleiding, 1x (1H)
- Door voorlichting, 2x (2U)
- Niet betrokken, 3x (5H)

Vraag 13.	***Vragenlijst Bestuur***
	In welke mate wordt in (interne) opleidingen aandacht geschonken aan vormen van veiligheids- en crisismanagement? Heeft u daarover beleid geformuleerd? *

* Zie vraag 12.

Vraag 14.	***Vragenlijst Bestuur***
	Worden in uw instelling oefeningen gehouden ter training van veiligheidsbewustzijn en crisismanagement? Zo ja, wat is karakter en de frequentie hiervan? Heeft u daarover beleid geformuleerd?

Antwoord:
- BHV, 6x (3U,3H)
- CMT, 3x (3U)
- Ontruiming, 9x (3U,6H)
- Geen, 4x (4H)

Vraag 15.	***Vragenlijst Bestuur***
	Wat zijn volgens u de grootste risico's rond veiligheid in het hoger onderwijs?

Antwoord:
- Calamiteiten met veel mensen, 4x (3U,1H)
- Fysieke risico's, 6x (3U,3H)
- Sociale risico's, 5x (2U,3H)
- Kennis/ICT-risico's, 4x (3U,1H)
- (On)veiligheid gebouwen, 2x (2U)
- Terreur, 2x (2U)
- Onveiligheid studenten, medewerkers en docenten in het buitenland, 1x (1H)
- Geen, 3x (3H)

Vraag 16.	***Vragenlijst Bestuur***
	Welke ontwikkelingen ten aanzien van veiligheid in het hoger onderwijs verwacht u op de langere termijn?

Antwoord:
- Meer beleid/ middelen, 8x (4U,4H)
- Strengere toegangseisen, 4x (3U,1H)
- Maatschappelijke ontwikkelingen die de veiligheid aantasten, 4x (1U,3H)
- Geen, 4x (4H)

VRAGENLIJST SOCIALE VEILIGHEID

Vraag 1.	***Vragenlijst Sociale veiligheid***
	Welke functie bekleedt u?

Vraag 2.	***Vragenlijst Sociale veiligheid***
	Binnen welk onderdeel van de organisatie?

Vraag 3.	***Vragenlijst Sociale veiligheid***
	Wat zijn uw exacte taken op het gebied van sociale veiligheid?

Vraag 4.	***Vragenlijst Sociale veiligheid***
	Wat zijn volgens u de grootste risico's rondom veiligheid in uw taakveld voor uw instelling?

Antwoord:
- Geweld, 5x (3U,2H)
- Criminele activiteiten, 2x (2U)
- Te weinig aandacht voor preventie, 1x (1U)
- Fraude, 1x (1H)
- Schending privacy of lichamelijke integriteit, 2x (1U,1H)
- Geen grote risico's, 3x (2U,1H)

Vraag 5.	***Vragenlijst Sociale veiligheid***
	Welke ontwikkelingen ten aanzien van veiligheid in het hoger onderwijs ziet u in uw taakveld op de lange termijn?

Antwoord:
- Toenemende mate van criminele handelingen, 3x (2U,1H)
- Intensievere samenwerking universiteiten en HBO's, 1x (1U)
- Meer maatregelen en beleid, 5x (3U,2H)
- Geen, 3x (3H)

Vraag 6.	***Vragenlijst Sociale veiligheid***
	Welke prioriteit heeft veiligheid ten opzichte van andere taken binnen uw functie?

Antwoord:
- Hoog, 4x (4U)
- Gemiddeld, 5x (1U,4H)
- Laag, 4x (1U,3H)

Vraag 7.	***Vragenlijst Sociale veiligheid***
	Welke prioriteit krijgt het bevorderen van veiligheid in uw taakveld naar uw mening binnen uw instelling?

Antwoord:
- Hoog, 6x (5U,1H)
- Gemiddeld, 1x (1H)
- Laag, 6x (1U,5H)

Vraag 8.	***Vragenlijst Sociale veiligheid***
	Is de aandacht voor veiligheid in uw taakveld toe- of afgenomen in de afgelopen vijf jaar?

