SIXTAT

Statistiek Marktonderzoek Software

Opzet enquête
financieel-economische criminaliteit
en
computercriminaliteit

30 juli 2009

Prof. dr. D. Sikkel dirk.sikkel@uvt.nl

Schout van Eijklaan 98
2262 XV LEIDSCHENDAM
070-3200031

Opzet enquête financieel-economische criminaliteit en computercriminaliteit

Een onderzoek, uitgevoerd in opdracht van het WODC van het Ministerie van Justitie

Inhoudsopgave

Voorwoord

In dit rapport wordt verslag gedaan van de ontwikkeling van een meetinstrument voor slachtofferschap van computercriminaliteit en financieel-economische criminaliteit. Dit instrument is ontwikkeld in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) van het Ministerie van Justitie. Bestrijding van deze vormen van criminaliteit valt onder het project Veiligheid begint bij Voorkomen, dat weer onderdeel is van Pijler 5 van het beleidsprogramma van het kabinet. Computercriminaliteit en financieel-economische criminaliteit vallen onder het onderdeel *ernstige criminaliteit*. Computercriminaliteit is een type misdrijf dat in opkomst is. De afhankelijkheid van de samenleving van informatie- en communicatietechnologie leidt tot nieuwe vormen waarin men crimineel actief kan zijn. Financieel-economische criminaliteit krijgt door de ontwikkeling van deze technologie bovendien een nieuwe impuls. ICT biedt criminelen derhalve kansen die er zonder de computer en het internet niet waren geweest. De meting van de gevolgen staat echter nog in de kinderschoenen. Op dit moment zijn in een beperkt aantal landen instrumenten ontwikkeld om het slachtofferschap van technologie-gerelateerde criminaliteit te meten.

In dit rapport wordt eerst beschreven hoe computercriminaliteit en financieel-economische criminaliteit worden ingedeeld, welk type misdrijven hieronder vallen. Vervolgens worden de verschillende meetinstrumenten in het buitenland geïnventariseerd. Daarna wordt een opzet beschreven voor een onderzoek zoals dat in Nederland onder burgers en bedrijven kan plaatsvinden. Tevens bevat het rapport de vragenlijsten die bij dit onderzoek kunnen worden gebruikt.

Het onderzoek is begeleid door een begeleidingscommissie die bestond uit de volgende leden: Wouter Stol (voorzitter, Noordelijke Hogeschool Leeuwarden), Hennie Vreugdenhil (Ministerie van Justitie) en Frank Willemsen (WODC). Graag wil ik de leden van de begeleidingscommissie bedanken voor hun constructieve bijdrage aan dit project.

Dirk Sikkel
onderzoeker

Samenvatting

Het project Veiligheid begint bij Voorkomen (VbbV) is opgestart teneinde veiligheid, stabiliteit en respect in de samenleving te bevorderen. Jaarlijks wordt vanuit diverse bronnen onderzocht in welke mate de hoofddoelstellingen van VbbV worden gehaald. Er zijn slachtofferenquêtes onder burgers en bedrijven en een recidivemonitor waaruit relevante kentallen worden gedestilleerd. Voor bepaalde vormen van criminaliteit die expliciet in VbbV worden behandeld, financieel-economische criminaliteit en computercriminaliteit, bestaat op dit moment nog geen meetinstrument. Dit project is bedoeld om een eerste versie van een dergelijk instrument te maken. Deze wordt gebaseerd op de inhoudelijke kennis die reeds in Nederland bestaat, samengevat in Van der Hulst en Neve (2008), en de ervaringen die in het buitenland zijn opgedaan met soortgelijke instrumenten.

De enquêtes, die bedoeld zijn voor zowel burgers als bedrijven, kunnen verschillende doelstellingen hebben, te weten:

- vaststellen aard en omvang: welke delicten komen voor, hoe vaak worden deze gepleegd en wie zijn de slachtoffers?
- inzicht in melding- en aangiftegedrag en reactie: maken slachtoffers melding van delicten, doen ze daar aangifte van bij de politie en wat gebeurt daar mee?
- ramen van de schade: wat is directe en indirecte schade die wordt geleden , wat is de psychologische impact op de slachtoffers en wat is de weerslag daarvan op hun gedrag?
- beschrijven van preventieve maatregelen: welke preventieve maatregelen nemen burgers?

