PLAN TOT IMPLEMENTEREN VAN INTEGRAAL VEILIGHEIDSMANAGEMENT OP DE UT
1E FASE: RAPPORTAGE UITGEVOERDE QUICK SCAN

Opsteller: J.I.M. Halman
11 oktober 2019

SAMENVATTING EN VOORUITBLIK

Afspraken binnen het kader van de VSNU ten aanzien van veiligheid zijn:
- Hoger onderwijsinstellingen nemen de verantwoordelijkheid voor het organiseren van integraal veiligheidsbeleid om een veilig leef, leer- en werkklimaat en bedrijfscontinuïteit in extreme omstandigheden te waarborgen.
- Veiligheidsbeleid in het hoger onderwijs is integraal: kosten en baten van veiligheidsmaatregelen worden onderling vergeleken zodat alleen de meest verstandige een plaats krijgen.

Om conform bovenstaande afspraken binnen de UT Integraal Veiligheidsmanagement te implementeren, wordt een voorstel uitgewerkt voor de inrichting en monitoring van Integraal Veiligheidsmanagement op de UT. Hierbij wordt de navolgende fasering aangehouden:

1e Fase: Starten met een Quick Scan: in kaart brengen van de status quo op het gebied van veiligheidsmanagement op de UT
2e Fase: Externe oriëntatie en het opstellen van een plan voor de inrichting van integraal veiligheidsmanagement op de UT
3e Fase: Opstellen van een plan voor de monitoring en het borgen van integraal veiligheidsmanagement binnen de UT

Deze rapportage bevat een verslaglegging van de 1e Fase. Gesproken is met 26 personen binnen de UT-gemeenschap die verantwoordelijkheid dragen op het gebied van veiligheid.
Uit de gehouden interviews blijkt dat er een groot draagvlak bestaat voor het implementeren van Integrale Veiligheid binnen de UT. Het onderwerp wordt als bijzonder belangrijk gezien voor de UT.

Op basis van de gehouden Quick Scan concludeer ik dat voor het vervolgtraject de navolgende onderwerpen in ieder geval met prioriteit moeten worden aangepakt:

- Het ontwikkelen van continuïteitplannen voor het primaire proces van de UT. In het geval Osiris uitvalt dor een calamiteit of cyberaanval, zal een belangrijk deel van het onderwijs geen doorgang kunnen vinden
- Een integrale benadering van veiligheid door de relatie tussen cybersecurity en de andere veiligheidsaspecten nadrukkelijker te beschouwen en uit te werken
- Het uitwerken van een protocol en de organisatie en inrichting van veiligheidsrisico's veroorzaakt door medewerkers of studenten die in psychische nood verkeren
- Het verhogen van de bewustwording op het gebied van Integrale Veiligheid onder medewerkers en studenten
- Uitwerken wat de implicaties van internationaliseren zijn voor het succesvol invoeren van Integrale Veiligheid op de UT
- Het verhogen van de verkeersveiligheid op de campus
- Het verhogen van het anticiperend vermogen op moeilijk te voorziene veiligheidsissues door het periodiek uitvoeren van scenarioanalyses
- Het inbedden van Integrale Veiligheid door dit op te nemen in de Planning & Control cyclus van de UT

1e Fase: Quick scan Rapportage Integrale Veiligheid UT

Opsteller: J.I.M. Halman
11 oktober 2019

In de periode 22 juli 2019 – 4 september 2019 hebben interviews plaatsgevonden met belangrijke portefeuillehouders voor veiligheidsmanagement aan de UT.

In totaal zijn gesprekken gevoerd met 26 personen binnen de UT gemeenschap: De leden van het College van Bestuur; de secretaris van het CvB; David Korringa, directeur Bedrijfsvoering ET; Marion Kamp directeur Bedrijfsvoering BMS; Christy Schoonheijt-Oude Veldhuis, directeur Bedrijfsvoering TNW; Stephan Maathuis, directeur Bedrijfsvoering EEMCS; Ton Veldkamp en Annemarie Arets van het ITC; Joost Sluijs, directeur HR; Jan Laurens Lasonder, directeur LISA; Pim Fij, directeur Campus & Facility Management; Hans Oeloff directeur van het CES; Benno Kiers, hoofd Beveiliging UT; Henk Swaters, Afdelingshoofd Demand Supply Management, Richard Sanders, Safety officer HRM; Henk Bleijerveld, Emergency response coördinator UT; Peter Peters, Security management LISA; Bertus Dierink VGM-TNW; Nancy Heijnekamp (VGM-ET) en Herman Kuiper (CFM-ET); Andries Klijnstra Facilitair teamleider van de gebouwen Vrijhof, Ravelijn, Cubicus en Citadel; Marco Boevink (CFM), Ellen Giebels van BMS en Rogier Jansen van de AIVD Oost-Nederland.
Van elk gehouden interview is een verslag gemaakt die vervolgens is teruggekoppeld naar de geïnterviewden met het verzoek tot correctie en/of aanvulling.

Doel van de interviews is geweest om de zienswijzen van de portefeuillehouders op het gebied van Integrale Veiligheid in kaart te brengen. Gevraagd werd wat naar hun oordeel voor wat betreft de verschillende aspecten van veiligheid voorspoedig loopt; wat verbetering behoeft; op welke wijze monitoring van veiligheid plaatsvindt en waar men de noodzaak ziet tot uitbreiding en integratie van veiligheidsaspecten. In deze rapportage wordt ingegaan op de belangrijkste uitkomsten van de gehouden interviews.

Hierbij is de navolgende indeling aangehouden:

1. Algemeen, uitgangspunten ten aanzien van Integrale Veiligheid
2. Cyber security
3. Gebouwen en laboratoria
4. Campus
5. Werknemers en studenten
6. Integriteit en ethisch handelen
7. Internationalisatie
8. Reputatierisico's
9. Politieke veiligheid
10. Systemen voor het monitoren van de veiligheid op de UT
11. Inrichting en organisatie van Integrale Veiligheid
12. Bewustwording op het gebied van Integrale Veiligheid bij medewerkers en studenten
13. Oefenen van crisissituaties
14. Overige voorstellen op het gebied van Integrale Veiligheid
15. Conclusie en vervolg

1. Algemeen

Als universiteit streven we na een instelling te zijn van “open science” en “open access”. Veiligheid is als aandachtsgebied de afgelopen jaren in belang en omvang gegroeid. Belangrijke ontwikkelingen op de UT zoals een toenemende graad van digitalisering en internationalisering en het feit er in de afgelopen periode een paar serieuze incidenten zijn geweest op het gebied van fysieke en/of psychische veiligheid, hebben hiertoe bijgedragen. Door een toenemende internationalisering ontstaan steeds weer nieuwe platforms. Dit alles maakt het steeds makkelijker om op wereldschaal met elkaar samen te werken. Echter, we zullen bij deze toenemende transparantie ook de veiligheid moeten kunnen garanderen. Hierbij spelen zaken als het bewaken van de privacy, open databeleid, het beheer van patenten en de interactie met het bedrijfsleven.
Een belangrijk principe bij het implementeren van Integrale Veiligheid op de UT moet zijn: Hoe bevorder je bewustwording en adequaat handelen van organisatie, medewerkers en studenten ten aanzien van integrale veiligheid, zonder dat dit verlammend werkt?

