Gids voor Risicobeheersing

Beveiliging

Introductie

Om te voorkomen dat indringers, vandalen en brandstichters toegang krijgen tot een pand, zijn passende beveiligingsmaatregelen essentieel. Sommige indringers zullen opportunistisch zijn, maar anderen zijn vastberaden, georganiseerd en hebben hun huiswerk gedaan door zich op de 'zwakste schakel in de keten' te richten. Dit is de reden waarom een benadering met "gelaagde bescherming" vaak de beste benadering is om een beveiligingsniveau te bereiken dat in overeenstemming is met het risico..

Essentiële principes voor beveiliging van eigendommen

Beveiligingsmaatregelen kunnen worden beschouwd in drie categorieën:

- Fysieke veiligheid
- Electronische beveiliging
- Menselijk veiligheid

Enkele belangrijke punten om te onthouden bij het beoordelen of overwegen van beveiligingsmaatregelen zijn:

- Gebruik gespecialiseerde installateurs die zijn gecertificeerd en goedgekeurd door de juiste bestuursorganen en die installeren in overeenstemming met de toepasselijke norm en de richtlijnen van de fabrikant
- Integreer beveiligingsmaatregelen die samengaan. Dit omvat zowel integratie met brand-, gezondheids- en veiligheidsmaatregelen als cyberveiligheidsmaatregelen
- Zorg dat beveiligingsmaatregelen in overeenstemming zijn met het risico
- Zorg dat beveiligingsmaatregelen regelmatig worden beheerd en onderhouden
- Zorg dat het personeel is opgeleid in het gebruik van beveiligingssystemen en weet hoe te reageren op activeringen of storingen

Best practices bij het beoordelen van bestaande of geplande beveiliging zijn te vinden in Essential Principles for the Security of Property (S20), gepubliceerd door RISCAuthority. Dit omvat veiligheidsrisico-beoordeling, effectieve communicatie, vermindering van intrinsiek risico, strategie, actieve en passieve beschermingsmaatregelen, selectie van leveranciers, training, onderhoud, continue beoordeling en het bewaren van documenten.

Beveiligingshekwerk

Beveiligingsafrastering, vooral in combinatie met statische afschermingen en / of beveiligingsverlichting, en CCTV is een zeer nuttige primaire verdedigingslinie.

Er zijn twee hoofdtypen omheiningen:

- Omtrekhekwerk, zoals gaas, gelast hekwerk en stalen palissade
- Geëlektrificeerde veiligheidsafrastering

Gecertificeerde bedrijven kunnen omheiningen installeren volgens de relevante nationale norm en richtlijnen van de fabrikant.

Onderhoud van veiligheidshekken is erg belangrijk en er moeten procedures zijn waarbij het hekwerk regelmatig in zijn geheel wordt geïnspecteerd, afhankelijk van de mate van het risico.

Eventuele breuken, gaten of andere beschadigingen moeten onmiddellijk worden gerepareerd. Bomen en kreupelhout mogen, waar mogelijk, niet te dicht bij de afrastering (aan weerszijden) groeien, aangezien deze voor verhulling kunnen zorgen en mogelijk een hulpmiddel kunnen zijn bij het beklimmen van de afrastering. Om dezelfde redenen mogen pallets, materiaalopslag, bijgebouwen, bakken, enz. niet dicht bij een veiligheidshek worden geplaatst.

Poorten in veiligheidshekken moeten worden geïnstalleerd met een evenredig beveiligingsniveau als het hek zelf. In het bijzonder mogen ze geen gaten of klimhulpmiddelen hebben die door indringers kunnen worden benut.

De scharnierpennen van veiligheidspoorten moeten worden afgedekt met een schijf van zacht staal die aan de bovenkant van de pen is gelast om te voorkomen dat de poorten van hun scharnieren worden getild, en hangsloten met gesloten beugels van goede kwaliteit moeten worden gebruikt om poorten te beveiligen.

Alarmsignalering op hekken kan lokaal (hoorbaar) zijn voor een on-site beveiligingsfaciliteit of op afstand naar een particulier alarmcentrale (PAC) - zie verder voor meer informatie over inbraakalarmen..