In een later stadium kunnen er mogelijk doelstellingen geschrapt worden; hier wordt ervan uitgegaan dat al deze gebruiksmogelijkheden van de enquêtes van belang zijn. Ze zijn dan ook leidraad geweest bij het opstellen van de vragenlijsten voor burgers en bedrijven.

Cybercrime en financieel-economische criminaliteit komen in vele gedaanten voor. Dit geldt zeker in technische zin. De manieren waarop botnets worden gebruikt, de technieken die worden toegepast bij phishing en het karakter van Trojaanse paarden zijn cruciaal bij de bestrijding van cybercrime, maar zullen de overgrote meerderheid van de gebruikers ontgaan. De vragenlijsten, met name voor burgers, hebben daarom vooral betrekking op wat de slachtoffers ervaren, in plaats van wat er technisch aan de hand is. Daarbij wordt onderscheid gemaakt in drie brede groepen delicten:

- *cybercrime in brede zin*: hierbij speelt de computer vaak een rol, maar strikt nodig is dat niet. Voorbeelden zijn identiteitsfraude, voorschotfraude en marktmanipulatie;
- *cybercrime in enge zin*: hierbij is de computer essentieel. Voorbeelden zijn hacken, verspreiden van computervirussen en omkopen van hooggekwalificeerd ICT-personeel;
- *financieel-economische criminaliteit*: dit is een verzamelnaam voor een groot aantal vormen van misleiding met het doel om anderen geld afhandig te maken. Voorbeelden zijn spooknota's, verduistering en corruptie.

Het aantal landen waarin deze en dergelijke onderwerpen middels een slachtofferenquête zijn onderzocht is beperkt. Het zijn vooral Engelstalige landen. Vaak gaat het dan om enquêtes met een beperkte vragenlijst, die onderdeel uitmaken van een groter geheel, bijvoorbeeld een arbeidskrachtentelling. Een in termen van aantal onderwerpen grootschalige enquête onder burgers bestaat nog niet. Met name voor bedrijven zijn er ook commerciële enquêtes onder IT-specialisten

met een beperkt aantal respondenten. In de Verenigde Staten is er wel een goed voorbeeld van een grootschalige enquête onder bedrijven op het gebied van cybercrime.

De kwaliteit van de enquêtes in het buitenland valt alleen in de Verenigde Staten enigszins vast te stellen, omdat daar goede, en ook goed gerapporteerde cognitieve testonderzoeken voorafgaand aan de enquêtes zijn gehouden. Met name voor de bedrijfsenquête is dat een reden om veel vragen uit de Verenigde Staten over te nemen. Voor de slachtofferenquête onder burgers moest de vragenlijst geheel nieuw worden ontworpen, met daarin slechts een paar vragen die ook in de Amerikaanse enquête naar identiteitsfraude voorkomen.

Voor de wijze van afnemen van een enquête zijn in beginsel vier mogelijkheden:

- face to face (met een interviewer)
- schriftelijk
- telefonisch
- via het internet

Het onderwerp, en de daaruit voortvloeiende vragenlijst is te complex om telefonisch of schriftelijk te bevragen. Face to face is uit oogpunt van kwaliteit te prefereren, maar het is onwaarschijnlijk dat de daardoor behaalde kwaliteitswinst opweegt tegen de veel hogere kosten vergeleken met ondervraging via het internet.

Na een aantal inleidende vragen vervolgt de vragenlijst voor burgers met een screeningslijst van 39 delicten waarvan men slachtoffer kan zijn, uiteenlopend van een traag werkende computer tot diefstal van laptops. Voor elk ondervonden delict worden toepasselijke vervolgvragen gesteld op het gebied van aangiftegedrag, reactie van politie, daderkennis, schade en (gebrek aan) preventie. De vragenlijst voor bedrijven heeft als onderwerpen op het gebied van cybercrime:

- virussen
- denial of service
- elektronisch vandalisme/sabotage
- verduistering
- fraude
- diefstal van intellectueel eigendom
- diefstal van persoonlijke of financiële informatie
- overige veiligheidsincidenten

en met betrekking tot financieel-economische criminaliteit komen onder meer cv-fraude, omkoping, infiltratie, spionage, afpersing, spooknota's en niet betalen of betalen met valse middelen aan de orde.