Antwoord:
- Toegenomen, 10x (6U,4H)
- Gelijk gebleven, 3x (3H)

Vraag 9.	***Vragenlijst Sociale veiligheid***
	Registreert en analyseert u of anderen in uw instelling incidenten rond sociale veiligheid?

Antwoord:
- Ja, 11x (6U,5H)
- Nee, 2x (2H)

Vraag 10.	***Vragenlijst Sociale veiligheid***
	(indien onder 9. 'ja') Op welke wijze vindt registratie en analyse plaats?

Antwoord:
- Centraal, 10x (5U,5H)
- Decentraal, 1x (1U)

Vraag 11.	***Vragenlijst Sociale veiligheid***
	Wat gebeurt binnen uw instelling met lessen uit incidenten?

Antwoord:
- Het nemen van (ad hoc) maatregelen 7x (4U,3H)
- Vertaling in adviezen voor leidinggevenden, 1x (1U)
- Aanpassing beleid/ procedures, 4x (1U,3H)
- Mededeling in personeelskrant, 1x (1H)
- Scholing medewerkers, 1x (1H)
- Geen maatregelen gezien uitzonderlijkheid voorvallen, 2x (2H)

Vraag 12.	***Vragenlijst Sociale veiligheid***
	Worden risico- of kwetsbaarheidanalyses binnen uw instelling uitgevoerd op het gebied van een sociale veiligheid?

Antwoord:
- Ja, 9x (6U,3H)
- Nee, 4x (4H)

Vraag 13.	***Vragenlijst Sociale veiligheid***
	Welke plannen zijn voorhanden ter bevordering van de sociale veiligheid?

Antwoord:
- RI&E, 3x (2U,1H)
- Bedrijfsnoodplan/ veiligheidsplan, 4x (4U)
- Anders, 3x (2U,1H)
- Geen, 7x (1U,6H)

Vraag 14.	***Vragenlijst Sociale veiligheid***
	Wat is de inbreng van externe bedrijven ten aanzien van sociale veiligheid?

Antwoord:
- Onderzoek en advies, 5x (4U,1H)
- Beveiliging, 7x (3U,4H)
- Opleiding en training, 1x (1U)
- Geen, 3x (1U,2H)

Vraag 15.	***Vragenlijst Sociale veiligheid***
	Kunt u een voorbeeld geven van een *best practice* ten aanzien van sociale veiligheid in uw instelling? *

* De antwoorden op deze vraag zijn in het rapport verwerkt.

Vraag 16.	***Vragenlijst Sociale veiligheid***
	Worden (kritische) op- of aanmerkingen over het beleid rond sociale veiligheid gestimuleerd vanuit de leiding van uw instelling?

Antwoord:
- Via de medezeggenschapsraad, 1x (1U)
- Via integriteitcoördinatoren/ vertrouwenspersonen, 1x (1U)
- Incidenteel, 1x (1U)
- Anders, 6x (3U,3H)
- Niet, 4x (4H)

Vraag 17.	***Vragenlijst Sociale veiligheid***
	Wat wordt binnen uw instelling ten aanzien van bewustwording van de sociale veiligheid gedaan richting studenten?

Antwoord:
- Voorlichting, 5x (3U,2H)
- Via vertrouwenspersonen/ decaan, 1x (1U)
- Klachtenloket, 1x (1U)
- Incidentele aandacht na incident, 2x (2H)
- Betrekken studenten bij beleidsontwikkeling terzake, 2x (1U,1H)
- Niets, 3x (2U,1H)

Vraag 18.	***Vragenlijst Sociale veiligheid***
	Wat wordt binnen uw instelling ten aanzien van bewustwording van de sociale veiligheid gedaan richting personeel?

Antwoord:
- Voorlichting, 7x (2U,5H)
- Training en cursussen voor personeel, 4x (2U,2H)
- Opstellen gedragscode, 3x (2U,1H)
- Incidentele aandacht na incident, 4x (1U,3H)
- Niets, 2x (2U)

Vraag 19.	***Vragenlijst Sociale veiligheid***
	In welke mate wordt in opleidingen aandacht geschonken aan veiligheids- en crisismanagement?

