**Wat als Security cultuur meetbaar wordt?**

**Security management with a future: deel 2**

**Artikel UA**

**september 2011**

Annemie De Boye, zaakvoerder Modus Operandi en senior security consultant Robrechts & Thienpont

Paul Robrechts, afgevaardigd bestuurder Robrechts & Thienpont

**De M-factor**

In het voorgaande artikel beschreven we hoe het thema “veiligheid” steeds meer evolueert naar een nieuw paradigma om de specifieke problemen rond de mens en zijn systeem inzake security ten gronde op te lossen. We noemden dit het “betrokkenheidsparadigma”. Cruciaal hierbij is de gedachte dat de mens als volwaardige factor dient te worden betrokken bij het systeem en de waarden van het bedrijf. In dit artikel ontwikkelen we het concept volledig vanuit security, maar het woord “security” kan perfect vervangen worden door safety: de benadering is zo goed als identiek.

In security-vraagstukken is de menselijke factor overal en altijd aanwezig. Het volstaat dus niet om binnen een bedrijf het securitybeleid en de technieken te optimaliseren: wie het menselijke security-*gedrag* over het hoofd ziet, verwaarloost een belangrijke en veelal zwakke schakel in zijn veiligheidsketen. Dit is bijvoorbeeld het geval wanneer medewerkers zich niet bewust zijn van security-risico’s. Of wanneer men security wel belangrijk vindt, maar het niet als een eigen verantwoordelijkheid beschouwt. Wanneer securityprocedures geen onderdeel zijn van de dagelijkse routine blijft het onderwerp “veiligheid” voor de meeste leden van de onderneming een abstracte ver-van-mijn-bed-show.

De security-ontwikkelingen in het laatste decennium hebben zich dan ook in aanzienlijke mate gericht op deze menselijke factor. Via opleidingen en trainingen tracht men het uitvoerend personeel niet enkel kennis en kunde met betrekking tot veiligheid bij te brengen, maar wil men ook het veiligheidsbewustzijn (de *security awareness*) verhogen.

Uit diverse wetenschappelijke studies alsook uit de ervaringen in de praktijk blijkt echter dat het louter verhogen van het veiligheids*bewustzijn* via procedures, opleidingen en trainingen, niet noodzakelijk volstaat om ook een veiligheids*cultuur* (security culture) te creëren. Vaak blijkt er een discrepantie te bestaan tussen de theorie die mensen verkondigen (espoused theory) en hun gedrag in de praktijk (theory in use)[[1]](#footnote-1). Een ontwikkelde veiligheidscultuur veronderstelt dat àlle leden van de organisatie intentioneel, bewust én consistent met security omgaan. Dit betekent concreet dat veiligheidscultuur een inherent onderdeel uitmaakt van de algemene bedrijfscultuur. Is dit niet het geval, dan kan het invoeren van beveiliging bemoeilijkt worden door de heersende organisatiecultuur en de relaties tussen medewerkers. De security manager moet zich dus steeds afvragen of de security policy past in de organisatiecultuur en andersom[[2]](#footnote-2).

Dat een ontwikkelde veiligheidscultuur voor vele bedrijven nog een vaag na te streven doel is, blijkt uit een ondervraging van veiligheidsverantwoordelijken in middelgrote en grote bedrijven door het onderzoeksbureau Bon Bini. Het grootste struikelblok inzake security wordt door deze verantwoordelijken gedefinieerd als “het ontbreken van voldoende middelen zoals tijd, personeel of geld”. Als tweede moeilijkheid noemen ze “het op sleeptouw nemen van collega’s omwille van een gebrek aan veiligheidsbewustzijn”. De overige problemen benoemen ze als “een gebrek aan expertise”, “het ontbreken van een veiligheidscultuur”, “het ontbreken van medewerking van de bedrijfsleiding” en “een gebrek aan technische ondersteuning en aan gevoeligheid voor veiligheidsproblemen”.[[3]](#footnote-3)

Idealiter gaat het nu net binnen het bedrijf om een veiligheidscultuur “waar werknemers zich mede eigenaar voelen binnen een vaste set van security principes, waarbij ze voortdurend worden opgeleid in goede security praktijken, en waarin zij zich ook verantwoordelijk voelen voor wat ze ondernemen”. [[4]](#footnote-4) Een optimale security cultuur omvat dus zowel mensen, processen als technologie. Vanuit deze stelling is veiligheid dan ook geen exclusief probleem van de werkvloer, maar tevens een opdracht van het algemeen management[[5]](#footnote-5).