Summary

The project Safety starts with Prevention is initiated with the aim to improve safety, stability and respect in society. This project is fed with information from different sources, like victimization surveys amongst citizens and businesses and a recidivism monitor amongst juveniles. Presently, there is not yet a measurement tool for two emerging types of crime: financial economic crime and cybercrime. The current project entails the development of a first version of such an instrument. The development process is based on the existing substantive knowledge in the Netherlands, as is described in Van der Hulst and Neve (2008), and recent experiences in other countries.

The surveys, which are aimed at both citizens and businesses, can have different objectives, such as

- to determine size and nature: which groups are at risk, which forms of crime occur how often?
- to record notification and reaction: do victims contact the police and how does the police react?
- to assess damage: how much money is involved, what is the psychological impact on the victims and what are the consequences for their behaviour?
- to describe preventive behaviour: what preventive measures do citizens take?

At a later stage, objectives may possibly be cancelled; here it is assumed that all possible usages which are mentioned here are of interest. As a consequence they are the guidelines for the construction of the questionnaires for citizens and businesses.

Cybercrime and financial economic crime are products par excellence by intelligent creative criminal minds, and come therefore in many appearances. This is especially true in the technical sense. The way botnets are used, the techniques which are applied for phishing, the character of Trojan horses are crucial when fighting cybercrime, but will escape the large majority of computer users. The questionnaires, especially for citizens, are based on what victims experience instead of the technical diagnosis. Three groups of crimes are distinguished.

- *cybercrime in the broad sense*: here the computer often plays a role, but this is not strictly necessary. Examples are identity fraud, advance fraud and market manipulation;
- *cybercrime in the narrow sense*: here the computer is essential. Examples are hacking, spreading of computer viruses and bribing of highly qualified ICT staff;
- *financial economic crime*: this is a generic term for a large number of types of deception with the aim of taking money from others. Examples are phantom invoices, embezzlement and corruption.

The number of countries in which these and similar subjects are investigated using a victimization survey is limited. They are mainly English speaking countries. Often, it concerns surveys with a limited questionnaire, which are part of a larger survey, e.g. a labour force survey. A large scale survey (in terms of number of topics) amongst citizens does not yet exist. Particularly for businesses there are commercial surveys amongst IT-specialists with a limited number of respondents. In the US there is, however, a good example of a large cybercrime survey amongst businesses.

The quality of the surveys outside the Netherlands can only be assessed in the US. Only there were good, and well reported, cognitive test procedures in the construction stage of the surveys.

Especially for the survey for businesses this was a reason to use similar questions as in the US. For the victimization survey amongst citizens the questionnaire had to be developed from scratch, using only a few questions which were part of the American survey of identity fraud.

For the interviewing mode, there are basically four possibilities:

- face to face (with an interviewer)
- by mail
- by phone
- through the internet

The subject of financial economic crime and cybercrime, and the resulting questionnaire, is too complex to ask questions without visual feedback or guidance with respect to routing. This rules out a telephone or mail survey. Face to face interviewing is to be preferred from the point of view of data quality, but it seems unlikely that the gain in quality outweighs the much higher costs compared to internet interviewing.

After a number of introductory questions, the questionnaire for citizens continues with a screening list of 39 types of crime, varying from a slowly operating PC to the theft of laptop computers. For each experienced crime, applicable follow up questions are asked on the subject of notification behaviour, reaction by the police, familiarity with the offender, damage and (lack of) prevention. The questionnaire for businesses contains the following subjects with respect to cybercrime:

- viruses
- denial of service
- electronic vandalism/sabotage
- embezzlement
- fraud
- theft of intellectual property
- theft of personal or financial information
- other computer safety incidents

With respect to financial economic crime, amongst others the following topics are in the questionnaire: cv-fraud, corruption, infiltration, espionage, extortion, phantom invoices and paying with counterfeit money.

