

Crisis stimuleert gelegenheid

Opvallend is dat bedrijven bewuster lijken te worden van de interne criminaliteit. Traditiegetrouw werden beveiligingsmaatregelen vooral gericht op externe dreigingen, maar nu is binnen bedrijven een verschuiving te zien van repressief naar proactief optreden als het gaat om de aanpak van interne criminaliteit. Juist door de economische crisis is de schade van interne fraude extra voelbaar. Bedrijven zijn hierdoor eerder bereid te investeren in oplossingen voor de langere termijn, zoals het screenen van personeel en de inzet van een Quick Security Review (risicoanalyse en advisering). Ook de krappere arbeidsmarkt en de tijd die bedrijven tegenwoordig hebben bij het aannemen van personeel, maakt dat de P&O-afdelingen zorgvuldiger te werk gaan. Kandidaten worden tegenwoordig vaker onderworpen aan een integriteitonderzoek, dat een betrouwbaar beeld geeft van de integriteit van de kandidaat.

Vormen van criminaliteit Interne criminaliteit wordt volgens het MKB gezien als diefstal van geld of goederen door het eigen personeel. Echter, interne criminaliteit gaat veel verder dan dat. Vormen van onterecht ziekteverzuim en schending van het concurrentiebeding zouden ook als een vorm van interne criminaliteit gezien moeten worden.

Analyse van rechercheonderzoeken, uitgevoerd in 2009 door Trigion RCT, laat zien dat in 86 procent van de criminele incidenten de dader een interne medewerker is. Het merendeel van de criminaliteit komt daarmee uit een hoek waar men het juist niet verwacht. Onderzoek van het MKB uit 2008 bevestigt dit. Interne criminaliteit blijkt veelvuldig voor te komen. In totaal is 5 procent van alle bedrijven in Nederland in aanraking gekomen met interne criminaliteit.

Wanneer we kijken naar de relatie tussen het type dienstverband en daders van interne criminaliteit, valt op dat het overgrote deel van de daders (85

De economische recessie blijkt in 2009 invloed te hebben gehad op de vormen van fraude waardoor bedrijven worden getroffen. Dit constateert de afdeling Recherche, Consultancy & Training (RCT) van Trigion. Daar waar in voorgaande jaren een toename was van witteboordencriminaliteit, is nu juist weer een stijging van 'opportunistische' interne fraude te zien.

procent) personeel betreft met een fulltime aanstelling.