Het ontwikkelen van een veiligheidscultuur bij een bedrijf is vaak gerelateerd aan een specifieke gebeurtenis. Het meest bekende voorbeeld op het gebied van veiligheid is afkomstig van het Franse bedrijf DuPont. De motivatie van het explosievenbedrijf om van veiligheid een prioritaire bedrijfsdoelstelling te maken is al bijna 200 jaar oud. In 1818, kort na oprichting van het bedrijf, explodeerde een buskruitmolen. Veertig personen kwamen om en de buskruitmolen was vernietigd. De eigenaar, wiens vrouw gewond was geraakt, realiseerde zich dat het voortbestaan van zijn bedrijf afhankelijk was van het voorkomen van dit soort ongevallen. Om het management meer bij veiligheid te betrekken werden deze verplicht om op het bedrijfsterrein te wonen.

Het begrip veiligheidscultuur is verder in de belangstelling komen te staan bij de rapportage van de International Atomic Energy Agency (IAEA) over de ramp in de kerncentrale in Tsjernobyl (1986). In dit rapport staat dat veiligheidscultuur de verzameling van karakters en houdingen in de organisaties en van individuen is. Deze moeten ervoor zorg dragen dat, met de hoogste prioriteit, nucleaire veiligheidsonderwerpen de noodzakelijke aandacht krijgen. Daar heeft het in de kerncentrale van Tsjernobyl aan geschort. Het ongeval is, volgens de IAEA, mede veroorzaakt door de gebrekkige veiligheidscultuur. Deze constatering heeft geleid tot het ontwikkelen van een dynamiek rond veiligheidscultuur en tot aanbevelingen om deze te verbeteren[[6]](#footnote-6).

**Veiligheidscultuur en The Catalyst**

Als we stellen dat de veiligheidscultuur ingebed moet zijn in of minstens congruent moet zijn met de geldende organisatiecultuur, dringt zich uiteraard de noodzaak op om het begrip “cultuur” te definiëren. Er is immers geen eenduidige definitie van het begrip veiligheidscultuur. De in de literatuur gevonden begripsomschrijvingen van veiligheidscultuur beperken zich veelal tot het opereren van risicovolle bedrijven, zoals in de sector van de kerncentrales of van de (petro-)chemische industrie.

Voor deze bijdrage beschouwen we cultuur als “dat wat binnen de onderneming als goed wordt beschouwd[[7]](#footnote-7)”, zijnde “een geheel van normen en waarden, veronderstellingen, interpretaties en werkwijzen die voor de organisatie kenmerkend zijn[[8]](#footnote-8)”. Deze cultuur omvat zowel zichtbare en expliciete elementen, als onzichtbare en impliciete elementen..

Veiligheidscultuur ontstaat niet uit een toevallige samenloop van omstandigheden. Het volwaardig integreren van security in de bedrijfsvoering is een precieze evenwichtsoefening tussen drie componenten: de ondersteuning door het **management**, het beheer van het veiligheidsbeleid op het niveau van de **security manager**, en de **security practice** van elk lid van de onderneming afzonderlijk. Een klare kijk op de invulling van het veiligheidsbeleid voor elk van deze componenten is een absolute must om het veiligheidsbeleid te verbeteren. Ze zijn immers onderling sterk verbonden, en beïnvloeden elkaar voortdurend.

Robrechts & Thienpont ontwikkelde voor de interactie tussen deze componenten de Security Culture Circle of The Catalyst. Het circulair weergeven van de dynamiek rond veiligheid benadrukt dat het ontwikkelen van een veiligheidscultuur geen trapsgewijs proces is, maar een voortdurend zoeken naar evenwicht waarbij de diverse actoren binnen de organisatie elkaar constant beïnvloeden en in beweging zetten.



De Security Culture Circle werkt zodoende als een katalysator voor duurzame verandering. Het model benadert de organisatie vanuit een globaal, geïntegreerd geheel, en werkt parallel op de drie componenten. De evolutie naar een sterkere veiligheidscultuur verloopt via verschillende bewegingen op verschillende niveaus, die elk op hun beurt aanzetten tot security change management-processen. En dat werkt in het voordeel van alle partijen die bij de onderneming betrokken zijn: de medewerkers, managers, klanten én zakenrelaties.

**De maturiteitsschaal : The Security Maturity Model**

Boven beschreven we hoe security meer en meer ten dienste staat van de kernactiviteiten van de onderneming. Bijdragen tot de ondernemingsdoelstellingen wordt essentieel, en beveiliging evolueert aldus naar een volwaardig element van de bedrijfsvoering. Indien we erin slagen om de organisatiecultuur, en met name de veiligheidscultuur binnen een organisatie in kaart te brengen, dan kunnen we de onderneming een positie toekennen op de zogenaamde maturiteitsschaal. Deze geeft aan in welke mate de beoogde evolutie naar een volwaardige rol en positionering van security binnen de organisatie reeds werd voltrokken.

