Risico's bij het reizen naar

deel 1

Als wij naar het Journaal kijken wordt één ding steeds duidelijker: het wordt onrustiger in de wereld. Maakten wij ons vroeger alleen zorgen als medewerkers van de organisatie op reis gingen naar verre onbekende oorden, blijkt het nu helaas maar al te vaak dat het ook dichter bij huis onveiliger wordt. De werkgever is echter verantwoordelijk voor het creëren van een veilige werkomgeving voor de werknemer. Deze verantwoordelijkheid brengt met zich mee dat de organisatie een rol heeft als de werknemer zakelijk moet reizen. Steeds vaker komt de vraag naar voren wat had een werkgever vooraf kunnen of misschien wel moeten weten, voordat hij zijn medewerker op reis laat gaan?

Als een medewerker op reis gaat, kan er nogal wat fout gaan. Er kunnen ongelukken gebeuren, de medewerker kan ziek worden of de medewerker kan te maken krijgen met geweld dat direct of indirect tegen hem of haar gericht is. Wat de zaak complex maakt, is dat als er in het buitenland sprake is van geweld gericht tegen een medewerker de vraag opkomt of dit ongelukkig toeval is, op de verkeerde tijd op de verkeerde plaats, of dat het daadwerkelijk tegen de specifieke medewerker gericht is. Als het dan al specifiek tegen de medewerker gericht is, komt dit dan door zijn of haar nationaliteit of gedrag, of omdat deze voor een bepaalde organisatie werkzaam is? Dit zijn allemaal vragen die beantwoord moeten worden bij het bepalen van het risico voordat een medewerker op (dienst)reis gaat. Gebeurt er niets, dan lijkt het werk overbodig. Gebeurt er wel iets, dus doet er zich een incident voor, dan zal de werkgever op al deze vragen een antwoord moeten kunnen geven. Financieel zal een organisatie schade die een werknemer tijdens een (dienst)reis oploopt waarschijnlijk wel kunnen dragen. De grootste schade zal een organisatie op het vlak van imago kunnen oplopen, zeker als er aantoonbaar bewust risico's zijn geaccepteerd, en de medewerker daar het slachtoffer van wordt.

Management-summary

Werkgevers zijn verantwoordelijk voor het creëren van een veilige werkomgeving voor werknemers. Deze verantwoordelijkheid brengt ook met zich mee dat de organisatie een rol heeft als werknemers zakelijk moeten reizen. Steeds vaker komt de vraag naar voren wat had een werkgever vooraf kunnen of misschien wel moeten weten, voordat hij zijn medewerker op reis laat gaan? Is het voldoende om bij een commerciele aanbieder diensten op het gebied van travel security in te kopen, en blindelings op deze provider te vertrouwen, of had de werkgever kunnen en moeten weten dat dit niet voldoende is? Lastige vragen om te beantwoorden. In deze serie over travel security zal een context worden gegeven waar een werkgever rekening mee zal moeten houden wil hij niet verrast worden als er iets 'onvoorziens' gebeurt tijdens de dienstreis van een medewerker. De kernvraag is dan steeds was een incident inderdaad 'onvoorzien' of heeft de werkgever een risico geaccepteerd omdat het incident wel te voorzien was (lage kans en hoge impact).

Criminaliteit Wat kan een medewerker overkomen op (dienst)reis wat los staat van zijn nationaliteit of doel van zijn of haar bezoek aan een land? Vaak worden de begrippen 'geweld', 'overval', 'beroving', 'gijzeling' aanslag of 'kidnap' in één adem genoemd. De vraag is nu of de werkgever voor aanvang van een (dienst)reis daadwerkelijk al deze mogelijke incidenten bekijkt. Als het antwoord positief is, dan is de tweede vraag op basis van welke informatie afwegingen worden gemaakt. Het is achteraf natuurlijk lastig uit te leggen dat een medewerker afreist naar een relatief veilig land en veilige stad, maar toevallig in een hotel verblijft dat zich in de meest slechte buurt van de stad bevindt. Had de werkgever dat kunnen en moeten weten? De meeste commerciële aanbieders van diensten op het vlak van travel security zullen deze gedetailleerde informatie ook niet direct verstrekken. Welke aanvullende beveiligingsmaatregelen hadden getroffen kunnen, en misschien wel moeten worden, bij bekende criminele dreigingen? Ook een lastige vraag. In het tweede artikel van deze serie travel security, dat verschijnt in juni 2016, wordt ingegaan op dit deelonderwerp.