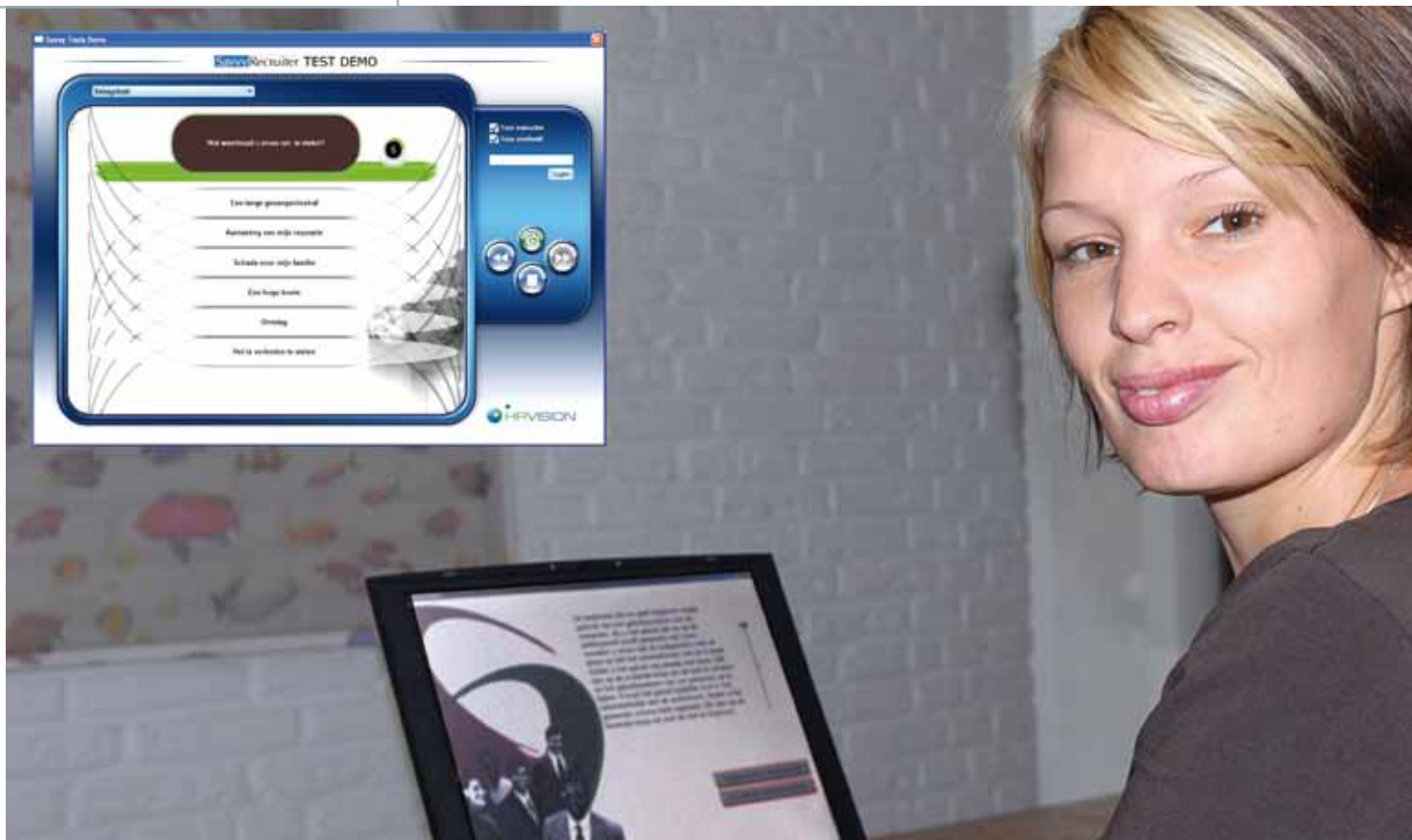
Opportunistisch Opvallend is de groei van de opportunistische fraudegevallen: de graai uit de kas of het ontvreemden van elektronische middelen. Daders die de gelegenheid zien en de kans grijpen zijn vaak slecht voorbereid en vallen als eerste door de mand. Zij nemen, bewust of onbewust, het risico en zien de kans doordat de interne beveiligingsprocedures niet sluitend zijn. Deze dadergroep bestaat vaak uit lager geschoold personeel met financiële problemen en/of loonbeslagen. Wellicht nog opmerkelijker is dat in een derde van de onderzochte incidenten de dader een personeelslid was met een leidinggevende functie. Criminaliteit gepleegd door personeel met een hogere functie kan worden gezien als een vorm van witteboordencriminaliteit (Sutherland, 1940). Het beroep of de positie van een witteboordencrimineel in het bedrijfsleven brengt sociale status en daardoor macht en vertrouwen met zich mee. Witteboordencriminaliteit wordt om deze reden ook wel gezien als 'a certain violation of trust'. De schade gaat namelijk verder dan financieel verlies; het is juist de emotionele schade die erin hakt. Denk hierbij aan het vertrouwen tussen collega's onderling en een verminderd gevoel van veiligheid op de werkplek.