2. Cybersecurity

Bij Integrale Veiligheid is het belangrijk om de relatie tussen cybersecurity en de andere veiligheidsaspecten te analyseren. Erg veel verloopt tegenwoordig immers via het ICT-netwerk. We hebben een enorme afhankelijkheid opgebouwd van ICT. Bij een eventuele “aanval” waarbij de veiligheid van de UT gevaar loopt, is de kans reëel dat het zal gaan om een dubbele aanval (ook het uitschakelen van het ICT-netwerk) met hierdoor een dubbel risico.
Er bestaan duidelijke raakvlakken tussen de verschillende aspecten van veiligheid. Dit noodzaakt tot een integrale benadering van veiligheid. Het fysiek beveiligen van bijvoorbeeld het BMS-lab is bedoeld om de IT-apparatuur en de privacygevoelige data in dit lab te beveiligen. Evenzo is de beveiliging van ons datacentrum zowel een IT-security aangelegenheid als een fysieke ter voorkoming van inbraak en diefstal van de daar aanwezige apparatuur en opgeslagen data. Tijdens een van de crisisoefeningen door het Centrale crisisteam werd een ongeval geoefend waarbij een potentiële fysieke ernstige storing in een zuurkast geïnitieerd werd middels het netwerk. Het fysieke en het digitale raken steeds meer met elkaar verweven.

Op het gebied van Cybersecurity is er een CERT-UT (Computer Emergency Response Team). Daarnaast neemt de UT ook actief deel aan security voor het SURF netwerk in CERT-SURF. Bij Cybersecurity is het van groot belang om de trends en mogelijke dreigingen continu te volgen. China, Rusland en ook Iran zijn geavanceerd bezig. Als UT moeten we zowel aandacht hebben voor de medewerkers en studenten die frequent of voor een periode in het buitenland zijn als voor medewerkers en studenten die komen uit landen die actief bezig zijn met spionageactiviteiten. De UT maakt gebruik van het “Quarantainenet” met geavanceerde software waarmee vreemd computergedrag van medewerkers en studenten kan worden opgespoord. Het quarantainenet is in het verleden ontwikkeld door “Tesorion” (www.tesorion.nl), een startup van de UT. Daarnaast werkt LISA samen met de “Twente Hackers squad” een groep van studenten en promovendi van de UT die geïnteresseerd zijn in het opsporen van lekken in het computernetwerk. De UT heeft een procedure voor “responsible disclosure” waarmee lekken in het computernetwerk en -applicaties van de UT gemeld kunnen worden. De melder kan een eervolle vermelding krijgen als hij/zij dat wil. Het oplossen van de geconstateerde kwetsbaarheden wordt bewaakt in de security kwartaal rapportage. De UT neemt binnen surfnet-verband actief deel aan cybercrisisoefeningen zoals OZON (https://www.surf.nl/ozon-oefen-hoe-je-bij-een-cybercrisis-reageert) en kleinere oefeningen zoals NOZON (https://www.surf.nl/agenda/voorbereidingsbijeenkomst-cybercrisisoefening-nozon-2019).

Als organisatie zijn we wellicht teveel gefocust op de typen van (on)veiligheid waar we al bekend mee zijn. Door de toenemende digitalisering dienen zich echter ook nieuwe issues aan, zoals de persoonlijke veiligheid van medewerkers, bijvoorbeeld door bedreiging via internet en sociale media. Een externe persoon of ex-medewerker kan negatieve commentaren plaatsen over een medewerker op internet (facebook, instagram, twitter etc.). Dit heeft niet alleen een enorme impact op de betreffende medewerker maar indirect ook op de UT als geheel. Hoe hierop adequaat en voortvarend te handelen is een issue, als UT hebben we dit nog niet goed op orde.

3. Gebouwen en laboratoria

Een vraag die van belang is als het gaat om de fysieke veiligheid van gebouwen en laboratoria: Is de toegang tot werkruimten en alle laboratoria wel goed geregeld? De toegang tot het gebouw en het toegangssysteem tot het gebouw worden vanuit de facilitaire organisatie beheerd. Het is essentieel dat er heldere afspraken zijn tussen de facilitaire organisatie en de directeur bedrijfsvoering met betrekking tot de uitgifte van sleutels voor de toegang tot het gebouw, de toegang tot kantoorkamers en andere ruimten en het al dan niet uitlenen van een loper.

Sommige ruimten op de campus, zoals de cleanrooms, hogedruklab, overige speciale labs en de gasopslag, etc. verdienen extra aandacht vanwege de gevaarlijke stoffen waarmee gewerkt wordt. Een aantal van de chemicaliën in de laboratoria zijn te typeren als gevaarlijke, soms ook kankerverwekkende stoffen. Belangrijk is het bijhouden van een register met de personen die in aanraking komen met deze stoffen. De ene onderzoeker is heel frequent in contact met deze gevaarlijke stoffen terwijl een andere onderzoeker maar 1-2 keer per jaar hiermee in aanraking komt. Er ontbreekt nu inzicht in het contactpatroon per medewerker met deze gevaarlijke stoffen. Op dit moment voldoen we als UT niet aan de vigerende wetgeving en bevinden we ons in een “grijs gebied” hetgeen voor alle Universiteiten overigens geldt. Voor de UT ligt hier een aandachtspunt voor verbetering.
Bij het aanstellen van promovendi en medewerkers die komen te werken in laboratoria met een verhoogd veiligheidsrisico zal vooraf ook de kennis met betrekking tot veiligheid moeten worden vastgesteld. Bij TNW worden promovendi per vakgroep opgeleid hoe met gevaarlijke chemicaliën moet worden omgegaan. Toegang tot de laboratoria kan alleen via de ARBO/Milieu coördinator van de desbetreffende vakgroep. Daarnaast is er vier keer per jaar een introductie voor medewerkers van TNW waarin ook aandacht wordt besteed aan de veiligheid in het omgaan met giftige chemicaliën. De opkomst van de introductiesessies is redelijk, zo’n 60-70% neemt hieraan deel.

Alle gebouwen beschikken over een BMI (BrandMeldingsInstallatie) en een OAI (OntruimingsAlarmInstallatie). Daarnaast beschikken een aantal van de gebouwen (Carre, de Horst, Ravelijn en de Technohal) over een SMI (SprinklerMeldInstallatie). Met het Picasse systeem van de UT kunnen leden van de BHV teams of leden van de (decentrale en centrale) crisisteams snel telefonisch worden opgeroepen.

Alle BHV teams zijn op sterkte en hebben ook een systeem dat elk gebouw een ”buddy-gebouw” heeft. Dus als er in een gebouw tijdens een calamiteit te weinig BHVers zijn, gaat er een automatische melding voor ondersteuning naar het buddy gebouw. De teams hebben genoeg middelen om hun functie te kunnen uitvoeren. Bezuinigingen zijn tot op heden bij de UT niet van toepassing omdat er genoeg bewustwording is over het belang van BHV-teams bij het CvB, de dienstdirecteuren en decanen. De BHV teams Horst en Carré oefenen 10 keer per jaar gedurende twee uur een ongevalssituatie onder begeleiding van twee instructeurs. Na afloop vindt evaluatie plaats: wat ging goed, wat zou beter kunnen. De overige teams oefenen 6 keer per jaar. De BHV

coördinator houdt een ongevallen register bij. Afgelopen jaar hebben zich zo'n 75 ongevallen voorgedaan. De meest voorkomende ongevallen zijn het onwel worden van een medewerker of student, een epileptische aanval of een verwonding die iemand oploopt. Drie keer heeft een BHV team assistentie kunnen verlenen omdat iemand een hartstilstand opliep. De in de gebouwen aanwezige AED (Automatische Externe Defribillator) apparaten die het hartritme kunnen herstellen na een hartstilstand, worden regelmatig gecontroleerd. De persoon die een ernstig ongeval is overkomen, wordt per ambulance meegenomen voor verdere controle in het ziekenhuis.