Via vragenlijsten en interviews kan de organisatie worden beoordeeld op de drie pijlers van The Catalyst: het management support, het security management en de uitvoering op de werkvloer, de security practices. Elk niveau wordt daarbij gescoord op de drie primaire elementen die het menselijke gedrag beïnvloeden : kennis, vaardigheden en commitment. Kennen, kunnen én willen zijn immers drie noodzakelijke voorwaarden om tot een effectieve veiligheidscultuur te komen.

Het resultaat van deze analyse vormt een matrix met 9 cellen. Elke cel krijgt een score op de Security Maturity schaal, gaande van de laagste score “denial” tot de hoogste score “strategic. Zo kunnen we voor elk niveau van de onderneming (management, security manager en uitvoerend personeel) nagaan in welke mate zij via hun kennis, kunde en commitment al dan niet bijdragen tot een positief veiligheidsklimaat.

Beschouwen we vervolgens alle cellen samen, dan komen we ook tot een globale score voor het hele bedrijf. Dit vormt als het ware een opnamemoment, een scan waarop het bedrijf niet enkel de eventuele discrepanties tussen bepaalde niveaus aangetoond ziet, maar ook een globale inschatting krijgt van haar positie op de algemene cultuurschaal



**Denial**

Organisaties in de denial-fase ontkennen alle veiligheidsrisico’s. Er is weinig of geen aandacht voor security, en de mensen op de werkvloer worden niet bereikt. Er is dus ook geen sprake van veiligheidsgedrag of van een veiligheidsbeleid.

**Reactive**

Ondernemingen die zich in de reactieve fase bevinden opereren ad hoc en slechts bij concrete incidenten. Men bereikt wel individuele werknemers met losse procedures, maar dit enkel met het oog op het beheersen van de schade. Vaardigheden en kennis rond security worden ontwikkeld op basis van concrete voorvallen. Beveiliging wordt gebruikt als een middel tot symptoombestrijding.

*Voor de beide bovengenoemde niveaus is er geen sprake van een structureel of preventief veiligheidsbeleid. Het thema veiligheid krijgt er enkel aandacht op het ogenblik dat zich problemen of incidenten voordoen. Organisaties die zich op één van deze beide levels bevinden benaderen security enkel vanuit een reactief perspectief.*

*Vanaf het derde niveau echter wordt de benadering meer en meer proactief. Organisaties die zich op één van de drie volgende trappen bevinden beschouwen veiligheid als een risico dat op het niveau van de onderneming beleidsmatig en vanuit preventief oogpunt moet worden aangepakt.*

**Systematic**

Bedrijven, die een systematische aanpak hanteren, implementeren hun veiligheidsbeleid zowel op het niveau van het management als van de deelgroepen. Veiligheid wordt hier op dezelfde systematische wijze behandeld als de andere bedrijfsrisico’s. De onderneming beschikt dan ook over de nodige systemen om deze risico’s te beheren. Veiligheidsgedrag vindt plaats vanuit een individuele motivatie. Het personeel wordt algemeen getraind op de collectieve systeemindicatoren. De functie van de security manager blijft hoofdzakelijk operationeel en dicht bij het primaire proces.

**Proactive**

Wanneer een organisatie zich op het proactieve niveau bevindt, zijn naast het uitvoerend personeel ook het management en de collectieve organisatie zich bewust van het belang van security. Veiligheid wordt proactief geïntegreerd in het business proces. Opleidingen rond security worden gedifferentieerd en aangepast aan de individuele behoeften. Security wordt meer en meer een onderdeel van het management en de security manager krijgt een meer beleidsmatige, strategische functie en positie.

**Strategic**

Op het hoogste niveau, het strategische, is de gehele organisatie van de aandeelhouders en de stakeholders tot de werkvloer doordrongen van het belang van security. Het securitybeleid wordt als een vanzelfsprekendheid beschouwd, en veiligheidsgedrag is voor iedereen een automatisme. Security is volledig geïntegreerd in het business proces en behoort tot de kernwaarden van de onderneming. Niet alleen de security manager maar ook het hele topmanagement stralen deze waarden uit.