Maatregel De sectoren Horeca en Detailhandel scoren het hoogste als het gaat om diefstal van geld of goederen door eigen personeel (8 procent). Opvallend is dat supermarkten voor 30 procent te maken hebben gehad met interne criminaliteit. Dit is een aanzienlijk

hogere percentage dan het gemiddelde van 8 procent in de gehele detailhandelsector. In de bouwsector blijkt 5 procent van de bedrijven in 2008 te maken hebben gehad met interne criminaliteit. De meest toegepaste maatregel tegen interne criminaliteit blijkt het controleren van referenties bij de aanname van nieuw personeel (MKB, 2008). Opvallend is dat slechts vier op de tien bedrijven aangifte doet bij interne criminaliteit. Dit houdt in dat zes op de tien veroorzakers van interne criminaliteit gewoon een verklaring omtrent het gedrag kunnen overleggen. Juist om deze reden is het aan te bevelen om het personeel te (laten) screenen. Zo'n screening bestaat uit een achtergrondonderzoek aangevuld met een integriteit- en persoonlijkheidsonderzoek. Het achtergrondonderzoek kan worden opgedeeld in het raadplegen van het kadaster, insolventiebronnen en een kredietinformatiebureau. Daarnaast heeft Trigion RCT een samenwerkingsverband met de Informatie Beheer Groep voor het verifiëren van diploma en opleidingsgegevens. Op deze wijze worden diplomagegegevens snel en accuraat gecontroleerd.

Controle vragen Een volgende stap van de screening is een integriteit- en persoonlijkheidsonderzoek. In het integriteitonderzoek wordt de kandidaat getest op een zestal onderwerpen te weten: diefstal, eerlijkheid, omkoping, loyaliteit en drugs- en alcoholgebruik. Het integriteitonderzoek corrigeert voor sociaal wenselijke antwoorden door een meting te doen van de gemiddelde responstijd van de kandidaat. Vragen met een afwijking op de gemiddelde responstijd worden door middel van

dsfraude



controlevragen nogmaals aan de kandidaat gesteld. Op deze manier levert de test een eindrapport op met antwoorden die niet, ofwel in mindere mate integer zijn, dan wel met tegenstrijdige antwoorden.

Aansluitend volgt een persoonlijkheidsonderzoek. Uit onderzoek blijkt dat de combinatie van een persoonlijkheids- en integriteitsonderzoek een veel betrouwbaarder beeld geeft dan enkel een persoonlijkheids- of integriteitsonderzoek. Voorbeeld hiervan is dat wanneer een kandidaat risicovol scoort op het gebruik van overmatig alcohol (op het werk) en ook laag scoort op de schaal van gematigdheid in het persoonlijkheidsonderzoek, beide resultaten elkaar versterken. De resultaten van beide testen worden in een aansluitend interview besproken. Hierdoor worden interpretatieverschillen tot een minimum beperkt en wordt een compleet beeld van de kandidaat verkregen, betreffende zijn of haar integriteit.