Antwoord:
- Opleiding studenten, 1x (1H)
- Opleiding medewerkers, 5x (5U)
- Anders, 2x (2H)
- Niet, 4x (1U,3H)

Vraag 20.	***Vragenlijst Sociale veiligheid***
	Indien oefeningen worden gehouden in het kader van veiligheids- en crisismanagement: wat is het karakter en de frequentie van deze oefeningen?

Antwoord:
- Crisismanagement, 2x (2U)
- Gericht op bhv en aspecten van fysieke veiligheid, 6x (3U,3H)
- Niet, 7x (1U,6H)

VRAGENLIJST ORGANISATIEVEILIGHEID

Vraag 1.	***Vragenlijst Organisatieveiligheid***
	Welke functie bekleedt u?

Vraag 2.	***Vragenlijst Organisatieveiligheid***
	Binnen welk onderdeel van de organisatie?

Vraag 3.	***Vragenlijst Organisatieveiligheid***
	Wat zijn uw exacte taken op het gebied van organisatieveiligheid?

Vraag 4.	***Vragenlijst Organisatieveiligheid***
	Wat zijn volgens u de grootste risico's rondom veiligheid in uw taakveld voor uw instelling?

Antwoord:
- Brand, 8x (4U,4H)
- Inbraak, 2x (1U,1H)
- RSI en ongevallen, 4x (1U,3H)
- Gebouwgebonden risico's, 3x (3U)
- Ongeoorloofde toegang, 4x (2U,2H)
- Geen, 2x (1U,1H)

Vraag 5.	***Vragenlijst Organisatieveiligheid***
	Welke ontwikkelingen ten aanzien van veiligheid in het hoger onderwijs ziet u in uw taakveld op de lange termijn?

Antwoord:
- Maatschappelijke ontwikkelingen die de onveiligheid vergroten, 3x (1U,2H)
- Meer voorzieningen treffen, 10x (5U,5H)
- "Gewone" risico's, 1x (1H)
- Beperking toegang, 1x (1U)
- Coördinerende en stimulerende taak HBO-raad, 1x (1H)
- Geen, 1x (1H)

Vraag 6.	***Vragenlijst Organisatieveiligheid***
	Welke prioriteit heeft veiligheid ten opzichte van andere taken binnen uw functie?

Antwoord:
- Hoge prioriteit, 8x (6U,2H)
- Gelijk gebleven, 6X (6H)
- Lage prioriteit, 2x (2H)

Vraag 7.	***Vragenlijst Organisatieveiligheid***
	Welke prioriteit krijgt het bevorderen van veiligheid in uw taakveld naar uw mening binnen uw instelling?

Antwoord:
- Neemt toe, 8x (4U,4H)
- Is gelijk gebleven, 5x (1U,4H)
- Is afgenomen, 1x (1H)
- Weet het niet, 2x (2H)

Vraag 8.	***Vragenlijst Organisatieveiligheid***
	Is de aandacht voor veiligheid in uw taakveld toe- of afgenomen in de afgelopen vijf jaar?

Antwoord:
- Toegenomen, 15x, (5U,10H)
- Weet het niet, 1x (1H)

Vraag 9.	***Vragenlijst Organisatieveiligheid***
	Registreert en analyseert u of anderen in uw instelling incidenten rond organisatieveiligheid?

Antwoord:
- Ja, 15x (5U,10H)
- Nee, 1x (1H)

Vraag 10.	***Vragenlijst Organisatieveiligheid***
	(indien onder 9. 'ja') Op welke wijze vindt registratie en analyse plaats?

Antwoord:
- Centraal, 14x (4U,10H)
- Decentraal, 1x (1U)

Vraag 11.	***Vragenlijst Organisatieveiligheid***
	Wat gebeurt binnen uw instelling met lessen uit incidenten?