De BHV medewerkers bij de teams Carre en Horst volgen op jaarbasis zo'n 20 uur aan training, exclusief de ademlucht trainingen met een Brandweer instructeur. Voor de andere teams geldt 12 uur training per jaar voor de medewerkers. Jaarlijks volgen ook zo'n 150 studenten de BHV opleiding en zo'n 150 studenten krijgen een herhaal training. De studenten melden zich aan als vrijwilliger. Studenten op de UT die bij hun vereniging achter de bar werken krijgen een opleiding verantwoord alcohol schenken. In deze cursus wordt ook geleerd hoe je moet omgaan met dronken bezoekers. Beide opleidingen vinden regelmatig plaats omdat er jaarlijks wisselingen bij de studenten plaatsvinden.

Om het gevaar van het uitbreken van brand in gebouwen te voorkomen moeten we verantwoorder omgaan met voorzieningen zoals kachels na werktijd uitzetten, geen illegale koffiezetapparaten gebruiken en het bewaken van de veiligheid in laboratoriumfaciliteiten. We zullen elkaar hierbij periodiek moeten 'wakker schudden'. In het Horstgebouw brak er enige tijd terug brand uit door oververhitting van een 3D printer. Tegen de vigerende regels in was het Lab met de 3D printer tijdens het printen onbezet. Door dit incident is er weer extra aandacht voor het bewaken van de veiligheid in de laboratoria.
Met enige regelmaat vinden er gebouwrondes plaats waarbij gecontroleerd wordt op de werking van de brandslangen en of er eventuele blokkades zijn in de gebouwen die bij het zich voordoen van een calamiteit of crisissituatie een hindernis kunnen vormen bij de hulpverlening.
Voor het organiseren van activiteiten in gebouwen is toestemming noodzakelijk van de gebouwbeheerder. De besturen van de studieverenigingen zijn zich bewust van wat wel en niet kan tijdens een door hen georganiseerde borrel of event. Hiertoe vindt op regelmatige basis overleg plaats met de gebouwbeheerder en de betreffende studieverenigingen.
In de stad is de "Pakkerij" in gebruik bij vier studentenverenigingen. Deze vier ruimten vallen onder verantwoordelijkheid van de Student Union. CFM is verantwoordelijk voor de algemene entreeruimte. In alle ruimten zijn camera's opgehangen zodat achteraf bij een eventueel incident kan worden nagegaan welke personen hierbij betrokken waren. Binnen de "Beheercommissie Pakkerij (BCP)" vindt maandelijks overleg plaats over het onderhoud en de veiligheid van de Pakkerij, de organisatie van bedrijfshulpverleners (BHVers), feesten die zullen plaatsvinden en eventuele incidenten die zich hebben voorgedaan. De Beheercommissie Pakkerij is samengesteld uit leden van de sociëteitsbesturen van de vier Pakkerijverenigingen, een Facilitair teamleider van het CFM, de portefeuillehouder Accommodatie van de Student Union en een coördinator ARBO en Hoofd BHV van de UT. De BCP brengt jaarlijks een jaarverslag uit.

Studenten werken buiten de campus ook in eigen werkplaatsen. Zo is er een werkplaats waar men experimenteert met waterstof en heeft ook het solarteam van studenten van de UT een werkplaats buiten de campus. Mocht zich in een dergelijke werkplaats een ongeval voordoen dan zal in de media zeker ook een discussie ontstaan of de UT hierin tekort geschoten is. Het is daarom van belang om studententeams die werken in dit soort werkplaatsen bewust te maken van de mogelijke risico's en bekend te maken waar zij op de UT terecht kunnen voor ondersteuning.

4. *Campus en terrein*

CFM is verantwoordelijk voor het waarborgen van de veiligheid bij evenementen en activiteiten die op de campus plaatsvinden. Een van de grootste evenementen is de jaarlijkse Batavierenrace. Dit jaar hebben ruim 8500 studenten deelgenomen aan de Batavierenrace waarvan een groot deel ook blijft slapen in het sportcentrum en in tenten op de campus. Aan het afsluitende feest nemen zo'n 12.000 studenten deel. Voor een dergelijk evenement huurt de afdeling CFM zo'n 30 veiligheidsbewakers in. Maar absolute veiligheid, ook met deze extra veiligheidsbewakers is natuurlijk niet te garanderen.

De servicedesks bij de ingangen van de gebouwen zijn getraind om goed te kijken wie er allemaal binnen komt. Door onvoorzichtigheid (open laten staan van kantoorkamer en bij studentenwoningen de eigen kamer) kan er makkelijk worden ingebroken en laptops e.d. worden gestolen. Dit gebeurt met de nodige regelmaat. Tijdens de "Kick in" dagen worden nieuwe studenten geattendeerd op de mogelijkheid van diefstal, maar ook het gevaar van brand. Politie en brandweer doen mee met de voorlichting tijdens de jaarlijkse Kick in. Toch zie je pas een gedragsverandering optreden als zich in de directe omgeving van een student of van een medewerker een diefstal of ander incident heeft voorgedaan. Ook de toenemende criminaliteit ten gevolge van de drugshandel, die ook op de campus van de UT plaatsvindt (o.a. bij festivals) is een zorg. Veel van de criminelen zijn bekenden van de Politie. Vanuit de beveiliging wordt hier goed op gelet. Er dient binnen dit kader een goede afstemming te zijn tussen de beveiligers van de UT en de Politie, zodat ook snel geëscaleerd kan worden wanneer zich een potentiële crisissituatie voordoet. De relatie tussen de beveiliging en de Politie is op dit moment goed, de Politie is goed bereikbaar en snel ter plekke.

Een aandachtspunt betreft de verkeersveiligheid op de campus. Op de campus van de UT vinden er met enige regelmaat verkeersongelukken plaats op lastige verkeerspunten (kruisingen van fietser en auto's). Er is sprake van een stijgende trend. Conform gegevens van de Beveiliging werden in de periode tussen januari 2013 – februari 2019, 130 ongevallen geregistreerd, ongeveer 20 ongevallen per jaar. In 50% van de gevallen was sprake van letsel bij één van de betrokkenen. Er zijn bij gevaarlijke kruisingen wel knipperende driehoeken geïnstalleerd, maar de voorrang van de fietsers leidt niet per definitie tot een veiliger situatie. Snelle fietsen en e-bikes kunnen opeens onverwacht voor een kruisende auto verschijnen. Aan het bedrijf Keypoint is gevraagd een advies uit te brengen hoe de verkeersveiligheid op de campus te verhogen. Dit onderzoek loopt nog.

