Het beveiligingsbewustzijn is het besef van het bestaan van beveiligingsmaatregelen. Zichzelf te realiseren wat dit betekent voor het gedrag, evenals het effect van het gedrag op het beperken van de aanwezige beveiligingsrisico's. Ofwel, dat ~~vele~~ ~~werknemers~~ niet alleen bekend zijn met de getroffen beveiligingsregelen en dat zij weten wat er ten aanzien van beveiliging van hun wordt verwacht, maar ook wat het effect is van hun gedrag op de risico's als zij zich al dan niet houden aan deze ~~vele~~ beveiligingsregels. Een ~~mooi~~ voorbeeld om het beveiligingsbewustzijn te ~~tonen~~ is de 'cleandesk' maatregel. Deze maatregels wordt ~~veelal~~ gezien als een noodzakelijk kwaad om er voor te zorgen dat medewerkers hun bureau ~~net~~ maken. Dat 'cleandesk' een maatregel is die ongewenste informatiespreiding door onbevoegden ~~verkleint~~, wordt vaak over het hoofd gezien. Denk maar eens na hoeveel mensen toegang tot een werkplek hebben als een medewerker er niet is? Denk hierbij aan de storingsmonteur of schoonmaker die in het kantoor werkzaamheden komen verrichten. Of de beveiliging, die even binnenkijkt tijdens een controleronde. Niet te vergeten de collega die de lege werkplek tijdelijk als vergaderplek gebruikt (al dan niet met externen). Informatie is in de maatschappij een kostbaar bezit en daardoor een groot risico. Beveiligingsbewustzijn is belangrijk, omdat het een ~~bedrijf~~ geld kan kosten! Soms ~~verschrikkelijk~~ veel geld! Denk aan het vergoeden van materiaal

te
medewerkers
maat
e
aanwezige
aardig
onderstrepen illustreren
normaal
schoon
ver reduceert
bevoegd
1/2/3/4/5
organisatie heel
hierbij

door inbraak of diefstal of het ~~foutief~~ lopen van die ene grote deal door het vroegtijdig lekken van informatie. Dit soort gebeurtenissen zijn voor veel organisaties een 'ver van hun bedshow'. Echter, er ~~moet~~ gekeken te worden naar beveiligingsrisico's

in de ~~ruimste~~ zin van het woord. Een gedachte binnen een ~~grote~~ organisatie is, dat het toch de taak is van de beveiligingsverantwoordelijke om de organisatie te beschermen tegen risico's? Inderdaad deze persoon zal zorg dragen voor het

beveiligingsbeleid, de kaders en randvoorwaarden. Daarnaast zal deze nauw betrokken zijn bij het in kaart brengen van de risico's. Echter een van de risico's voor een organisatie wordt - onbewust of bewust - gevormd door medewerkers. Door het open

laten staan van een ~~venster~~, het laten rondslingeren van ~~gegevens~~ of teveel informatie vertellen aan een ~~vriend~~ of collega over een bepaald onderzoek. Daarnaast ~~weet vele~~ organisaties niet wie ze in dienst hebben. Om een voorbeeld te

nemen: worden beveiligingsmedewerkers die alle in en outs van de beveiliging van de ~~vereniging~~ weten, gescreend? En de ~~Informaticus~~ die toegang heeft tot alle digitale informatie binnen de ~~vereniging~~? ~~Collega's~~ vormen één van de meest complex te

controleren risico's van een organisatie. Door ~~personeel~~, op alle niveaus, ~~goed~~ bewust te maken van de ~~afspraken~~, en het effect dat hun gedrag heeft op de risico's, kunnen incidenten ~~minimaal~~ gereduceerd worden. Uiteraard zijn er in ieder

→ dient

→ breedste veelvoorkomende

→ of het beveiligingsbedrijf

____ vet

→ raam

→ informatie enthousiast

→ kennis

→ weten veel

___vet → organisatie

→ ICT'er

→ organisatie

→ Medewerkers

→ medewerkers

→ maatregelen

e

~~bedrijf~~ verschillende doelgroepen te benoemen, ⟵ organisatie
waarvan het noodzakelijk is dat zij zich bewust
zijn van de getroffen beveiligingsmaatregelen. ___ onderstrepen
Operationele beveiligingsmaatregelen zijn voor
allen gelijk. Als het ~~noodzakelijk~~ is dat iedereen ⟵ vereist

zijn toegangspas zichtbaar draagt, dan ~~is~~ dit ook ⟵ geldt
~~geldig~~ voor ~~allen~~. Dus ook voor de ~~CEO~~ Maar de mate ⟵ ⟵ iedereen ⟵ directeur
van bewustzijn is niet voor iedereen gelijk. m
Bewustzijn wordt bepaald door de omgeving en de voor een deel
instelling van de persoon. Omdat ~~collega's~~ in een ⟵ medewerkers

~~bedrijf~~ in positie en afkomst verschillen, is het ⟵ onderneming
onvermijdelijk dat beveiligingsmaatregelen ~~niet~~ ⟵
~~terzelfdertijd~~ ontvangen worden. Daarom zijn ⟵ verschillend
binnen een organisatie ~~andere~~ niveaus van bewustzijn _ ⟵ verschillende
te onderscheiden. Beveiliging begint bij de

bedrijfsleiding. Deze ~~verzameling~~ bestaat uit leden ⟵ groep
van de Raad van Bestuur, hoofden, en directieleden, 1/2/3/4/5/6/7
zowel lijnmanagement als staf. De leidinggevenden .
op dit niveau dienen bewust een besluit te nemen
over het ~~al dan~~ niet investeren in beveiliging. ⟵ wel of