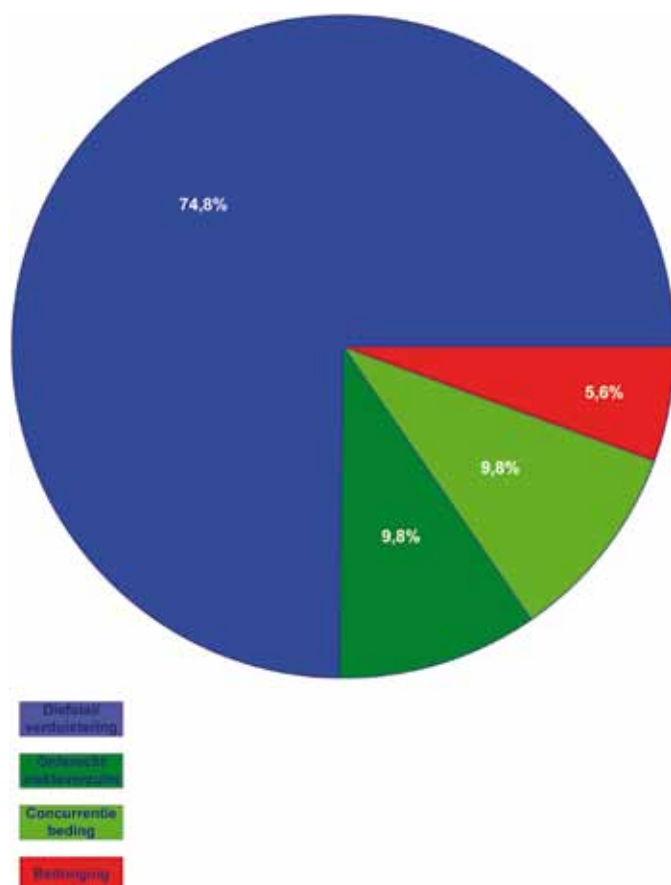
Balans Bij onderzoeken door consultants van Trigion RCT is duidelijk geworden dat er bij veel bedrijven geen goede balans is tussen veiligheidsgevoel en veiligheid. Daar waar een bedrijf scherpe maatregelen neemt, is vaak het bewustzijn laag en hebben de beveiligingsmaatregelen niet het gewenste effect. Daarnaast kan het gevoel van veiligheid aanzienlijke invloed hebben op het wel en wee van mensen. Een gevoel van onveiligheid kan resulteren in onder andere angst, stress en onrust. Wanneer dit wordt vertaald naar bedrijven of organisaties, kan een onveilig gevoel resulteren in improductiviteit, onrust onder werknemers, langdurige ziekte en daardoor indirecte schade aan het bedrijf of de organisatie. Veiligheid en beveiliging zouden alleen daarom al hoog in het vaandel moeten staan bij directeuren en managers. Een gevoel van veiligheid kan men beïnvloeden door het nemen dan wel verbeteren van maatregelen rondom veiligheid en beveiliging. Deze maatre-

gelen dienen bij mensen tot de verbeelding te spreken zodat het veiligheidsgevoel wordt bevorderd. Feitelijke veiligheid gaat echter primair niet uit van het gevoel van mensen, maar redeneert vanuit veiligheidsrisico's (kans x impact) en effectiviteit van getroffen maatregelen (effect op kans en/of impact).

De brug tussen 'het gevoel van veiligheid' en de 'feitelijke veiligheid' dient te worden gevormd door een bijzonder belangrijk onderdeel van veiligheid en beveiliging te weten: 'awareness'. Hiermee wordt bedoeld een voldoende mate van bewustzijn bij een ieder ten aanzien van de risico's die men zelf of de organisatie loopt aangaande veiligheid en beveiliging, het belang en het effect van maatregelen en procedures om veiligheid en beveiliging te borgen en de persoonlijke rol, invloed en verantwoordelijkheid ten aanzien van de veiligheid en beveiliging.

Inefficiënt Bij 80 procent van de ►

Overzicht van aanleidingen van onderzoek door Trigion RCT waarbij een selectie is gemaakt naar interne criminaliteit (N=51).



onderzochte bedrijven bleek dat de beveiliging een onvoldoende volwaardig onderdeel van het beleid en de bedrijfsvoering binnen de organisaties vormde. Hierdoor krijgen risico's en maatregelen rondom veiligheid en beveiliging onvoldoende aandacht. Dit heeft grote invloed op draagvlak en awareness bij medewerkers ten aanzien van de veiligheid en beveiliging. Beveiliging wordt door deze 'houding' vaak voorspelbaar en iets dat slechts bij de in- en uitgang wordt gehandhaafd. Veiligheid en beveiliging zijn binnen veel bedrijven of organisaties duidelijk nog niet iets dat iedereen aangaat. Het vormt dan ook geen (beoordelings-)onderdeel van het functioneren van een werknemer.

Negen van de tien onderzochte bedrijven hebben de beschikking over dure toegangbeheerssystemen. Helaas laat 70 procent van deze bedrijven het vervolgens vaak na om de organisatie hieromtrent voldoende sluitend te maken. Hierdoor is de investering inefficiënt en ineffectief. Toegangssystemen worden nog onvoldoende uitgeput om bijvoorbeeld logistieke processen en veiligheid te borgen.