Antwoord:
- Nemen van (ad hoc) maatregelen, 5x (3U,2H)
- Analyse, 4X (1U,3H)
- Betrekken personeel en studenten bij veiligheidsbeleid, 1x (1U)
- Aanpassing beleid, 3x (1U,2H)
- Informeren studenten en medewerkers, 1x (1H)
- Geen specifieke stappen gezien uitzonderlijkheid calamiteit, 2x (1U,1H)

Vraag 12.	***Vragenlijst Organisatieveiligheid***
	Worden risico- of kwetsbaarheidanalyses binnen uw instelling uitgevoerd op het gebied van een organisatieveiligheid?

Antwoord:
- Ja, 10x (4U,6H)
- Nee, 6x (1U,1H)

Vraag 13.	***Vragenlijst Organisatieveiligheid***
	Welke plannen zijn voorhanden ter bevordering van de organisatieveiligheid?

Antwoord:
- Bedrijfsnoodplan, 3x (2U,1H)
- Ontruimingsplan, 2x (2H)
- Communicatieplan, 1x (1U)
- Anders, 9x (4U,5H)
- Geen, 4x (1U,3H)

Vraag 14.	***Vragenlijst Organisatieveiligheid***
	Wat is de inbreng van externe bedrijven ten aanzien van organisatieveiligheid?

Antwoord:
- Risico-inventarisatie, 2x (1U,1H)
- Samenwerking met arbodienst, 3x (3H)
- Onderzoek en advies, 5x (2U,3H)
- Technisch onderhoud, 5x (4U,1H)
- Beveiliging, 2x (1U,1H)
- Geen, 2x (1U,1H)

Vraag 15.	***Vragenlijst Organisatieveiligheid***
	Kunt u een voorbeeld geven van een *best practice* ten aanzien van organisatieveiligheid in uw instelling? *

De antwoorden op deze vraag zijn in het rapport verwerkt.

Vraag 16.	***Vragenlijst Organisatieveiligheid***
	Worden (kritische) op- of aanmerkingen over het beleid rond organisatieveiligheid gestimuleerd vanuit de leiding van uw instelling?

Antwoord:
- Ja, 10x (6U,4H)
- Nee, 6x (6H)

Vraag 17.	***Vragenlijst Organisatieveiligheid***
	Wat wordt binnen uw instelling ten aanzien van bewustwording van de organisatieveiligheid gedaan richting studenten?

Antwoord:
- Betrekken bij oefeningen en trainingen, 4x (2U,2H)
- Voorlichting, 10x (5U,5H)
- Betrekken studenten bij vormgeven veiligheidsbeleid, 2x (2H)
- Als onderdeel van het curriculum, 4x (4H)
- Niets, 1x (1H)

Vraag 18.	***Vragenlijst Organisatieveiligheid***
	Wat wordt binnen uw instelling ten aanzien van bewustwording van de organisatieveiligheid gedaan richting personeel?

Antwoord:
- Betrekken bij oefeningen en trainingen, 5x (3U,2H)
- Voorlichting, 9x (4U,5H)
- Betrekken werknemers bij vormgeven veiligheidsbeleid, 1x (1H)
- Lid van de BHV-organisatie, 5x (2U,3H)
- Niets, 0x

Vraag 19.	***Vragenlijst Organisatieveiligheid***
	Wordt in opleidingen aandacht geschonken aan veiligheids- en crisismanagement?

Antwoord:
- Ja, 7x (2U,5H)
- Nee, 9x (4U,5H)

Vraag 20.	***Vragenlijst Organisatieveiligheid***
	Indien oefeningen worden gehouden in het kader van veiligheids- en crisismanagement: wat is het karakter en de frequentie van deze oefeningen?

Antwoord:
- Crisismanagement, 4x (3U,1H)
- BHV, 5x (4U,1H)
- Ontruiming, 9x (6U,3H)
- Geen, 4x (4H)

VRAGENLIJST KENNISVEILIGHEID

Vraag 1.	***Vragenlijst Kennisveiligheid***
	Welke functie bekleedt u?

Vraag 2.	***Vragenlijst Kennisveiligheid***
	Binnen welk onderdeel van de organisatie?

Vraag 3.	***Vragenlijst Kennisveiligheid***
	Wat zijn uw exacte taken op het gebied van ICT-veiligheid / fraude en misbruik / integriteit?