**Het nieuwe paradigma : streven naar een strategische benadering van veiligheid**

Het is duidelijk dat dit strategische niveau binnen het nieuwe “betrokkenheidsparadigma” het na te streven doel wordt. Het betrekken van de gehele organisatie bij de security-politiek is hier een *top*management verantwoordelijkheid geworden. Een onderneming die security op strategische wijze benadert kenmerkt zich door de volgende elementen :

- Security neemt een belangrijke plaats in binnen de bedrijfsstrategie, en de interventies op het gebied van veiligheid zijn opgenomen in de kernwaarden van het bedrijf. Leidinggevenden geven dan ook bredere en langere termijn perspectieven aan veiligheid, geven richting aan en kunnen mensen **overtuigen** van het belang en de noodzaak van security. Deze ultieme strategische benadering van security kenmerkt zich door een zichtbare inzet op het niveau van het hoger management en de raad van bestuur.

- Bovendien houdt het management **voeling** met het uitvoerend proces door zich op de werkvloer te begeven, te praten met het personeel en feedback te vragen over het veiligheidsbeleid. Zij zijn zich hierbij bewust van hun voorbeeldfunctie en leven daartoe heel uitdrukkelijk zelf alle veiligheidsmaatregelen na.

- Tevens beschikt men binnen dit strategische kader over een uitvoerig **gedocumenteerd beleid** dat duidelijk de inzet van het bedrijf op het gebied van veiligheid omschrijft. Het is ontwikkeld door middel van overleg en het wordt uitvoerig gecommuniceerd aan de werknemers en andere mogelijke betrokken partijen. Het vraagt een duidelijke inzet van het topmanagement om continu de prestaties op het gebied van veiligheid te verbeteren.

- Uiteraard worden ook de nodige **middelen** voorzien om het securitybeleid vorm te geven : men voorziet budgetten voor opleiding, middelen of deskundigen op het gebied van veiligheid, en men besteedt een gedeelte van de managementtijd aan security. Tevens voorziet men middelen om erover te waken dat de verbeteringen op het gebied van veiligheid rendabel zijn.

- Werknemers **participeren** in de security activiteiten en werken ten volle samen met de werkgevers voor veilige werkplekken. Met het uitvoerend personeel wordt ook systematisch overlegd over de nieuwe en reeds gevestigde beleidsvormen, praktijken en prestaties op het gebied van veiligheid. Op democratische wijze zijn doelen en doelstellingen geformuleerd die samenhangen met het beleid om de voortdurende verbeteringen op het gebied van security te garanderen, en deze worden regelmatig herzien. Iedere werknemer is zich bewust van zijn verantwoordelijkheid met betrekking tot de veiligheid van diegenen die ze onder zich hebben, van zichzelf, van anderen met wie ze werken en ieder ander die de site bezoekt.

- Een continu **opleiding**sprogramma tenslotte zorgt ervoor dat de werknemers zich bewust blijven van de problemen op het gebied van veiligheid, en van hun eigen verantwoordelijkheid daarin. De opleidingen zorgen er tevens voor dat ze bekwaam zijn om de hen opgelegde taken uit te voeren ; de vakbekwaamheid wordt beoordeeld en herhalingscursussen worden systematisch voorzien.[[9]](#footnote-9)

Veiligheidscultuur past aldus binnen een highreliability-organisation. Om dit te realiseren heeft het management de juiste informatie, rapporteert de werkvloer over relevante veiligheidszaken en is de organisatie in staat om zich aan situaties aan te passen en te leren van de eigen ervaringen. Veiligheid op en voor de werkvloer houdt ook verband met de onderlinge collegialiteit: de bereidheid om elkaar aan te spreken op onveilig gedrag en zo mensen en organisatie te behoeden voor ongevallen. Belangrijke voorwaarde is dat het een ‘schuldvrije’ organisatie is, met een heldere grens tussen aanvaardbaar en onaanvaardbaar gedrag[[10]](#footnote-10).

**Security culture matrix : a useful tool**

Het meten van de veiligheidscultuur binnen een onderneming is niet enkel nuttig als aanzet tot een eventuele cultuurverandering. Ook losstaand daarvan heeft de meting op zichzelf reeds een positieve impact. Uit een Noorse studie blijkt dat het meten van het veiligheidsbewustzijn en van het naleven van security best practices het niveau van security praktijken binnen organisaties kan verhogen, wat resulteert in minder security incidenten als gevolg van onachtzaamheid of verwaarlozing. De werknemers namen in een dergelijke omgeving meer verantwoordelijkheid voor de beveiliging van fysieke- en data materialen, en ze namen een actievere rol op in het ontdekken en rapporteren van incidenten.[[11]](#footnote-11)

De metingen verhogen bovendien niet alleen de betrokkenheid van de werknemers bij de veiligheidscultuur. Ze kunnen ook gebruikt worden voor het bevorderen van een bedrijfsbrede waakzaamheid door leidinggevenden en lijnmanagers bij de regelmatige analyse van de security metingen te betrekken.[[12]](#footnote-12)

Het bewustzijn op zich van werknemers en managers dat er op regelmatige basis security culture cijfergegevens worden verzameld én dat deze door het hoger management worden gezien kunnen tenslotte eveneens substantieel bijdragen aan de naleving van het securitybeleid.