5. Werknemers en studenten

Naast zorg voor de fysieke veiligheid is ook de geestelijke veiligheid een belangrijk onderwerp voor Integrale Veiligheid. In dit verband spelen zaken zoals hoe om te gaan met ongewenste intimiteit, psychische intimidatie en hoe dit soort zaken bespreekbaar te maken.
Bij de introductie van een nieuwe medewerker zal deze uitvoerig voorgelicht moeten worden over welke zienswijze de UT heeft met betrekking tot de zorg voor een inclusieve, veilige en gezonde werkomgeving en wat binnen dit kader van een medewerker of leidinggevende verwacht mag worden. Hetzelfde moet ook gebeuren tijdens de Kickin die georganiseerd wordt om nieuwe studenten wegwijs te maken op de UT. Ofschoon positief en zeker belangrijk bij de introductie, voor de bewustwording en internalisering is dit onvoldoende. De zienswijze van de UT met betrekking tot een inclusieve, veilige en een gezonde werkomgeving zal met enige regelmaat per jaar onder de aandacht dienen te worden gebracht.

Naar aanleiding van de #MeToo discussie en aanbevelingen van de arbeidsinspectie is er een agressieprotocol voor de UT uitgewerkt. Dit document beschrijft welk gedrag de universiteit wel en niet tolereert en wat de procedures en sancties in deze gevallen zijn. De nieuwe maatregelen richten zich niet alleen op fysieke agressie, maar ook op vormen die minder makkelijk te herkennen zijn,

zoals bijvoorbeeld pesten. Het protocol is opgesteld door Nicole Torka van HR.
De zorg voor het creëren van een veilige en gezonde werkomgeving moet ook herkenbaar zijn in het door ons te voeren personeelsbeleid. Bij het aannemen van medewerkers moeten we serieus nagaan of de betreffende persoon eerder elders conflicten heeft veroorzaakt. Dit door het uitvoeren van een antecedentencheck. Niet alleen om referenties vragen maar deze referenten ook serieus bevragen.

Wij dienen een veilige werkomgeving te kunnen bieden waarbij wederzijdse verwachtingen helder worden gecommuniceerd en duidelijke afspraken worden gemaakt met betrekking tot de in te vullen rollen. Dit geldt zowel voor studenten en medewerkers. Medewerkers en studenten zullen zich voldoende veilig moeten voelen om, indien nodig, het ervaren van een te grote werkdruk of van ongewenst gedrag aan te kaarten.
Binnen het kader van het omgaan met klachten rond ongewenste intimiteiten is het de vraag of ons instrumentarium en het instellen van een vertrouwenspersoon wel afdoende zijn. Wat zijn goede spelregels om te hanteren? Hoe bespreken we een aangemeld geval met het slachtoffer, respectievelijk de vermeende dader? Moeten ook directe collega's worden geraadpleegd? En wat zijn de consequenties voor de dader indien de klacht terecht blijkt te zijn? Het geven van een "gele kaart" of gelijk al een "rode kaart"? Ongewenste intimiteiten kunnen zich voordoen tussen studenten en medewerkers onderling maar ook tussen een student en een medewerker of leidinggevende en tussen een medewerker en een leidinggevende.

Vertrouwenspersonen kunnen ook lang niet alles delen met de organisatie. De UT heeft daarom besloten om naast vertrouwenspersonen ook een ombudspersoon aan te stellen. In eerste instantie gaat het om een pilot van twee jaar. Medewerkers kunnen zich bij het ervaren van ongewenst gedrag door collega's of leidinggevenden (denk bijvoorbeeld aan het verrichten van ongeoorloofde financiële transacties door de leidinggevende), onterechte beoordelingen en herplaatsingen melden bij de ombudspersoon. De ombudspersoon kan ook bemiddelen bij conflicten en zelf onderzoek doen.

Toenemende werkdruk kan leiden tot gevaarlijke situaties. De afgelopen paar jaar is het aantal burn-out klachten van medewerkers bij de UT duidelijk toegenomen. Medewerkers en studenten kunnen in zulke gevallen zelf een veiligheidsrisico gaan vormen. Het gaat in de meeste gevallen om een combinatie van werk en privé.

Belangrijk is om alert te zijn op mogelijk afwijkend gedrag dat kan ontstaan onder toenemende werkdruk. De leidinggevende vervult bij de signalering hiervan een belangrijke rol. De UT heeft inmiddels een taskforce werkdrukbeheersing ingericht die het CvB adviseert op het gebied van werkdrukbeheersing. Deze taskforce initieert, coördineert en ondersteunt een UT-brede aanpak en draagt voorstellen aan tot verbeterpunten.
Waar wij als UT nog onvoldoende op voorbereid zijn, is onze omgang met medewerkers die verkeren in psychische nood. Het is verstandig als de UT zich eigen maakt hoe te communiceren met een persoon die in een mentale crisissituatie verkeert. De politie beschikt over ervaren onderhandelaars die getraind zijn om de juiste vragen te stellen. Philippe Huinen en Heidi Nieboer verzorgen op dit gebied trainingen en hebben als politieonderhandelaars hier ruime ervaring mee opgedaan. Het is ook aan te bevelen om de vertrouwenspersonen en de beveiligers van de UT bij een dergelijke training te betrekken.

6. Integriteit en ethisch handelen

Integriteit en ethisch handelen is van strategisch belang vanwege de mogelijke reputatieschade die de UT kan oplopen in geval van een schending van de integriteit of bij onethisch landen.

Vanuit de VSNU is er een nieuwe code Integriteit opgesteld. Deze zal komend jaar worden uitgerold binnen de UT. Binnen dit kader is door Haico te Kulve en Nicole Torka een notitie opgesteld over het door de UT te voeren integriteitsbeleid en het implementeren van een "House of Integrity". De notitie is binnen het college van decanen en het CvB besproken op 11 juli 2019 en besloten werd tot implementatie van de voorgestelde acties. Het "House of Integrity" omvat drie dimensies van integriteit: wetenschappelijke integriteit (e.g. zorgvuldig data management en onderzoekethiek), sociale integriteit (relaties en omgangsvormen op de werkplek) en organisatie-integriteit (zorg voor een veilige werkomgeving en het bewaken van de privacy van medewerkers). Voor de implementatie van het House of Integrity lopen een vijftal projecten:
(1) Het bevorderen van het bewustzijn onder medewerkers en studenten;
(2) Het bevorderen van een integriteitscultuur
(3) Research Data management
(4) Publicatiebeleid
(5) Ethische normen en procedures.

Integriteit is een verplicht onderdeel (2 EC) in de opleidingsprogramma's van promovendi en zal ook gaan gelden voor externe promovendi. Een vraag is hoeveel tijd we voor onderwerpen als Integriteit en ethisch gedrag kunnen vragen. Het is ook iets dat qua vanzelfsprekendheid zal groeien. Het voorkomen en bestrijden van plagiaat is tegenwoordig bijvoorbeeld vanzelfsprekend en standaard en kan via een simpel proces worden nagegaan.

7. Internationalisatie

De internationalisatie van de universiteit gaat gepaard met de komst van buitenlandse medewerkers en studenten en hiermee ook uiteenlopende normen en waarden. Zo is er, afhankelijk van het land van herkomst, een andere omgang met vrouwen. Vrouwelijke studenten, maar ook medewerkers kunnen hier last van hebben. Internationale studenten en medewerkers zullen wegwijs gemaakt moeten worden over de heersende omgangsvormen in Nederland. Wellicht dat studentenmentoren en studieadviseurs hierin een constructieve rol kunnen spelen. En in het geval van medewerkers zullen we als organisatie alert moeten zijn en hier adequaat op inspelen.