Vraag 4.	***Vragenlijst Kennisveiligheid***
	Wat zijn volgens u de grootste risico's rondom veiligheid in uw taakveld voor uw instelling?

Antwoord:
- Hackers, 3x (2U,1H)
- Kwetsbare infrastructuur, 5x (3U,2H)
- Kennisveiligheid, 2x (1U,1H)
- Onbevoegd toegang tot bestanden, 7x (1U,6H)
- Fraude, 1x (1H)
- Sabotage, 3x (3H)
- Virussen, 3x (1U,2H)
- Dataverlies, 1x (1H)
- Anders, 4x (3U,1H)
- Geen, 1x (1H)

Vraag 5.	***Vragenlijst Kennisveiligheid***
	Welke ontwikkelingen ten aanzien van veiligheid in het hoger onderwijs ziet u in uw taakveld op de lange termijn?

Antwoord:
- Additionele beleidsontwikkeling en middelen, 7x (2U,5H)
- Verbetering software, 1x (1H)
- Strengere toegangseisen, 6x (2U,4H)
- Internationalisering, 4x (3U,1H)
- Toegenomen kwetsbaarheid, 5x (2U,3H)
- Geen, 0x

Vraag 6.	***Vragenlijst Kennisveiligheid***
	Welke prioriteit heeft veiligheid ten opzichte van andere taken binnen uw functie?

Antwoord:
- Hoog, 9x (3U,6H)
- Gemiddeld, 7 (1U,6H)
- Laag, 0x

Vraag 7.	***Vragenlijst Kennisveiligheid***
	Welke prioriteit krijgt het bevorderen van veiligheid in uw taakveld (veilige ICT-omgeving, tegengaan fraude en misbruik, bevorderen integriteit) naar uw mening binnen uw instelling?

Antwoord:
- Hoog, 8x (4U,4H)
- Gemiddeld, 2x (2H)
- Laag, 6x (2U,4H)

Vraag 8.	***Vragenlijst Kennisveiligheid***
	Is de aandacht voor veiligheid in uw taakveld (ICT-omgeving / voorkomen van fraude of misbruik / integriteit) toe- of afgenomen in de afgelopen vijf jaar?

Antwoord:
- Toegenomen, 16X (5U,11H)
- Gelijk gebleven, 0x

Vraag 9.	***Vragenlijst Kennisveiligheid***
	Registreert en analyseert u of anderen in uw instelling incidenten rond ICT-verstoringen / fraude en misbruik / integriteit?

Antwoord:
- Ja, 14x (5U,9H)
- Nee, 2x (2H)

Vraag 10.	***Vragenlijst Kennisveiligheid***
	(indien onder 9. 'ja') Op welke wijze vindt registratie en analyse plaats?

Antwoord:
- Systematisch, 7x (4U,3H)
- Incidenteel, 9x (1U, 8H)

Vraag 11.	***Vragenlijst Kennisveiligheid***
	Wat gebeurt binnen uw instelling met lessen uit incidenten?

Antwoord:
- Nemen van (ad hoc) maatregelen (bijvoorbeeld versterking beveiliging), 10x (3U,7H)
- Analyse, 3x (2U,1H)
- Aanpassing netwerkreglement/ procedures, 3x (1U,2H)
- Geen verdere stappen, 1x (1U)

Vraag 12.	***Vragenlijst Kennisveiligheid***
	Worden risico- of kwetsbaarheidanalyses binnen uw instelling uitgevoerd op het gebied van een veilige ICT-omgeving / fraude- en misbruikgevoeligheid / integriteitrisico's?

Antwoord:
- Ja, systematisch, 3x (1U,2H)
- Ja, afwisselend, 7x (1U,6H)
- Nee, 6x (3U,3H)

Vraag 13.	***Vragenlijst Kennisveiligheid***
	Welke plannen zijn voorhanden ter bevordering van een veilige ICT-omgeving / tegengaan van fraude en misbruik / bevorderen integriteit?

Antwoord:
- Formele beleidsplannen, 6x (5U,1H)
- Gebruikersprotocol, 1x (1H)
- Geen, 9x (9H)

Vraag 14.	***Vragenlijst Kennisveiligheid***
	Wat is de inbreng van externe bedrijven ten aanzien van veiligheid?