Gesloten Televisie Circuit (CCTV)

De aanwezigheid van een CCTV-systeem wordt algemeen aanvaard als een nuttig middel om ongeoorloofde toegang en criminele activiteiten af te schrikken of anderszins te helpen opsporen en beperken.

Er zijn veel soorten CCTV-systemen beschikbaar. Welk type systeem er ook wordt gebruikt, het is belangrijk dat het betrouwbaar is, storingsbestendig en over de juiste dekking beschikt. Alle 'risicogebieden' moeten worden afgedekt, bijv. toegangspunten, naderingsroutes en gebieden die aantrekkelijk zijn voor indringers / criminelen. Een geschikte methode voor 'realtime' monitoring en reactie op bekeken gebeurtenissen is ook essentieel.

Gecertificeerde bedrijven kunnen CCTV installeren volgens de relevante nationale normen in overeenstemming met de richtlijnen van de fabrikant.

Door detector geactiveerde CCTV-systemen, bewaakt in een video- of alarmcentrale op afstand, zorgen dat inbraak op afstand kan worden gedetecteerd en geobserveerd zonder dat continue bewaking ter plaatse nodig is. Ze moeten worden geïntegreerd met inbraakalarmsystemen en, wanneer aan specifieke voorwaarden wordt voldaan, kunnen ze in aanmerking komen voor een reactie van de politie.

Voorafgaand aan de installatie van CCTV-systemen dient in overleg met verzekeraars een zorgvuldige analyse te worden gemaakt.

Deuren

Deuren, vooral die met een lichtere constructie, kunnen kwetsbaar zijn voor aanvallen door indringers, zelfs als ze zijn uitgerust met sloten en grendels van de beste kwaliteit. Deurpanelen kunnen worden ingetrapt of handgereedschap kan worden gebruikt om een gat in de vorm van een lichaam te snijden.

Zelfs deuren die er solide uitzien, blijken bij nadere inspectie vaak slechts een halfvaste constructie te hebben en / of gevuld met lichtgewicht materiaal. Het is daarom essentieel om dergelijke deuren te versterken met plaatstaal; met name voor buitendeuren of binnendeuren in kwetsbare of risicogebieden.

Houten deuren moeten van buitenkwaliteit zijn en een minimale dikte van 45 mm hebben, waarbij opgemerkt wordt dat hardhout over het algemeen sterker is dan zachthout.

De volgende specificatie is geschikt voor slotenmakers of bouwers bij het bekleden en verbeteren van de deurbeveiliging:

- Deuren die aan de buitenkant moeten worden bekleed met een enkel paneel van plaatstaal van niet minder dan 1,5 mm, bevestigd met slotbouten met een minimumdiameter van 6 mm die door de volledige dikte van de deur gaan en rond de omtrek van de deur op een onderlinge afstand van maximaal 150 mm worden geplaatst

- Slotbouten die op gelijke afstand door de dwarsverbanden en middenrails van de deur moeten worden aangebracht
- Alle borgmoeren en ringen moeten aan de binnenkant van de deur aan de bouten worden gelast, of als alternatief moeten de uiteinden van de bouten worden aangepast (geboord) zodat ze niet gemakkelijk ongedaan kunnen worden gemaakt
- Als het in uitzonderlijke omstandigheden nodig is om de deur aan de binnenkant met staal te versterken, moeten houtschroeven met een diameter van 5,5 mm met terugslagkoppen en een lengte van minstens 25 mm worden gebruikt met h.o.h. afstand van niet meer dan 100 mm in plaats van slotbouten
- Scharnierbouten moeten boven en onder worden geïnstalleerd. Om het extra gewicht te kunnen dragen, kan het nodig zijn om extra scharnieren aan de deur te monteren

Een alternatief is het installeren van interne of externe afsluitbare stalen spijlen / gaasdeuren, rolluik en of interne inklap- of vouwbare stalen roosters. Deze moeten professioneel worden aangebracht en gecertificeerd zijn in overeenstemming met de erkende nationale veiligheidsnorm.