Tijdens verschillende van de gehouden interviews kwam naar voren, dat mede door de internationalisering van de UT, het aantal psychische klachten is toegenomen. Heimwee, de druk om binnen de voorgeschreven tijd af te studeren of te promoveren, een visum dat kan verlopen wanneer de student of promovendus niet binnen de voorgeschreven tijd klaar is en het stigma van falen binnen de eigen cultuur, zorgen voor toenemende stress onder buitenlandse studenten en promovendi. Buitenlandse studenten en promovendi zijn ook minder geneigd om voor hulp aan te kloppen. Alertheid bij studiebegeleiders voor het signaleren van zorgwekkend gedrag is daarom belangrijk. In het geval van buitenlandse promovendi speelt vaak ook de gezinssituatie een rol: partner en kinderen hangen er vaak maar een beetje bij. Als UT dragen we hiervoor een bijzondere verantwoordelijkheid. Daarnaast zou ook de internationale PhD community op de UT een rol van betekenis kunnen spelen door als gemeenschap beter op elkaar te letten en te waarschuwen wanneer men zich zorgen maakt over een collega-PhD student.
TGS biedt inmiddels workshops aan hoe om te gaan met deze stress. Ook de spelregels rond een promotietraject worden aangepast: er wordt in het vervolg uitgegaan van twee promotores en de qualifier is mede een taak van de promotores. Het geheel moet leiden tot een geborgen basis voor de promovendi. Binnen VSNU-verband zijn regels opgesteld voor een gezonde promotiepraktijk. Het is de bedoeling om deze regels nu binnen de UT te implementeren.

De afgelopen tijd hebben zich ook een paar psychische crisissituaties voorgedaan met buitenlandse promovendi. De verwachting is dat dit soort incidenten in de komende tijd wellicht kan toenemen. De BHV teams zijn niet goed opgeleid om hier adequaat mee om te gaan. De oranje overalls van de BHV teams werken mogelijk zelfs agitatie op. Wellicht dat het instellen van een UT-brede "Interventiegroep" met kennis van zaken over psychotisch gedrag en hoe hiermee om te gaan een oplossing kan zijn. De Interventiegroep is dan bij het zich voordoen van een psychotisch incident oproepbaar via het Picasse systeem. Het is verstandig als de UT investeert in het aannemen van 1-2 experts op dit gebied, want het zal ook in de komende jaren weer voorkomen. Deze experts zijn dan idealiter altijd aanwezig om crisissituaties op te vangen en erger te voorkomen. Op dit moment zijn we afhankelijk van Mediant en dat gaat niet altijd in het tempo dat we nodig hebben.

Faculteiten binnen de UT kunnen wellicht leren van twee door ITC gevolgde werkwijzen voor buitenlandse studenten en promovendi:
Voor studenten kent de faculteit ITC twee study affairs officers. Buitenlandse studenten kunnen met een scala van problemen (die ook niet-studie gerelateerd kunnen zijn) bij deze officers aankloppen. Er geldt een laagdrempelige, open door policy. Wanneer zich een potentieel probleem voordoet horen de officers dit snel en kunnen ze proactief hierop actie ondernemen.
Bij ITC start men met een homologatiejaar voor buitenlandse promovendi. Dit om zeker te stellen dat een promovendus beschikt over de vereiste kennis en vaardigheden om succesvol een promotieproject te doorlopen.

8. Reputatierisico's

Een goede reputatie van de UT is essentieel om contracten te kunnen sluiten met derden en om als organisatie aantrekkelijk te zijn voor medewerkers om bij de UT te willen komen of blijven werken en voor studenten om hier te studeren.

9. Politieke veiligheid

Wij zullen ons als UT meer bewust moeten worden van het risico van spionage. Internationale studenten en promovendi kunnen vanuit hun thuisstaat hiertoe aangespoord worden. Bij politieke veiligheid valt te denken aan kennis die onvoldoende door de UT is beveiligd en waarvan de deling van deze kennis met landen als Iran, Rusland of China, de UT schade kan berokkenen. Vanuit het Kabinet maakt men zich bijvoorbeeld in toenemende mate zorgen over het ballistische raketprogramma van Iran. Om die reden is het toezicht op studenten en onderzoekers die een link kunnen hebben met het Iraanse ballistische raketprogramma verscherpt. Voor het studiejaar 2019-2020 en daarna verscherpt het kabinet het toezicht op nieuwe studenten en onderzoekers die activiteiten willen ontplooien in één van de relevante onderwijs- en onderzoeksgebieden door deze groep te toetsen voordat zij met het onderwijs of onderzoek starten. Een complicerende factor hierbij is de mogelijkheid tot dual use (ontwikkeld bijvoorbeeld als applicatie binnen de gezondheid maar uiteindelijk ook toepasbaar voor defensiedoeleinden) en de toenemende samenhang tussen ICT, materialen, product- en productietechnologie. De keuze door het Kabinet voor een specifiek aantal onderwijs- en onderzoeksgebieden heeft bijgevolg een wat ad-hoc karakter. De opgelegde beperking plaatst de universiteit als zijnde een open instelling voor onderwijs en onderzoek voor nieuwe dilemma's hoe hier mee om te gaan. Op dit gebied ontbreekt het ons aan een duidelijk protocol. We zullen dus zelf beleid moeten ontwikkelen. Wellicht kunnen we leren van hetgeen TNO (die een sterke defensiepoot heeft) en de TU Delft (waar veel kennis wordt ontwikkeld dat van belang is voor militaire organisaties en voor de ruimte- en luchtvaart) op dit gebied aan protocollen hebben ontwikkeld.

Er bestaat de kans van toegang tot verschillende systemen (via studenten maar ook via medewerkers) en er is hiervoor geen overall aanspreekpunt binnen de organisatie die hierop toeziet. Er is een goede afstemming vereist tussen de externe organisatie en interne organisatie en een duidelijk overzicht van activiteiten die mogelijk schadelijk kunnen zijn voor de strategische belangen van de UT. Bijvoorbeeld het werken aan projecten waar Iran voordeel van kan hebben kan uiteindelijk schadelijk uitpakken voor onze relatie met de USA waar we als kennisinstelling heel veel uitwisseling mee hebben. De continuïteit van de UT als organisatie kan hiermee in het geding komen.

Een aandachtspunt bij een reis naar landen zoals China, Rusland, Iran en de USA betreft de IT-security. De AIVD heeft een e-learning module ontwikkeld die door medewerkers kan worden gevolgd. Belangrijk is een "lege" laptop mee te nemen naar het beoogde land en zeker niet in te loggen naar de website van de UT of gegevens op de UT.