Voor hen is het belangrijk om duidelijk te maken wat zeer
de 'return of investment' is ten aanzien van het ___ vet
~~aanbevolen~~ beveiligingsprogramma. Wat zijn voor de ⟵ voorgestelde
organisatie de risico's, wat kost het als 1/2/3/4/5
dergelijke risico's zich voltrekken en in welke

mate dekt het voorgestelde beveiligingsprogramma de ___ vet
risico's af? Als een beveiligingsprogramma door een
directie wordt aangemerkt als een ~~onkost~~ waar geen ⟵ kostenpost
compensatie tegenover staat, dan zal er bij andere
prioriteiten snel worden gesneden in het ___ onderstrepen

beste versterkt worden door het vertalen van het beveiligingsconcept in ekonomische termen. Managers uit het ~~lagerkader~~ hebben een andere kijk op het beveiligingsconcept dan de directie. Het belang van deze manager ligt bij de prestaties van de

beveiligingsbudget. Het is dus zaak inzichtelijk te maken dat het investeren in ~~afspraken~~ tegen iets dat wellicht nooit zal ~~gebeuren~~ (bijvoorbeeld een terroristische aanval) opweegt tegen de kosten als het wel plaatsvindt. En dat blijkt in de

~~realiteit~~ lastig te zijn. Vaak zijn de baten van beveiligingsmaatregelen concreet niet aantoonbaar te maken en heeft dit als consequentie dat de perceptie bestaat uit afname van de winst. Het bewustzijn van het hoger management kan nog het

afdeling. Hierop word hij beoordeeld. Als een manager de perceptie heeft dat ~~vele~~ beveiligingsmaatregelen buitenproportioneel zijn of dat beveiligingseisen de productiviteit van de afdeling beïnvloeden, zal deze ~~manager~~ een ~~het~~

~~negatieve~~ houding ten opzichte van het beveiligingsconcept hebben. Is hij aan de andere kant zich bewust van de risico's ~~buiten~~ zijn afdeling en ook wat de ~~grote~~ gevolgen voor de afdeling zijn indien een risico zich voltrekt, zal

hij de beveiligingsmaatregelen juist als een ~~on~~belangrijk onderdeel van het functioneren van zijn ~~bedrijf~~ gaan zien. Het bewustzijn van het middenkader kan bevorderd worden door ze zeer nouw te betrekken bij het opstellen van

c
middenkader
vet
maatregelen
plaatsvinden
praktijk
t
verantwoordelijke
afkeurende
binnen
afdeling
a

Tot slot lichten we er ook managers uit, met beveiliging en ict in hun ~~geldbeugel~~. Deze doelgroep ~~van~~ facilitair managers vervult een belangrijke rol in het ~~maken~~ van beveiligingsbewustzijn. Hij zal ~~voor~~ zijn afdeling beveiligingsmaatregelen. Ook ~~moet~~ helder aangegeven te worden wat de gevolgen zijn van het niet navolgen van de maatregelen. Dikwijls worden collega's bij de start van het dienstverband op de hoogte gebracht van de actuele beveiligingsregels en maatregelen. Naast veel andere, voor hen belangrijke, informatie moet het onderwerp ~~inzake~~ beveiliging ook nog even in een introductiedag worden geperst. De ~~laatste~~ indruk is dan dat de organisatie het dan wel niet zo nauw zal nemen met de beveiliging en de negatieve tendens is gezet. Onderwerpen die voor de medewerker van persoonlijk belang zijn of direct een ~~verband~~ hebben tot zijn functie goed opgepikt worden en als de medewerker dat nodig acht, zelfs enkele keren herhaald, zodat hij weet wat er van hem verwacht wordt. Als tijdens een introductie voor de medewerker niet ~~onmiddellijk~~ duidelijk is dat het beveiligingsprogramma belangrijk is voor de invulling van zijn functie, zal hij het aannemen ter kennisgeving en er verder niet meer op terugkomen. Tenslotte is voor hem de noodzaak niet ~~er~~ om er op terug te komen! ~~Bovendien~~ bestaat het risico dat hij zelfs geïrriteerd raakt door het effect van de maatregelen op zijn werkzaamheden.

facilitair
portefeuille
creëren
binnen
dient
vet
d
C
t
heel
eerste
cursief
relatie
goed
onderstrepen
direct
vet
aanwezig
Daarnaast

het beveiligingsbewustzijn als een tweede natuur
onder de aandacht van de beveiligingsmedewerkers ___ cursief
moeten brengen. Tenslotte is beveiliging voor hem
'core business'. Zijn ~~gebruikers~~ moeten zich er ⊢⊣ mensen
onder andere van bewust zijn dat ze, doordat ze

fysiek op bijna alle plaatsen binnen een
organisatie toegang hebben, hierdoor ook risico's
lopen en aan bepaalde verleidingen bloot staan. ___ vet
Hetzelfde geldt voor de afdeling ict. ~~Enkel~~ gaat ⊢⊣ Alleen
het hierbij over ~~gewone~~, geautoriseerde toegang. ⊢⊣ logische