Ramen

Veel indringers geven de voorkeur aan toegang via een raam om onbevoegde toegang te krijgen.

Raamsloten bieden een minimaal beschermingsniveau dat voldoende kan zijn om een onervaren opportunist af te schrikken, maar ze zijn niet bestand tegen een vastberaden poging tot inbraak. Het verwijderen van een heel raamkozijn met handgereedschap, of het simpelweg breken en verwijderen van een ruit is doorgaans voldoende om toegang te krijgen.

Het kan daarom in veel gevallen wenselijk zijn om te zorgen dat glas wordt gelaagd, en om stalen tralieroosters aan te brengen op ramen, met name op kwetsbare locaties.

De volgende specificatie is geschikt voor slotenmakers of bouwers bij het installeren van raamroosters:

- Roosters die bestaan uit verticale massieve stalen staven met een diameter van ten minste 20 mm of een vierkante doorsnede met een onderlinge afstand van niet meer dan 100 mm. De staven moeten worden gelast aan verbindingsstaven van plat staal met een tussenafstand van niet minder dan 35 mm x 6 mm en een onderlinge afstand hebben van niet meer dan 600 mm
- Roosters te bevestigen, bij voorkeur aan de binnenkant van een raamopening, op een van de volgende manieren:
    - Staven die boven- en onderaan in het metselwerk worden ingegoten tot een diepte van minimaal 50 mm en minimaal 50 mm teruggezet van het oppervlak van de muur
    - Trekstangen die moeten worden gesneden, uitgespreid en in metselwerk worden gevoegd tot een diepte van minimaal 50 mm en minimaal 50 mm teruggezet van het oppervlak van de muur
    - De spijlen moeten worden vastgelast aan een frame van hoekijzer met een minimale afmeting van 35 mm x 35 mm x 3 mm die aan het metselwerk rondom het raam (niet aan het raamkozijn) wordt bevestigd met een 75 mm x 9 mm gepatenteerde ankerbout voor bevestiging in metselwerk (bijv. keilbouten) of verzonken houtschroeven met een diameter van 75 mm en 5,5 mm met geschikte gepatenteerde muurpluggen met intervallen van 300 mm rondom de opening. Bouten of schroeven moeten aan het frame worden gepuntlast

U kunt ook overwegen om interne of externe afsluitbare stalen spijlen / gaashekken, rolluiken of interne inklap- of vouwbare stalen roosters te overwegen. Deze moeten professioneel worden aangebracht en gecertificeerd zijn als zijnde in overeenstemming met een erkende nationale veiligheidsnorm.

Sloten

Een breed scala aan veiligheidssloten is te koop. Deze omvatten 5-puntsluitingen, Euro-cilindersloten, multi sluitingen en magnetische sloten. De complexiteit en kwaliteit van het ontwerp en de fabricage van een slot is fundamenteel voor het geboden beschermingsniveau en als zodanig zijn er veel normen die elk type slot beschrijven.

Beweringen dat een slot is getest volgens een bepaalde norm, kan alleen worden vertrouwd als de test is uitgevoerd en "gecertificeerd" door een erkende, onafhankelijke nationale testinstantie..

Inbraak Alarmen

Inbraakalarmen zijn vaak een voorwaarde voor verzekering. Ze bieden een hoog niveau van diefstalpreventie en vroege melding van ongeoorloofde toegang.

Inbraakalarmsystemen moeten worden geïnstalleerd en regelmatig worden onderhouden door een bedrijf dat door het desbetreffende nationale bestuursorgaan en de lokale politie is erkend als installateur van inbraakalarmsystemen. Dergelijke bedrijven kunnen installeren en onderhouden in overeenstemming met de toepasselijke normen en richtlijnen van de fabrikant.

Tenzij specifieker bevestigd, dient de beveiligingsklasse van het inbraakalarmsysteem (detectie- en controleapparatuur) klasse 3 te zijn, zoals beschreven in BS EN 50131.