Terrorisme Geweld tegen personen en groepen, vanwege nationaliteit of geloof, neemt toe in de wereld. Dit zal naar verwachting niet afnemen, maar eerder toenemen. Terrorisme, en gemakshalve vallen daar voor wat betreft deze serie ook de aanslagen van de active shooter onder, is echter iets waar de Westerse wereld de komende decennia echt mee moet gaan leren leven. De interessante vraag is hoe heeft de organisatie zijn of haar werknemers voorbereid op dergelijk geweld dat zich tijdens een (dienst) reis kan voordoen? Heeft de medewerker een mooi rapport gekregen waarin staat dat hij of zij pleinen, stations, specifieke buurten of wijken en grote

het buitenland



groepen zoveel mogelijk moet mijden of is er ook aan de medewerker in een persoonlijk contact verteld wat hij of zij moet doen als het verkeerd gaat? Weet de organisatie eigenlijk wel wat er in specifieke gebieden, en buurten in steden, kan gebeuren of wordt er wederom vertrouwd op de commerciële informatie van diensten op het vlak van travel security? Wat had de organisatie kunnen en moeten weten voordat de medewerker op (dienst)-reis ging? Zo zijn er organisaties die, vanwege de expertise die zij zelf hebben opgebouwd, medewerkers aangeven dat zij beter niet in bepaalde buurten in Brussel en Antwerpen kunnen komen. Zo dicht bij huis kan het al onveilig zijn. Ook is er een Nederlands bedrijf dat medewerkers, als zij naar bepaalde landen afreizen, bijvoorbeeld afraadt om zogenaamde 'cargobroeken met zakken' te dragen. Waarom? Omdat in die landen, bij het zien van iemand in deze broeken, de aanname is dat het om een persoon met Amerikaanse nationaliteit gaat en zij als een rijk en verderfelijk volk worden gezien door bepaalde culturen. Hierdoor kunnen zij dus een target vormen. Wederom, complexe risicoafwegingen die de werkgever moet maken voordat de medewerker op reis gaat.

Is uw travel security beleid 'intelligence driven' omdat u zelf zeker wilt zijn dat medewerkers op (dienst)reizen geen onnodige risico's lopen? Een 'intelligence driven' travel security beleid vraagt alleen wel om expertise en analyse capaciteit binnen de eigen organisatie, een kostenpost.

In september, in het derde artikel van deze serie, zal dit onderwerp nader worden uitgewerkt.

Spionage Zoals de directeur van de Franse buitenlandse inlichtingendienst in een ver verleden al eens zei: 'er zijn geen bevriende landen, er zijn alleen landen met gemeenschappelijke belangen'. En als deze belangen veranderen dan is ook de vriendschap over. Helaas zien wij op dit moment in de wereld, en ook heel dichtbij, dat nationale belangen steeds meer de boventoon gaan voeren. Er is in West-Europa geen land dat niet onlangs, als wij de pers moeten geloven, bespioneerd is door 'vrienden' of vrienden 'heeft bespioneerd'. Dan laten we de landen aan de overkant van het water of op andere continenten nog maar even buiten beschouwing. De vraag is nu of de werkgever weet, ▸