Antwoord:
- Inhuur capaciteit, 3x (3U)
- Onderzoek en advies, 10x (3U,7H)
- Geen, 5x (1U,4H)

Vraag 15.	***Vragenlijst Kennisveiligheid***
	Kunt u een voorbeeld geven van een *best practice* ten aanzien van veiligheid binnen uw taakveld (ICT-omgeving / voorkomen fraude en misbruik / bevorderen integriteit) in uw instelling? *

* De antwoorden op deze vraag zijn in het rapport verwerkt.

Vraag 16.	***Vragenlijst Kennisveiligheid***
	Worden (kritische) op- of aanmerkingen over het beleid rond veiligheid (een veilige ICT-omgeving / tegengaan van fraude en misbruik / bevorderen integriteit) gestimuleerd vanuit de leiding van uw instelling?

Antwoord:
- Ja, gestimuleerd, 11x (4U,7H)
- Nee, maar er wordt wel naar klachten/ opmerkingen geluisterd, 2x (1U,1H)
- Nee, 3x (3H)

Vraag 17.	***Vragenlijst Kennisveiligheid***
	Wat wordt binnen uw instelling ten aanzien van bewustwording van de veiligheid (een veilige ICT-omgeving / tegengaan van fraude en misbruik / bevorderen integriteit) gedaan richting studenten?

Antwoord:
- Netwerkreglement, 8x (3U,5H)
- Voorlichting, 8x (5U,3H)
- Aanspreken studenten op nalatig gedrag, 1x (1H)
- Aanwezigheid instructeurs en aandacht in college, 1x (1H)
- Sanctie na incident, 1x (1H)
- Niets, 0x

Vraag 18.	***Vragenlijst Kennisveiligheid***
	Wat wordt binnen uw instelling ten aanzien van bewustwording van de veiligheid (een veilige ICT-omgeving / tegengaan van fraude en misbruik / bevorderen integriteit) gedaan richting personeel?

Antwoord:
- Voorlichting, 7x (4U,3H)
- Collegiaal aanspreken, 1x (1H)
- Reglementen/ protocollen, 7x (2U,5H)
- Niets, 1x (1H)

Vraag 19.	***Vragenlijst Kennisveiligheid***
	Wordt in opleidingen aandacht geschonken aan veiligheids- en crisismanagement?

Antwoord:
- Ja, voor studenten, 4x (2U,2H)
- Ja, voor medewerkers, 4x (2U,2H)
- Nee, 8x (1U,7H)

Vraag 20.	***Vragenlijst Kennisveiligheid***
	Indien oefeningen worden gehouden in het kader van veiligheids- en crisismanagement: wat is het karakter en de frequentie van deze oefeningen?

Antwoord:
- Crisismanagementoefening, 1x (1U)
- Rampenoefening/ ontruimingsoefening, 4x (2U,2H)
- Regelmatige oefening met afbreken netspanning en backup-tapes, 1x (1H)
- Oefening vanuit de dagelijkse praktijk, 1x (1H)
- Geen, 9x (2U,7H)

BIJLAGE V
VERSLAG BESTUURLIJKE BIJEENKOMST

Op 13 mei 2004 vond een bestuurlijke conferentie plaats waarin de conceptrapportage van het onderzoek besproken werd.

Voor deze bijeenkomst waren alle colleges en raden van bestuur van hoger onderwijsinstellingen alsmede de besturen van de onderzoeksinstellingen uitgenodigd door het ministerie.

De volgende zaken zijn tijdens de bestuurlijke conferentie aan de orde gekomen:

- Het eerder geconstateerde beeld, dat het hoger onderwijs geen structurele aandacht heeft voor integraal veiligheids- en crisismanagement, werd bevestigd. De aanwezigen onderschreven de noodzaak om hiertoe te komen. Inzet van koepelorganisaties en ministerie werd daarbij door de aanwezigen gewenst.