Studenten en medewerkers gaan voor onderwijs en onderzoek vaak naar het buitenland. Breng vooraf in kaart in welke landen zij mogelijk grote veiligheidsrisico's kunnen lopen en spreek de mensen aan over hun verantwoordelijkheid ten aanzien van deze risico's. Als faculteit moet je beschikken over een protocol over de te volgen handelswijze wanneer een medewerker of student zich in een onveilig land bevindt of juist van plan is ernaar toe te gaan. Denk hierbij aan het informeren over de onveilige situatie, het ontraden en ook het terughalen. En bij weigering de verantwoordelijkheid volledig leggen bij de medewerker of student.
De faculteit ITC toetst bij buitenlandse reizen door studenten of medewerkers altijd het advies van BUZA: Bij "code rood" kan de reis niet doorgaan. Bij "code oranje" zal per geval worden nagegaan of er goede redenen zijn de reis te maken.
Bij CES houdt men bij waar zich wereldwijd calamiteiten (zoals Tsunami's, overstromingen, aanslagen of oproer zoals recent in Hong Kong) voordoen. Dit is belangrijk is om vervolgens te kunnen nagaan of er mogelijk studenten of medewerkers van de UT gevaar lopen. Het ministerie van Buitenlandse Zaken beheert een gratis te downloaden reis-app die studenten of medewerkers die op reis gaan, belangrijke informatie kan verschaffen over het betreffende land. Dit is zeker van belang wanneer zich een potentieel risicovolle situatie voordoet. Daarnaast heeft de UT zelf ook een reis-app (CHUBB) in ontwikkeling die de UT in staat stelt om, in geval in een bepaald land een risicovolle situatie dreigt of zich heeft voorgedaan, contact te leggen met studenten en/of medewerkers van de UT in dit land. Of juist omgekeerd, dat studenten en medewerkers contact kunnen leggen met de UT. De reis-app van de UT is nu nog in een experimentele fase. De evaluatie van de reis-app van de UT volgt nog.

10. Systemen voor het monitoren van de veiligheid op de UT

- *Sky-walker.* Met behulp van deze software kunnen allerlei soorten van storingen en incidenten die zich hebben voorgedaan worden opgeslagen. Ook camerabeelden van observaties door beveiligers (wanneer iemand zich bijvoorbeeld ongeautoriseerd in een gebouw of ruimte bevindt) kunnen met Sky-walker worden opgeslagen.
- *Milestone*. Deze bundelt alle camerabeelden. Benno Kiers maakt hiervan gebruik.
- *Brandweerdectiesystemen.* De UT beschikt over het ASCOM branddetectiesysteem. De verschillende detectieapparaten zijn met elkaar verbonden en als geheel te bedienen. Wel zijn er een aantal stand-alone systemen (van Siemens) die niet op het ASCOM systeem zijn aangesloten. De beveiligers maken van elk incident een specifiek rapport in "word". Deze wordt vervolgens in "excel" verwerkt tot een management rapportage.

- *Picasse*. Een oproepsysteem met behulp van een tablet dat nu sinds een jaar door de verschillende BHV-teams worden gebruikt. Teamleden krijgen via de tablet bericht over de aard van het incident en waar ze in actie moeten komen.
- *Galaxy*. Dit is een autorisatiesysteem die personen toegang verschaft tot gebouwen buiten kantoortijd. Per gebouw is een functionaris aangesteld die verantwoordelijk is voor de toewijzing van de autorisatie aan een medewerker, student of een extern persoon.
- *Inspraak systemen*. Per gebouw kan de bewaker op afstand een systeem inschakelen of juist uitschakelen.
- *Inbraken*. De afdeling Beveiliging heeft een goede samenwerking met de politie. Zo rapporteerde de politie onlangs een toename van het aantal inbraken in studentenhuizen. Graag zou het hoofd Beveiliging dan gelijk kunnen willen zien op welke locaties de inbraken zich hebben voorgedaan (op UT terrein of juist in de stad etc.).
- *Verkeersincidenten*: deze worden geregistreerd. Er is nu een apart formulier ontwikkeld voor de registratie van verkeersincidenten.
- *Cyber security.* LISA stelt ieder kwartaal een rapportage op over alle aspecten van Cyber Security op de UT. Deze wordt besproken in het CvB en gedeeld met hoger management. Binnen LISA zijn twee medewerkers belast met het uitbrengen van deze rapportage. Het zou goed zijn om deze rapportagevorm te integreren in een nog te ontwikkelen en te implementeren reguliere rapportage over de Integrale Veiligheid op de UT.
- *Rapportages van incidenten door Beveiliging.* De Beveiliging maakt rapportages van alle incidenten die zich op de campus en in de gebouwen voordoen. De facilitair team leiders krijgen deze rapportages. Het is goed om dit soort informatie ook te delen met de decaan en de directeur bedrijfsvoering. Dan krijgen ook zij een beter gevoel van wat belangrijke te nemen acties zijn op het gebied van veiligheid.
- VGM brengt elk jaar een verslag uit van de incidenten die zich hebben voorgedaan. Dit is belangrijk om achteraf te kunnen analyseren of er een patroon te herkennen valt waar wat aan gedaan kan worden. We moeten dan wel een cultuur opbouwen om ongevallen niet te bagatelliseren maar altijd te melden. Lang niet alle ongevallen worden namelijk gemeld. We moeten een cultuur opbouwen dat we ons mede verantwoordelijk voelen voor het opbouwen van een veilige werkomgeving. Dit geldt niet alleen voor het voorkomen van fysieke ongevallen maar ook in de zorg voor de wijze waarop we bijvoorbeeld ons data-management beheren. De opgedane ervaringen met data-lekken kunnen bij melding worden gedeeld en kunnen worden gebruikt op hieruit lering te trekken.

11. Inrichting en organisatie van Integrale Veiligheid

Voor alsnog ontbreekt het aan een integraal risicomanagement beleid op de UT. Dat is dan ook een belangrijke reden voor dit onderzoek. Voor de organisatie en inrichting van risicomanagement is het van belang dat op een structurele en systematische wijze potentiële interne maar ook externe risico's in kaart worden gebracht, dat er jaarlijks evaluaties en verbeterplannen worden opgesteld en dat vervolgens wordt nagegaan in hoeverre de ingevoerde verbeteringen effectief blijken te zijn.

Een belangrijke observatie die tijdens de gehouden interviews werd gemaakt is het ontbreken van continuïteitsplannen voor het primaire proces van de UT. In het geval Osiris uitvalt door een calamiteit of cyberaanval, zal een belangrijk deel van het onderwijs geen doorgang kunnen vinden.

Er is binnen faculteiten een scheiding waarneembaar tussen HR-activiteiten en ARBO zaken. Dit geldt ook op centraal niveau. Door deze splitsing wordt het moeilijker om regie te houden. Regie binnen de faculteit verloopt vooral via de Portefeuillehouder Bedrijfsvoering. Op centraal niveau is de

regiefunctie minder zichtbaar. Voor Integrale Veiligheid is het essentieel dat er een goede laterale verbinding is tussen deze twee aandachtsgebieden. Dit is een belangrijke voorwaarde voor het realiseren van Integrale veiligheid. Personen met verantwoordelijkheid op het gebied van Integrale Veiligheid moeten met enige regelmaat bij elkaar komen om ervaringen uit te wisselen. Dit verhoogt de alertheid en een grotere kans op patroonherkenning wanneer zich een bijzondere situatie voordoet.