Het is ook waarschijnlijk dat signalering op afstand naar een meldkamer een voorwaarde voor verzekeringsdekking is. De PAC moet worden geïnspecteerd en gecertificeerd door de juiste nationale overheidsinstantie. In sommige gevallen kan een beperktere selectie van installatie-, onderhouds- en / of bewakingsbedrijven gerechtvaardigd zijn. De verzending van alarmsignalen naar de meldkamer moet gebeuren via een dual path (DP) afstandssignaleringsproduct dat voldoet aan de vereisten voor een DP-niveau 4 zoals beschreven in BS EN 50136.

Om ook in aanmerking te komen voor een reactie van de politie, zal de politie formeel moeten afspreken dat het systeem compliant genoeg is om een respons te rechtvaardigen. Om dit te verkrijgen, moet het alarmsysteem voldoen aan de juiste nationale normen, zoals hierboven beschreven, en aan alle andere normen die van toepassing zijn op de verzending van "verifieerbare" waarschuwingen naar de meldkamer. Dergelijke waarschuwingen bieden de politie de zekerheid dat de waarschuwingen echt zijn en niet vals. Dit kan ook met zich meebrengen:

- Overeengekomen methoden voor het in- en uitschakelen van alarmen
- Naleving van het eigen beveiligingsbeleid van de lokale politie
- Opeenvolgende alarmdetecties binnen een bepaald tijdsbestek (twee detectoren bevestigen dat de waarschuwingen echt zijn, in plaats van slechts één)

Als het alarm is geactiveerd (of de activering nu is bevestigd of niet), of als een signaleringspad verloren gaat, moet de aangewezen sleutelhouder het pand (bij voorkeur niet alleen) onmiddellijk bezoeken om de reden voor de activering te onderzoeken.

Op een waarschuwing, storing of telefoontje van de meldkamer moet worden gereageerd door personeel van de locatie dat binnen 20 minuten aanwezig kan zijn (bij voorkeur niet alleen) of door een professionele erkende sleutelhouder, zelfs als de politie heeft gereageerd.

Als er een storing is in het alarmsysteem of een alarmsignaalpad, moet een alarmtechnicus worden gebeld en mag de sleutelhouder het pand niet onbeheerd achterlaten totdat deze volledig opnieuw is beveiligd, waarbij het alarmsysteem en de signaleringspaden volledig zijn gereset.

Stel de verzekeringsvertegenwoordigers onmiddellijk op de hoogte als er een melding is van een verlaagd niveau of intrekking van de politierespons op het inbraakalarmsysteem.

Laat het pand nooit onbeheerd achter, tenzij het fysiek is beveiligd en het alarmsysteem volledig is ingesteld inclusief de aangewezen methoden voor signalering op afstand.

Telefoonnetwerken in heel Europa worden binnenkort zodanig geüpgraded dat alarmsystemen moeten communiceren met de meldkamer met behulp van IP-technologie (Internet Protocol). Alarminstallateurs en meldkamers kunnen u adviseren over eventuele wijzigingen aan bestaande alarmsystemen.

Het volgende biedt verdere best practice richtlijnen die geschikt zijn voor de meeste bedrijfsgebouwen:

- Behalve voor aanvullende besturingsapparatuur (zoals afstandsbedieningen en digitale sleutellezers), moet besturings- en signaleringsapparatuur zich op een plaats bevinden waar deze voor het algemene zicht verborgen is en het minst kwetsbaar is voor aanvallen
- Hoorbare waarschuwing moet worden gegeven door ofwel twee externe zelf aansturende akoestische waarschuwingsapparaten of door één extern zelf aansturend waarschuwingsapparaat en een interne zelf aansturende sirene of tweekleurige elektronische sirene, elk met een geluidsemissie van ten minste 100 dB op 1 meter afstand waar lokale / nationale wetten dit toestaan)
- Waar het niet mogelijk is om een externe waarschuwingsinrichting hoger dan 3 meter te installeren (d.w.z. zodat deze niet gemakkelijk vanaf de grond bereikbaar is), monteer dan twee externe, zelf aansturende waarschuwingsinrichtingen. Ze moeten, waar mogelijk, op verschillende hoogtes van het pand worden geplaatst
- Als het systeem over signalering op afstand beschikt, wat normaliter wenselijk is, plaats dan een intern waarschuwingsapparaat op afstand van het bedieningspaneel om de positie van het paneel bij activering niet te identificeren. Om dezelfde reden moeten alle interne zoemers die worden gebruikt als onderdeel van de procedure voor het in- / uitschakelen van het alarm, ook op afstand worden geplaatst vanaf het bedieningspaneel.
- De manier om uit te schakelen moet gebeuren via een toegangsdeurslot dat is gekoppeld aan het alarm, tenzij de toegangsroute of het pand als laag risico wordt beschouwd, in welk geval het gebruik van een afstandsbediening (zender of transponder) bij binnenkomst acceptabel kan zijn
- Veel alarmbedrijven zullen inbraakalarmsystemen op afstand willen onderhouden, zonder het pand te bezoeken. In sommige gevallen kan deze functionaliteit de verzekeringsdekking ongeldig maken

Het niet volledig beveiligen en alarmeren van het pand kan de verzekeringsdekking ongeldig maken .

Bewaking

Traditionele bewaking blijft een steunpilaar in de beveiligingsstrategie. Om ervoor te zorgen dat bewakers een goede verdediging bieden, moeten ze worden onderworpen aan geschikte achtergrondcontroles en certificeringen, en aan geschikte systemen ter plaatse, zoals verificatie van bewakingsrondes en controles voor autonome werkers.

Beveiligingspersoneel met een geschikte overheidsbevoegdheid kan worden ingehuurd bij bedrijven met vergelijkbare vergunning.

Bewakingsoplossingen moeten zorgvuldig worden beheerd en geïntegreerd met alle andere beveiligingsmaatregelen.

Bescherming van leegstaande gebouwen

Brand, diefstal en opzettelijke schade in leegstaande panden zijn belangrijke oorzaken van schade.

Er zijn aanwijzingen dat zodra een gebouw is vernield, er binnen korte tijd nieuwe vernielingen kunnen plaatsvinden.

Goede beheerprocedures, waaronder regelmatige inspectiebezoeken (minstens één keer per week) en regelmatig onderhoud van het onroerend goed en de brand- en beveiligingssystemen, kunnen criminele aanvallen helpen voorkomen en ook de uiteindelijke kosten van herstelwerkzaamheden verlagen als zich een schade voordoet.

Het is belangrijk om te zorgen dat de structuur van het gebouw wordt onderhouden en in goede staat wordt gehouden. Zonder regulier onderhoud kan een leegstaand pand snel vervallen en ongewenste aandacht trekken, zoals van vandalen en kiepwagens. Graffiti moet worden verwijderd en eventuele schade moet onmiddellijk worden hersteld.

Leegstaande gebouwen zijn een aantrekkelijke speelplaats voor kinderen. Kinderen en andere overtreders zijn een zorgplicht verschuldigd, zodat zelfs leegstaande gebouwen voor zover redelijkerwijs mogelijk in een veilige

omgeving moet worden gehouden. Leegstaande gebouwen moeten natuurlijk worden gehandhaafd als veilige omgevingen voor mensen met legitieme toegang.

Best practice voorzorgsmaatregelen moeten de verwijdering van alle niet-essentiële inboedel en installaties omvatten. Voldoende fysieke beveiliging en alarmen moeten echter worden gehandhaafd. Verdere maatregelen kunnen het gebruik van bewaking, het dichttimmeren van ramen / deuren en het gebruik van tijdelijke alarmen omvatten.

Mistgeneratoren

Een mistgenerator is een elektronisch bediend beveiligingssysteem dat bij activering een dichte "mist" produceert om een potentiële inbreker te desoriënteren en verdere toegang tot het beschermde gebied te ontmoedigen / belemmeren.