- Binnen instellingen is op deelaspecten zoals beveiliging en arbo (inclusief BHV) wel aandacht voor veiligheidsmanagement, maar de mate waarin verschilt per instelling. Kwetsbaar punt is het beperkte veiligheidsbewustzijn van studenten, docenten en medewerkers.

- Toenemende druk werd gevoeld door de instellingen vanuit ‘externen’ (gemeenten, verzekeraars, arbodiensten) om te komen tot extra inspanningen op het gebied van risicobeheersing.

- Aanvullende wet- en regelgeving ter verbetering van de veiligheidssituatie achten de instellingen onwenselijk. Ze voelen zich al sterk gebonden door allerlei bestaande bepalingen, die soms het primaire proces (opleiden en onderzoeken)bemoeilijken (zoals de arbo-regelgevinggeving)

- De aanwezigen vanuit het hoger onderwijs onderkenden nog onvoldoende in staat te zijn om maatschappelijke tendensen (internationalisering, toenemende agressie, etc.) zelfstandig en gezamenlijk te vertalen naar risico’s binnen de instellingen.

- Best practices kwamen uitgebreid aan de orde vanuit de gevoelde noodzaak deze te delen. Als in eerdere bijeenkomsten werd gevraagd om een platform waarbinnen kennis gedeeld kan worden. Zo’n platform bestaat nu feitelijk alleen voor de hoofden beveiliging binnen de universiteiten. Een hiermee samenhangende wens was om te komen tot een vorm van (onderlinge) audits die vanzelfsprekend toekomstgericht zouden moeten zijn.

- Spanning werd gevoeld tussen inzet op enerzijds sociale veiligheid en kennisveiligheid en anderzijds de ‘openheid van instituties’ die in de perceptie nodig is voor goed onderwijs en onderzoek. Screening van studenten of docenten vindt bijvoorbeeld daarom nauwelijks plaats.

- Slecht zicht bestaat er binnen het hoger onderwijs op de achtergronden van personen in kwetsbare functies, zoals assistent-beheerders van laboratoria, schoonmaakpersoneel etc. die toegang hebben tot kwetsbare delen van de instellingen.

BIJLAGE VI
DEELNEMERSLIJST OPERATIONELE BIJEENKOMST 8 APRIL 2004

Aanwezigen op de workshop Operationele Aspecten van Veiligheid in het Hoger Onderwijs en Wetenschappelijk onderzoek gehouden op de Universiteit van Amsterdam op 8 april 2004:

- de heer Van Eijk, Universiteit van Tilburg
- de heer Hooglugt, Katholieke Universiteit Nijmegen
- mevrouw Jahnke, Technische Universiteit Eindhoven
- de heer Janssen, Universiteit van Amsterdam
- de heer Kagie, Universiteit Maastricht
- de heer Klein, Rijksuniversiteit Groningen
- de heer Klous, Vrije Universiteit
- de heer Van Kuijk, Universiteit Utrecht
- de heer Lukkien, Hanzehogeschool Groningen
- de heer Van der Meer, Technische Universiteit Delft
- mevrouw Reinders, Hotelschool Den Haag
- de heer Van Scherrenburg, Universiteit Wageningen
- de heer Velthuizen, Katholieke Universiteit Nijmegen
- de heer Verkaar, Universiteit Leiden
- de heer Versluis, Universiteit Utrecht
- de heer Weustink, Universiteit Twente
- mevrouw Winkler, Universiteit Twente

Namens het Ministerie van Onderwijs, Cultuur en Wetenschap was aanwezig de heer Oevering.

Namens het COT Instituut voor Veiligheids- en crisismanagement waren aanwezig de heren Helsloot, Ruitenberg, Jong en Verhaar

BIJLAGE VII
DEELNEMERSLIJST BESTUURLIJKE BIJEENKOMST 13 MEI 2004

Aanwezigen op de bijeenkomst Beleidsmatige Aspecten van Veiligheid in het Hoger Onderwijs en Wetenschappelijk Onderzoek gehouden op het Congrescentrum 'De Reehorst' op 13 mei 2004:

- mevrouw Borger, manager ondersteunende diensten, Hogeschool Zuyd
- de heren Braamhaar, hoofd Facilitaire Diensten, en Bloem, unitmanager Service en perszaken, Hogeschool Drenthe
- de heer Codée, manager onderwijsondersteuning, Hogeschool de Driestar Gouda
- de heer Geerken, directeur organisatie en planning, NWO
- de heer Van Helden, faculteit wis- en natuurkunde, Universiteit Leiden
- de heer Houben, Lid CvB, Hogeschool Fontys
- mevrouw Jahnke, hoofd BHV , Technische Universiteit Eindhoven
- de heer Janssen, hoofd beveiliging, Universiteit van Amsterdam
- de heer Jobse, Hogeschool IPABO
- de heer De Jongh, hoofd ICT, Hotelschool Den Haag
- mevrouw Knol, VNG
- de heer Labruyère, CvB, Hogeschool Inholland
- de heer Van Loosbroek, Universiteit van Tilburg
- de heer Mulders, voorzitter CvB, Hogeschool Edith Stein
- de heer Nuboer, HBO-Raad
- de heer Nugteren, hoofd afdeling Algemeen Bestuurlijke Zaken, Universiteit Utrecht
- mevrouw Schallies, Hogeschool van Utrecht
- de heer Stefens, sectorhoofd, Open Universiteit
- de heer Van der Wel, directeur Facilitaire Diensten, Hogeschool Rotterdam
- mevrouw Winkler, PA&O, Universiteit Twente
- de heer Van Winsen, arbo & milieuservices, Technische Universiteit Delft

Namens het Ministerie van Onderwijs, Cultuur en Wetenschap waren aanwezig de heren Vrolijk, Roborgh, Van Kouterik, Remmerswaal, Bonnink en Oevering.

Namens het COT Instituut voor Veiligheids- en crisismanagement waren aanwezig de heren Rosenthal, Helsloot, Ruitenberg, Jong en Verhaar

BIJLAGE VIII

LEDENLIJST BEGELEIDINGSGROEP

In het beginstadium van dit onderzoek is de onderzoeksopzet en de conceptrapportages doorgesproken met een door het ministerie ingestelde begeleidingsgroep. Deze groep bestond uit de volgende personen:

- De heer P.A. Binsbergen, secretaris college van bestuur, Universiteit Twente
- De heer J. Bonnink, ministerie Onderwijs, Cultuur en Wetenschap
- De heer J.P.G. Janssen, hoofd beveiliging, Universiteit van Amsterdam
- De heer Th. van Kouterik, ministerie Onderwijs, Cultuur en Wetenschap
- De heer M.W. Leeuw, hoofd biologisch en chemisch onderzoek,
  Prins Maurits Laboratorium TNO
- De heer B. Mast, Adviseur arbo, veiligheid en milieu, Hogeschool Leiden
- De heer L. Mooij, ministerie van Onderwijs, Cultuur en Wetenschap
- De heer K. van der Wal, directeur financieel economische zaken, Hanzehogeschool Groningen

BIJLAGE IX
GEÏNTERVIEWDE PERSONEN

In het kader van dit onderzoek zijn met de volgende personen diepte-interviews gehouden:

- BPRC, de heer R. Bontrop, Directeur
- FOM, de heer P. Louwrier, hoofd Arbo
- Hanzehogeschool Groningen, de heer K. van der Wal, Directeur Financieel Economische Zaken
- Hogeschool Leiden, de heer B. Mast, Adviseur Arbo, Milieu en Veiligheid
- KNAW, de heer C. Moen, Algemeen directeur en de heer De Hen, Directeur Juridische Zaken
- Koninklijke Bibliotheek, de heer J. Steenbakkers, Directeur bedrijfsvoering en informatietechnologie
- NWO, de heer B. Geerken, Directeur P&O en de heer A. van Geest, Hoofd bedrijfsvoering
- Prins Maurits Laboratorium TNO, Matthijs Leeuw, Hoofd biologisch en chemisch onderzoek
- Universiteit van Amsterdam, de heer J. Janssen, Hoofd beveiliging
- Universiteit Twente, de heer P. Binsbergen, Secretaris College van Bestuur
- Verbond voor Verzekeraars, de heer P. Vogelsang,