Een aandachtspunt bij de implementatie van Integrale Veiligheid is de organisatie van de verantwoordelijkheid voor Integrale Veiligheid. Het gevaar bestaat dat dit belegd wordt bij een "centrale coördinator Integrale Veiligheid" en dat dit dan los komt te staan van de lijnorganisatie en de wetenschappers. Voor andere opkomende overstijgende nieuwe thema's zoals "integriteit", "Internationalisatie" en "Inclusiviteit" bestaat een vergelijkbaar risico. Bij de afstemming tussen de centrale organisatie en de decentrale (faculteiten) organisaties is het van belang een goede balans tussen vertrouwen en transparantie voor ogen te hebben. Bij het delegeren wordt vertrouwen gegeven aan een decentrale organisatie. Dit moet vanuit een decentrale organisatie gepaard gaan met een transparante wijze van werken waardoor het vertrouwen bestendigt. Dit samenspel leidt dan weer tot een betrouwbare wijze van werken. In de komende periode is het belangrijk om voor de inrichting en organisatie van Integrale Veiligheid een effectieve modus operandi te ontwikkelen.

Belangrijk is om de opvolging van verbeterpunten ten aanzien van Integrale Veiligheid te monitoren en hiermee continue aandacht voor integrale veiligheid te realiseren. In dit verband is het aan te bevelen om Integrale Veiligheid ook op te nemen in de Planning & Control cyclus van de UT. Ook op strategisch niveau moet met enige regelmaat het onderwerp geagendeerd worden. Het is van belang dat aandachtsgebieden zoals het SEP-protocol, de promotieopleiding en het HR-beleid (talentontwikkeling) onderdeel gaan uitmaken van de normale planning & control cyclus.

12. Bewustwording op het gebied van Integrale Veiligheid bij medewerkers en studenten

Essentieel voor het verhogen van de veiligheid op de campus en in de gebouwen is een door iedereen gedeeld gevoel van verantwoordelijkheid voor veiligheid. Dit betekent dat we met z'n allen alert zijn. Een rood alarmlichtje bij een invalidetoilet noopt tot actie, een busje dat zich meldt voor "onderhoud aan beamers" en er vervolgens met de beamers vandoor gaat, noopt tot een stringentere controle van bedrijven die werkzaamheden verrichten voor de universiteit. Registratie van (onder)aannemers die werkzaamheden in de gebouwen verrichten is in dit verband belangrijk, ook bij het zich eventueel voordoen van een calamiteit. Medewerkers en studenten moeten weten bij wie je een potentieel onveilige situatie moet melden.

De UT heeft al veel regelgeving op het gebied van (sociale) veiligheid zoals het omgaan met agressie en relaties op de werkvloer. Een belangrijke vraag is echter hoe je dit ook op het netvlies krijgt van medewerkers en studenten? Het bewustzijn over Integrale Veiligheid onder medewerkers en studenten is nog laag. Het is van belang dat een medewerker of student tot actie komt wanneer hem/ haar iets overkomt of wanneer hij/zij ziet dat de sociale veiligheid van een collega of van een mede-student in het geding is. We zullen daarom beleid moeten ontwikkelen dat we ons hiervan binnen de organisatie bewuster worden. Belangrijk is dan de vraag hoe Integrale Veiligheid uit te rollen binnen de UT? De cultuur op de UT is te kenschetsen als informeel, zowel studenten als medewerkers voelen zich veilig. Bij de implementatie van Integrale Veiligheid op de UT past een "principle-based aanpak" beter bij de cultuur van de organisatie dan een "rule-based aanpak". Goed opgestelde principes worden idealiter afgeleid uit de identiteit die een organisatie nastreeft en de waarden die hieraan ten grondslag liggen. Bij het opstellen van principes werkt het vaak goed om niet alleen te beschrijven wat je wél doet maar ook wat je niet doet. Wanneer zich in de toekomst

echter meer excessen voordoen, zullen we wellicht meer moeten verschuiven naar een rule-based aanpak.

In het verleden kwam de ARBO langs bij een nieuwe medewerker om voorlichting te geven over veilig en gezond werken en hoe en wat te doen in probleemsituaties. Dit zou weer moeten worden ingevoerd.
Zoals in punt 5 reeds werd gesteld, is het bij de introductie van nieuwe medewerkers en ook daarna, van belang om te wijzen op het belang van Integrale Veiligheid. Elke medewerker zou naast het landelijke alarmnummer 112, ook het alarmnummer 053-489 2222 van de UT moeten kennen en weten hoe te handelen wanneer zich een noodsituatie voordoet. Het UT-alarmnummer zou in het mobieltje van elke medewerker moeten staan. Er wordt al het nodige gedaan om het noodnummer onder de aandacht te brengen van bezoekers, medewerkers en studenten. Dit gebeurt op het billboard bij de ingang van de UT en ook op de schermen binnen de gebouwen. In het geval van een noodsituatie, is het belangrijk om iedereen die zich in een gebouw bevindt, te kunnen bereiken. Elk gebouw beschikt inmiddels hiertoe over een omroepinstallatie. Medewerkers zouden idealiter ook via hun mobiel bereikt moeten kunnen worden in geval zich een crisissituatie voordoet.

Voor het verhogen van de bewustwording van medewerkers over ethisch handelen heeft Ellen Giebels in samenwerking met de Universiteit Utrecht, het initiatief genomen voor het ontwikkelen van een theatervoorstelling, zoals eerder ook met succes werd gedaan voor de top van ziekenhuizen, politie en defensie. Het ontwikkelen van een theatervoorstelling op het gebied van Integrale Veiligheid zou ook uitstekend kunnen werken binnen universiteiten.

Met enige regelmaat worden (ludieke) acties uitgevoerd om de bewustwording omtrent internetgevaren onder medewerkers en studenten te vergroten. Een voorbeeld hiervan is het vergroten van de bewustwording van het gevaar van “Phishing mails”. BMS heeft in het recente verleden samen met LISA een onderzoek uitgevoerd naar deze “Fishing-mails” door zelf een “Phishing mail” uit te zetten: wie trapt erin en waarom/ wanneer gebeurt dit? Andere voorbeelden die zijn ingezet om de bewustwording te vergroten waren een houten paard (Trojan Horse) op de campus, stickers om de camera op je laptop mee af te plakken, de aanwezigheid van LISA tijdens de kick-in van nieuwe studenten bij de aanvang van het collegejaar met de leus: “Behandel je wachtwoorden als je ondergoed; Deel niet met je vrienden, Laat het niet slingeren en Verwissel regelmatig”.
Een vergelijkbare actie die werd uitgevoerd met toegangspasjes voor werkruimten en laboratoria wees uit dat medewerkers in goed vertrouwen hun toegangspasje afgaven ter controle.

Het is belangrijk dat aan het verhogen van de bewustwording wordt gewerkt door dit op te nemen in de diverse opleidingsprogramma’s zoals het leiderschapsprogramma en bij de introductie van nieuwe medewerkers. Voor medewerkers is het van belang om bijvoorbeeld via intranet de diverse opties te kunnen evalueren (consulteren van ombudspersoon, vertrouwenspersoon etc.).

Dr. Saskia Kelders heeft een plan uitgewerkt om studenten via interactieve tools met spelelementen hun leerprestaties te laten verhogen. Zoiets zou ook ingezet kunnen worden voor het verhogen van het bewustzijn op het gebied van Integrale Veiligheid onder studenten en medewerkers

13. Oefenen van crisissituaties

Er bestaat een algemene neiging om protocollen uit te werken voor de omgang met veiligheidssituaties. Acute situaties die zich niet eerder hebben voorgedaan, zijn echter moeilijk te protocolleren. Als organisatie moet je in staat zijn om ook adequaat om te gaan met het onverwachte. Het opbouwen van een voldoende niveau van resiliency is hierbij cruciaal. Door middel

van het uitvoeren van scenario-analyses kunnen we anticiperen op toekomstige ontwikkelingen en ons hier vervolgens beter op voorbereiden.