Mist wordt geproduceerd door glycol (of een andere vloeistof) door een verwarmingsblok te leiden, waar het verdampt voordat het wordt uitgestoten in het te beschermen gebied. Terwijl de damp in de atmosfeer vrijkomt, condenseert deze onmiddellijk en vormt het een dichte witte mist. Op glycol gebaseerde producten worden als niet giftig beschouwd.

Mistbeveiliging kan worden gecombineerd met zwaailichten en sirenes om potentiële inbrekers verder te desoriënteren. Deze systemen worden doorgaans gebruikt in winkelomgevingen en er moet zorgvuldig worden nagedacht over de veiligheid van werknemers en klanten.

Mistgeneratoren moet worden ontworpen, geïnstalleerd en onderhouden in overeenstemming met de specificaties van de fabrikant en voldoen aan BS EN 50131-8 in combinatie met de vereisten van de verzekeraar.

Contant geld beveiliging en beveiliging tegen beroving

Contant geld blijft een van de meest attractieve goederen. Bedrijven die het meeste risico lopen hebben vaak hoogwaardige, gemakkelijk te vervoeren goederen, zoals sieraden, merkkleding, draagbare elektronische apparaten, tabaksproducten, wijnen en gedistilleerde dranken. Contant geld-gerelateerde activiteiten zoals postkantoren, pandjesbazen, wedkantoren en benzinestations lopen ook een hoog risico om aangevallen te worden. Geldautomaten verhogen ook de kans op een aanval, net als nachtelijke werkuren.

Waar mogelijk moet de hoeveelheid contant geld die op een bepaald moment wordt aangehouden tot een minimum worden beperkt. De kasvoorraad kan verder worden verminderd door betalingen te doen / ontvangen per cheque of elektronische overschrijving.

Personeel dat betrokken is bij blootstelling aan contant geld, en zelfs diegenen die niet rechtstreeks met contant geld omgaan, kunnen in een bedreigende situatie terechtkomen door simpelweg aanwezig te zijn ten tijde van een criminele aanval.

Naast het hebben van een goede gelaagde verdediging op het terrein, is er nog een aantal maatregelen die kan worden genomen om het risico te verkleinen, waaronder:

- Goed beheer en procedures bij het omgaan met contant geld
- Versterking van geldkamers, deuren en beglazing
- Borgen van contant geld en kostbaarheden in kluizen
- Gebruik van professionele gelddragers
- Mistgeneratoren

Beveiliging van computers en elektronische apparatuur

Computerapparatuur en andere elektronische kantoorapparatuur in bedrijfspanden zijn bijzonder aantrekkelijk voor dieven. De impact van diefstal is niet alleen gerelateerd aan het verlies van de hardware, maar kan ook de gegevensbeveiliging in gevaar brengen en aanzienlijke bedrijfsonderbreking veroorzaken.

In omgevingen waar dieven kunnen opereren, waaronder open kantooromgevingen, moet draagbare computerapparatuur veilig worden opgeborgen of aan het werkstation worden vastgemaakt wanneer ze niet worden gebruikt. De beveiligingsapparatuur moet compatibel zijn met de computerapparatuur en de bijbehorende garanties.

In omgevingen waar items van hoge waarde worden gebruikt of opgeslagen (bijvoorbeeld serverruimtes), is er een aantal apparaten en oplossingen zoals beveiligde ruimtes, kooien, verankeringsapparatuur enz. die kunnen worden ingezet om het risico op diefstal te minimaliseren. Daarnaast zijn er veel procedurele maatregelen die kunnen worden toegepast om risico's te verminderen.

Brandstofcriminaliteit

Bovengrondse dieseltanks op boerderijen, opslaglocaties voor goederen en woongebouwen zijn een doelwit voor brandstofdieven.

Bijkomende schade als gevolg van brandstofdiefstal kan vaak leiden tot brandstoflekkage die de grond verontreinigt, met bijbehorende hoge opruimkosten.

Gezien dit diefstalrisico moeten alle brandstofopslagfaciliteiten worden onderworpen aan een passende risicobeoordeling.