Tussen toegangbeheerssysteem, compartimentering en bezoekersregeling wordt regelmatig een disbalans geconstateerd. In praktijk zijn bezoekers eenmaal binnen het complex te vrij om te gaan en staan waar men wil. Bij 50 procent van de onderzochte bedrijven was dit het geval. Deels komt dit door onvoldoende compartimentering en deels door het onvoldoende naleven van de bezoekersregeling (bijvoorbeeld het begeleiden van bezoek). Dit heeft gevolgen voor zowel de beveiliging als voor de algemene en individuele veiligheid.

Incidentenregistratie Camera- en alarmsystemen zijn vaak als dure investering binnen bedrijven en organisaties aanwezig. Om de preventieve en repressieve werking van deze systemen te borgen dienen echter ook goede organisatorische maatregelen te worden getroffen. Helaas laat dit in

praktijk nog regelmatig te wensen over. Daarnaast is geconstateerd dat de mogelijkheden van deze systemen regelmatig onvoldoende volledig worden benut.

Incidenten worden over het algemeen wel gemeld en geregistreerd in rapportages. Men laat het echter regelmatig na om een gescheiden incidentenregistratie bij te houden, terwijl die waardevolle informatie kan opleveren om vanuit analyse de veiligheid en beveiliging te verbeteren. Daarnaast kan de bedrijfsvoering worden verbeterd doordat processen meetbaar worden gemaakt.

Als laatste worden incidenten vaak pas als incident betiteld wanneer er schade is of bijna is ontstaan. Wanneer incidenten breder worden getrokken dan voornoemde kan men uit analyses meer informatie halen voor veiligheid, beveiliging en bedrijfsvoering. Een concreet voorbeeld hiervoor is 'De vergeten pas'. Vaak wordt dit niet als incident betiteld, terwijl het er wel een is. Daarnaast kan dit incident, bij regelmatig voorkomen, een enorme impact hebben op de serviceverlening en werkbelasting.

Toolbox Zowel bedrijven, organisaties als individuen zijn in 2009 geconfronteerd met de economische crisis. Mede door de toename van de interne gelegenheidsdieven (opportunistische fraude), stijgt de behoefte aan het scherper inzetten van beveiligingsprocedures aan 'de voorkant', wat inhoudt dat medewerkers op hun integriteit worden getoetst.

Zo'n integriteitonderzoek kan een grote preventieve werking hebben, zeker als alle medewerkers tegelijkertijd de test moeten volgen. Zo gaan medewerkers namelijk nadenken over de zwakke plekken binnen hun organisatie. Bovendien wordt door zo'n collectieve test duidelijk dat het bedrijf integriteit hoog in het vaandel heeft staan. En de integriteit, loyaliteit en betrouwbaarheid die met zo'n test wordt gemeten, geldt natuurlijk ook de omgang met collega's. Maar wellicht het allerbelangrijkste is om het denken over integriteit 'in de genen van het bedrijf' te krijgen. Bedrijven kunnen dit bereiken met behulp van speciaal hiervoor ontwikkelde workshops en toolboxes door zo met regelmaat integriteitdilemma's te behandelen. Het zijn methodes die bijzonder geschikt zijn voor het alert houden van managementteams en het onderling bespreken of zelfs vaststellen wat goed en fout en gewenst en ongewenst is, en waar het bedrijf de grens wil trekken.

De grootste stap die gemaakt kan worden ter verbetering van de effectiviteit van de beveiliging is het investeren in veiligheidsbewustzijn rondom veiligheid en beveiliging. Dit veiligheidsbewustzijn is essentieel voor alle niveaus binnen de organisatie en vormt een rode draad in de risico's en maatregelen rondom veiligheid en beveiliging. Veiligheidsbewustzijn dient dan ook duidelijk op de kaart te worden gezet, helemaal in tijden van economische crisis.

■ Maarten IJzermans

Businessunit manager Trigion Recherche, Consultancy & Training