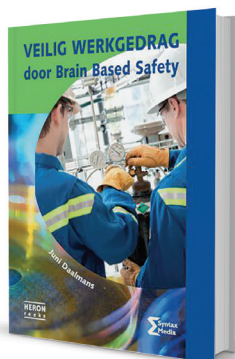


LITERATUUR**BOEKEN OP HET GEBIED VAN KWALITEITSMANAGEMENT****VEILIG WERKGEDRAG DOOR BRAIN BASED SAFETY**

Auteurs: Juni Daalmans

Uitgeverij: Syntax Media

ISBN: 978 94 91764 07 3

Prijs: € 35,00

We weten de laatste tijd veel meer over hoe het brein werkt: vooral over hoe het waarneemt, hoe het beslissingen neemt en hoe het acties voorbereidt en uitvoert. Voor dit boek is gebruikgemaakt van deze nieuwe kennis. Het stelt de vraag centraal wat de werking van het brein ons leert over veilig werkgedrag en welke mogelijkheden we hebben om dat gedrag te beïnvloeden. De auteur biedt de lezer

daarmee een vernieuwend inzicht in de psychologie die achter het succes of het falen van veel veiligheidsmaatregelen op het werk zit. Eén van de belangrijkste boodschappen is dat gedrag maar voor een zeer beperkt deel door bewuste processen wordt gedreven.

Vanuit zijn visie van Brain Based Safety illustreert Juni Daalmans hoe onveilig gedrag op de werkvloer effectief kan worden veranderd. Hij richt zich vooral op risicodetectie en risico-evaluatie, paraatheid, stress, de beleving van regels, teamwerk en leiderschap. De uitdaging is om de theorie en principes die Daalmans aanreikt in de praktijk van het veiligheidsmanagement toe te passen. Dit boek geeft een handreiking door duidelijke casuïstiek en het gebruik van voorbeelden uit de praktijk. Bovendien heeft ieder hoofdstuk behalve een samenvatting een afsluitend deel waarin de praktische mogelijkheden voor veiligheidsmanagement op een rij worden gezet.

BUSINESS CONTINUITY MANAGEMENT ... EN ICT

Je mag rustig stellen dat Business Continuity Management z'n oorsprong vindt in de ICT of misschien toen nog vooral de IT-functie van de organisatie. Vanaf het moment dat gebruikers een afhankelijkheid voelden, gingen zij eisen stellen. Nooit meer dan een bepaalde tijd zonder IT zitten en als er dan onverhoopt tóch iets mis gaat, absoluut geen gegevens kwijt zijn. Klonk als een redelijke eis, maar voor de IT-ers een opdracht c.q. uitdaging. Back-ups maken en dubbel uitgevoerde systemen waren onderdeel van de eerste continuïteitsinitiatieven. Gebruikers hadden echter vaak nog wel alternatieven; de oude werkwijze van voordat IT zo'n belangrijke rol kreeg. Hoe is dat nu?

Door Gert Kogenhop, bcm+

Tijdens de uitvoering van de risico-beoordeling binnen het Business Continuity Management Systeem (BCMS) komen ICT-gerelateerde bedreigingen in veel gevallen bovenaan de lijst te staan, met onder andere onverwachte uitval, hacking en andere vormen van cybercrime. Ook niet verwonderlijk is dat uit de Business Impact Analyse (BIA) blijkt dat de ICT-functies als uitermate belangrijk worden aangemerkt; veelal dé belangrijkste functie in de organisatie. Kunnen we nog wel zonder? Komt dit omdat we geen alternatieven meer hebben (Single Point of Failure)? Zijn er één of slechts enkele personen met specifieke kennis en vaardigheden binnen deze functie (Single Point of Knowledge)? Is alles binnen de ICT-

functie wel goed geborgd en vastgelegd in procesbeschrijvingen en procedures? Gaan we hier wel verantwoord mee om? Veel organisaties hebben een ICT-continuïteitsplan, dat bovendien vaak kwalitatief goed is. Er is nagedacht over zaken als contingency, uninterruptable power supplies, soms zelfs uitwijklocaties en disaster recovery met hersteltijdinstellingen die ook nog echt gehaald kunnen worden.

Maar de grote vraag is: 'Heeft de organisatie een continuïteitsplan voor het geval de ICT voor langere tijd niet beschikbaar is; een Operationeel Continuïteitsplan?' Hoe kan men de producten of diensten leveren aan afnemers en voldoet men bijvoorbeeld



nog aan wet- en regelgeving indien de computersystemen niet functioneren?

Denk eens over uw eigen situatie na. Is het goed geregeld? Laat u niet verrassen en besteed voldoende aandacht aan de dagelijkse gang van zaken ... en hoe doen we dat zonder ICT!