Beveiligingsmaatregelen voor brandstoftankdiefstal omvatten:

- Isolatie van elektrische pompen
- Gesloten beugelsloten op vuldoppen
- Antisifon inrichtingen
- Minimaliseren van brandstofniveaus
- Passende toegangscontroles, hekwerken, verlichting, CCTV en alarm waar praktisch

Metaaldiefstal

De stijgende wereldwijde vraag naar metalen heeft geleid tot een aanzienlijke stijging van hun marktwaarde, dat op zijn beurt heeft geleid tot een zeer sterke stijging van het aantal metaalgerelateerde diefstallen, met name van non-ferrometalen zoals koper en lood.

Bij veel van de schades waren dieven betrokken bij het zoeken in leegstaande gebouwen naar koperen kabels, leidingen, sanitair en lood op de daken.

Naast de kosten voor het vervangen van gestolen eigendommen, kan de schade aan de structuur van het gebouw door de gedwongen verwijdering ervan ook zeer hoge reparatiekosten oplopen. Waar de diefstal van lood op de daken niet snel genoeg werd ontdekt, zijn de schades sterk toegenomen als gevolgschade door het binnendringen van regenwater.

Het is belangrijk om alle potentiële risicogebieden te identificeren - voorraad, bouwfittingen, loden dakpannen, loodgieterswerk / leidingen, bekabeling / kabelgoten, boilers, apparatuur in de technische ruimte, hekken / poorten / palen, enz., aangezien sommige niet voor de hand liggen.

Tot de oplossingen behoren de oplossingen die al in deze gids zijn beschreven (beveiligde zones, alarmen, cameratoezicht enz.). Het gebruik van beveiligingslabels / markeringsschema's kan ook voordeel opleveren.

Normen en verdere bronnen

De volgende lijst bevat informatie over bronnen, richtlijnen en formele normen die in heel Europa relevant kunnen zijn.

Essentiële bronnen

RISCAuthority (het technisch adviesorgaan van de Britse vastgoedverzekeraars) is een gezaghebbende bron voor informatie over alle onderwerpen en maatregelen in dit richtsnoer. RISCAuthority is een gratis hulpmiddel. Eenmaal op de bestemmingspagina klikt u op Beveiliging en brandpreventie voor een lijst met begeleidingsdocumenten of zoekt u in het zoekvak.

Er is een groot aantal Europese normen met het voorvoegsel EN of BS EN met betrekking tot de beveiligingsonderwerpen dat hier wordt behandeld, en die allemaal kunnen worden gevonden bij British Standards Institution or the European Committee for Standardisation (CEN). Enkele van de relevante documenten worden vermeld in de volgende sectie.

Confederation of Fire Protection Associations (Europe). Deze website is een nuttige bron voor enkele algemene beveiligingsmaatregelen en standaarden die in heel Europa worden gebruikt.

European Certification Board - Security (ECB-S) schema voor certificering van beveiligingsproducten.

Disclaimer:

Dit document wordt alleen ter informatie aan klanten verstrekt en maakt geen deel uit van enig beleid tussen de klant en RSA. De verstrekte informatie vormt een reeks algemene richtlijnen en mag niet worden opgevat of vertrouwd als specialistisch advies. RSA garandeert niet dat alle gevaren en blootstellingen met betrekking tot het onderwerp van dit document worden gedekt. Daarom aanvaardt RSA geen verantwoordelijkheid jegens enige persoon die vertrouwt op deze Risk Control Guide, noch aanvaardt zij enige aansprakelijkheid voor de juistheid van gegevens die door een andere partij worden verstrekt of de gevolgen van het vertrouwen erop.

This document is provided to customers for information purposes only and does not form any part of any policy which is in place between the customer and RSA. The information set out constitutes a set of general guidelines and should not be construed or relied upon as specialist advice. RSA does not guarantee that all hazards and exposures relating to the subject matter of this document are covered. Therefore RSA accepts no responsibility towards any person relying upon the Risk Control Bulletin nor accepts any liability whatsoever for the accuracy of data supplied by another party or the consequences of reliance upon it.