**Besluit : the challenge**

“De totaalsom aan cijfergegevens van security technologieën, processen en gedrag kan een klaardere kijk geven op de security toestand van een onderneming, zeggen security experts. Echter, een instrument creëren om security culture te meten levert geen algemeen geldend en universeel toepasbaar pakket op. Elke organisatie is uniek, en de instrumenten die gedrag meten moeten met zorg worden aangepast om het relevante gedrag en de relevante processen te vatten.”[[13]](#footnote-13)

Er bestaat dus niet zoiets als een universeel auditschema dat voor alle bedrijven passend is. Elke organisatie is anders, en dus zal ook elke audit tailor-made moeten zijn : op maat van de cliënt. Een gestandaardiseerde aanvangsvragenlijst – een quick scan als het ware- kan niettemin nuttige informatie aanleveren voor de invulling van deze audit-op-maat. De scan laat toe bedrijven een positie te geven op de maturiteitsschaal en zich aldus te spiegelen aan een algemeen geldend referentiekader. De scan geeft bovendien aan in welke segmenten van de organisatie de zwakste plekken zitten, en waaraan men dus prioritaire aandacht zal moeten schenken. Op deze wijze krijgt niet enkel een daarop volgende audit richting en diepgang, maar wordt tevens de aanzet gegeven tot het inleiden van de nodige veranderingsprocessen…

“Veilig werken is en blijft mensenwerk, elke dag opnieuw. Waar het vandaag om draait is de manier waarop de totale organisatie veiligheid en welzijn van haar medewerkers integreert in haar dagelijkse denken en handelen. Veiligheid dus als keuze, als waarde en cultuur.”[[14]](#footnote-14) Rekening houdend met de specifieke risico’s

hebt U dus de keuze om te bepalen waar uw bedrijf zich wil positioneren op de maturiteitsladder of hoe belangrijk security voor jouw organisatie is.

1. “Veiligheidscultuur en de werking van het veiligheidsbeheerssysteem bij BRZO-bedrijven”, Ing. Menno Meems en Jan ten Hove [↑](#footnote-ref-1)
2. “Security culture : the missing link?” door Jaak Colson op het R&T congres “Security meets the future” van 15 maart 2011. [↑](#footnote-ref-2)
3. Bon Bini, “Veiligheids- en Welzijnsenquête 2011 : de resultaten” in Veiligheidsnieuws, september 2011 [↑](#footnote-ref-3)
4. “Measuring and Evaluating an Effective Security Culture”, white paper, Cisco Systems inc. [↑](#footnote-ref-4)
5. Paul Robrechts, deel 1. [↑](#footnote-ref-5)
6. ir E. van der Reijden augustus 2000,Master of Crisis and Disaster Management, “Veiligheidscultuur: wat kan de brandweer voor het repressief optreden leren van de chemische industrie?” [↑](#footnote-ref-6)
7. “Security culture : the missing link?” door Jaak Colson op het Robrechts & Thienpont congres “Security meets the future” van 15 maart 2011 [↑](#footnote-ref-7)
8. Definitie van Quinn en Cameron [↑](#footnote-ref-8)
9. Al deze kenmerken worden als specifieke aandachtspunten beschreven in het wedstrijdprogramma voor de “Prijs van de Hoge Raad voor preventie en bescherming op het werk”. De risico’s voor *veiligheid* zowel als *gezondheid op het werk* worden hier op gelijke wijze behandeld. [↑](#footnote-ref-9)
10. ir E. van der Reijden augustus 2000,Master of Crisis and Disaster Management, “Veiligheidscultuur: wat kan de brandweer voor het repressief optreden leren van de chemische industrie?” [↑](#footnote-ref-10)
11. “Measuring and Evaluating an Effective Security Culture”, white paper, Cisco Systems inc. [↑](#footnote-ref-11)
12. ibidem [↑](#footnote-ref-12)
13. Measuring and Evaluating an Effective Security Culture”, white paper, Cisco Systems inc. [↑](#footnote-ref-13)
14. Bon Bini, “Veiligheids- en Welzijnsenquête 2011 : de resultaten” in Veiligheidsnieuws, september 2011 [↑](#footnote-ref-14)