Met enige regelmaat worden crisisoefeningen uitgevoerd. Het is aan te bevelen om bij de oefeningen het pallet van mogelijke crisissituaties die zich kunnen voordoen uit te breiden. Recent heeft het landelijk uitvallen van het alarmnummer 112 bijvoorbeeld geleid tot onvoorziene noodsituaties. Ook moeten we continu kijken naar een goede afstemming tussen de verschillende crisisteams.

De oefeningen op het gebied van crisismanagement lopen op zich bevredigend. Maar het is aan te bevelen om ook aan opschalen te denken waarbij grotere doelgroepen worden ingeschakeld. Het Van Goghmuseum hield onlangs een oefening waarbij een terroristische aanval werd gesimuleerd.

Het is belangrijk om met enige regelmaat een crisisoefening te houden. Naarmate teamleden vaker een oefening hebben meegemaakt, raken ze ook beter op elkaar ingespeeld. Een punt van aandacht is wie/ wanneer een crisisteam bijeen roept. Toen zich bijvoorbeeld een grote storm op de campus voordeed kwam het idee spontaan bij een van de leden van het centrale crisisteam op dat de fysieke veiligheid op de campus mogelijk in gevaar kon komen en werd het crisisteam bijeen geroepen. Dit soort potentiële risico's zouden eigenlijk beter als standaard repertoire kunnen worden ingebed.

Een belangrijk punt is het leervermogen van de UT als organisatie. Hoe kunnen we leren van calamiteiten wanneer deze zich voordoen en wat kunnen we leren van crisisoefeningen? We zullen voor wat betreft Integrale Veiligheid onze websites toegankelijker moeten maken voor de uiteenlopende doelgroepen. Maak ook gebruik van de expertise die aanwezig is bij de diverse onderzoekers van de UT. En stel een jaarlijks van samenstelling wisselende externe expertisegroep samen, een "Raad van Anders" die de organisatie kan bevragen en suggesties kan doen op het gebied van Integrale veiligheid.

Als UT hebben we ook een centraal telefoonnummer. De kans is groot dat bij een eventuele bommelding, dit centrale nummer wordt gebeld. Er moet een protocol zijn hoe zo'n telefoontje af te handelen en de dienstdoende telefonist(e) dient dit goed te kennen.

14. Overige voorstellen op het gebied van veiligheid

Privacygevoelig onderzoek moet tegenwoordig op de UT worden voorgelegd aan een Ethische commissie. Het zou goed zijn als deze commissie ook de taak krijgt om na te gaan of voor het betreffende onderzoek het bewaken van de veiligheid wellicht een issue is en wat hier dan aan gedaan moet worden. Ten tijde van de evaluatie van het MH17-onderzoek dat uitgevoerd werd door een onderzoeksgroep van de faculteit BMS, werd er extern via internet gericht geprobeerd om data over dit onderzoek te achterhalen.

De toegankelijkheid en vindbaarheid van informatie op het gebied van integrale veiligheid (op de website) behoeft verbetering. Bij het zoeken zou voor de uiteenlopende doelgroepen, de gewenste informatie gemakkelijk vindbaar moeten zijn en overzichtelijk geordend.

Wat betreft het monitoren van veiligheid is het van belang om de "Cyberrapportage" te noemen die elk kwartaal wordt uitgebracht. Binnen LISA zijn twee medewerkers belast met het uitbrengen van deze rapportage. Het zou goed zijn om deze rapportagevorm te integreren in een nog te ontwikkelen en te implementeren reguliere rapportage over de Integrale Veiligheid op de UT.

Voor het verhogen van de veiligheid op het UT-internet, is het van belang om binnen het kader van de Integrale Veiligheid ook te denken aan het ontwikkelen en implementeren van uitwijkmogelijkheden in geval zich een calamiteit voordoet. Bijvoorbeeld van vaste lijnverbindingen

moeiteloos kunnen overschakelen naar mobiele verbindingen en bij communicatie het gebruik van face time als optie.

Naast het zich voordoen van incidenten en het oppakken hiervan is het ook goed om na te denken over hetgeen zich structureel aan risico's kan gaan voordoen op de UT. Bijvoorbeeld hoe te handelen bij structurele groei of juist bij structurele krimp? Als organisatie hebben we vaak de neiging om snel "tot de orde van de dag" binnen de eigen functionele koker over te stappen terwijl bij een structureel risico een integrale analyse en aanpak vereist is waarbij ook duidelijk wordt afgesproken wie hierin de leidende rol heeft.

Een verbeterpunt op de UT wat betreft de organisatie van ARBO/Milieu is het ontbreken van beleid op centraal niveau. Op faculteitsniveau wordt de uitvoering weliswaar adequaat aangepakt, maar door bezuinigingen in het verleden is op centraal niveau de beleidsfunctie op ARBO/Milieu gebied voor een groot deel komen te vervallen.

15. Conclusie en vervolg

In deze rapportage zijn de zienswijzen van de portefeuillehouders op het gebied van Integrale Veiligheid aan de UT in kaart gebracht. Uit de gehouden interviews blijkt dat er een groot draagvlak bestaat voor het implementeren van Integrale Veiligheid. Het onderwerp wordt gezien als van groot belang voor de UT. Het is een eerste stap om te komen tot een plan tot het implementeren van Integraal Veiligheidsmanagement op de UT. Deze interne oriëntatie wordt vervolgd met een externe oriëntatie waarbij wordt nagegaan welke externe ontwikkelingen van belang zijn voor de implementatie van Integraal Veiligheidsmanagement op de UT en wat de UT mogelijk kan leren van andere bedrijven en kennisinstellingen.

De uitgevoerde Quick Scan heeft duidelijk gemaakt dat veiligheidsmanagement een belangrijk onderwerp is voor de UT en dat er op dit gebied al veel werk wordt verricht. Belangrijke onderwerpen waar in het vervolg van deze studie in ieder geval aandacht aan zal worden besteed zijn:

- Het ontwikkelen van continuïteitplannen voor het primaire proces van de UT. In het geval Osiris uitvalt dor een calamiteit of cyberaanval, zal een belangrijk deel van het onderwijs geen doorgang kunnen vinden
- Een integrale benadering van veiligheid door de relatie tussen cybersecurity en de andere veiligheidsaspecten nadrukkelijker te beschouwen en uit te werken
- Het uitwerken van een protocol en de organisatie en inrichting van veiligheidsrisico's veroorzaakt door medewerkers of studenten die in psychische nood verkeren
- Het verhogen van de bewustwording op het gebied van Integrale Veiligheid onder medewerkers en studenten
- Uitwerken wat de implicaties van internationaliseren zijn voor het succesvol invoeren van Integrale Veiligheid op de UT
- Het verhogen van het anticiperend vermogen op moeilijk te voorziene veiligheidsissues door het periodiek uitvoeren van scenarioanalyses
- Het inbedden van Integrale Veiligheid door dit op te nemen in de Planning & Control cyclus van de UT
- Het verhogen van de verkeersveiligheid op de campus