voordat een medewerker op (dienst)reis gaat, wat de kans is dat deze medewerker door het bezoekende land of de bezoekende organisatie, als target wordt gezien? En als die kans bestaat, is de medewerker dan werkelijk voorbereid op de ongemakkelijke situaties die kunnen ontstaan?
Gezien de jaarverslagen van de verschillende Westerse veiligheidsdiensten, waarin geschreven wordt over vijandelijke inlichtingendiensten, had de werkgever de risico's kunnen en moeten weten. Zelden echter maakt een goede voorbereiding van de werknemer op dergelijke risico's deel uit van het standaard travel security beleid binnen organisaties. Zeer opmerkelijk als wij ons realiseren dat het vijandelijke inlichtingendiensten niet om de medewerker gaat, maar om de bedrijfsgeheimen waar deze medewerker toegang toe heeft. En het mooie van de hedendaagse terroristische dreiging is dat veel controles op buitenlandse luchthavens een prachtige cover opleveren voor spionage. Wilt u even uw laptop aanzetten en inloggen? Mooi, u krijgt uw laptop zo terug. Nee, wilt u dat niet? Daar is het vliegtuig terug, kijk het staat er nog. Aan het einde van het jaar zal dit onderwerp, spionage, en de maatregelen die u kunt treffen, worden uitgewerkt. Uitgangspunt is dat de medewerker nooit het slachtoffer mag worden, omdat hij als instrument wordt gezien, van inlichtingendiensten die bedrijfsgeheimen willen stelen.

Onrust Wat is de kans dat een medewerker terecht komt in een betoging, of erger, rellen vanwege politieke spanningen in een land? En als dergelijke betogingen en rellen zich voordoen, in welke steden en wijken kunnen deze dan voorkomen? Informatie die belangrijk is voor de medewerker die op (dienst)reis gaat naar een land waar spanningen zijn tussen politieke groeperingen. En wat is de kans dat 'onrust' wordt aangegrepen door een overheid om een medewerker van een bepaald land of organisatie aan te vallen omdat er tussen landen onenigheid is? Ook hier is weer het credo: gebeurt er niets, dan is dat natuurlijk goed. Doet er zich wel een incident voor, dan is de vraag wederom had dit voorkomen kunnen worden? Zo ja, had de werkgever kunnen weten of moeten weten dat aanvullende (beveiligings)maatregelen noodzakelijk waren? Het een na laatste artikel van deze serie zal inzoomen op de risico's die uit onrust en politieke spanningen voortkomen.
Loopt het nu helemaal uit de hand, dan zullen medewerkers die op (dienst)reis zijn zo snel mogelijk uit onveilige gebieden moeten worden weggehaald. Het laatste artikel van deze serie gaat uitvoerig in op het onderwerp repatriëring. Als recente incidenten een ding duidelijk hebben gemaakt, is het dat als er snel grote groepen mensen uit 'onveilige gebieden' moeten worden weggehaald, dat commerciële aanbieders van deze dienst vanwege de vele klanten die zij hebben toch vaak juist dan tegen problemen oplopen. Lokale contacten kunnen dan het verschil tussen dood en leven maken. De vraag is of de organisatie in dergelijke contacten heeft geïnvesteerd? Als het eenmaal fout gaat is het daar namelijk te laat voor. Weten oftewel goed geïnformeerd zijn kan veel ellende voorkomen.

Compliant De vraag is: bent u compliant, er is een contract met een aanbieder van diensten en dat is voldoende, of is uw travel security beleid 'intelligence driven' omdat u zelf zeker wilt zijn dat medewerkers op (dienst)reizen geen onnodige risico's lopen? Een 'intelligence driven' travel security beleid vraagt alleen wel om expertise en analyse capaciteit binnen de eigen organisatie, een kostenpost. Ook al omdat dit vraagt om het opbouwen en onderhouden van eigen (lokale) netwerken in het buitenland. Uiteindelijk gaat het om risicoacceptatie. Vindt de organisatie het belangrijk dat de risico's voor medewerkers op (dienst)reis geminimaliseerd worden, of mag er zo af en toe een ongelukje gebeuren? In het laatste geval hoeft de organisatie alleen maar te laten zien dat de medewerker een mooi rapport heeft meegekregen van een commerciële aanbieder van travel security diensten. Immers, 'shit happens', toch?

■ Berndt Rif MSc MBA Msec
Redactie@beveiliging.nl
■ Miranda Coppoolse
M.Coppoolse@live.nl