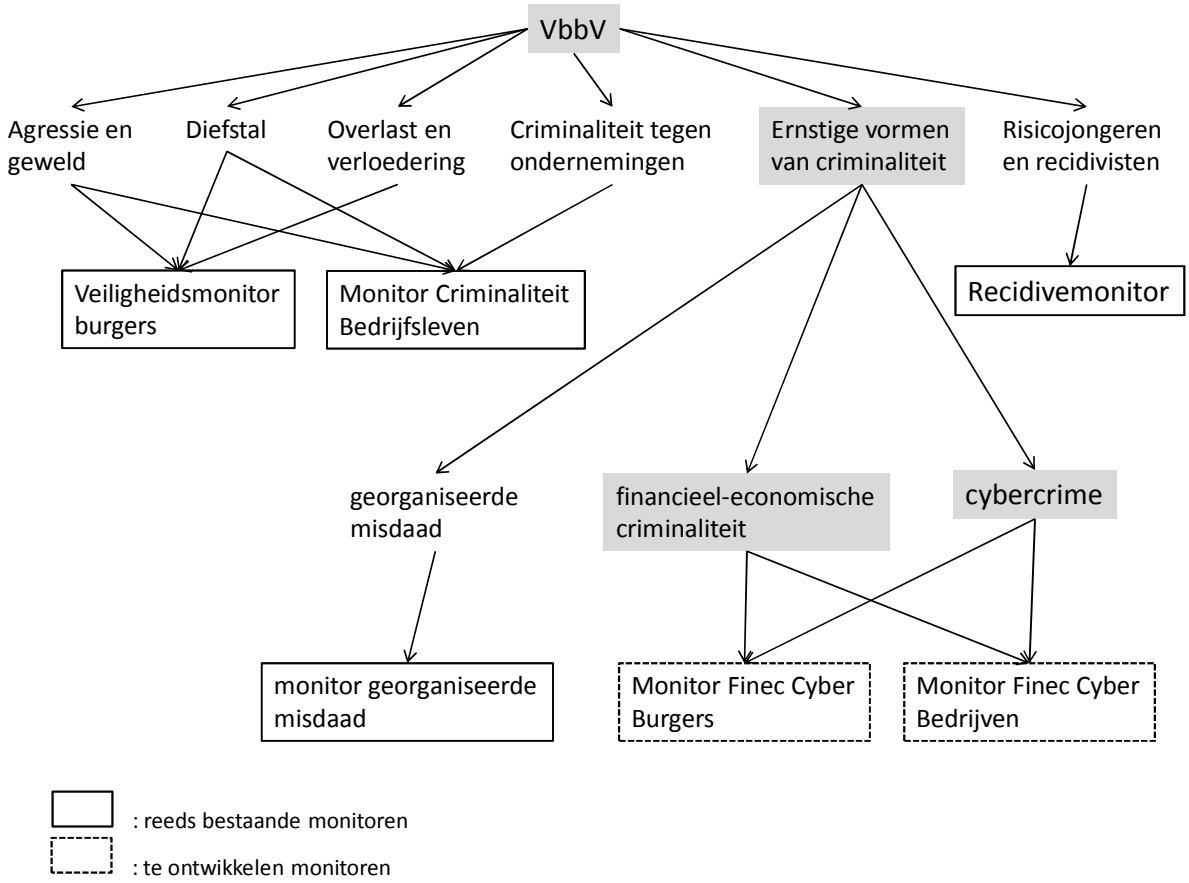
1. Inleiding

Veiligheid, stabiliteit en respect in de samenleving is een belangrijk beleidsdoel van het huidige kabinet. In het kader hiervan is het project Veiligheid begint bij Voorkomen (VbbV) geformuleerd. Dit is een breed project, waarin zes thema's aan de orde komen:

- de aanpak van agressie en geweld
- de aanpak van diefstal
- de aanpak van criminaliteit tegen ondernemingen
- de aanpak van overlast en verloedering
- de persoonsgerichte aanpak van risicojongeren en recidivisten
- de bestrijding van ernstige vormen van criminaliteit.

De hoofddoelstelling van VbbV is een reductie van criminaliteit (gewelds- en vermogensdelicten), fysieke verloedering en ernstige sociale overlast met 25% in 2010 ten opzichte van 2002. Voor het monitoren van de doelstelling van VbbV wordt de ontwikkeling van de door burgers ondervonden gewelds- en vermogensdelicten gevolgd. Ten behoeve van het genereren van de daarvoor benodigde informatie wordt gebruik gemaakt van de Veiligheidsmonitor Rijk en de Monitor Criminaliteit Bedrijfsleven. Beide monitoren meten slachtofferschap van respectievelijk burgers en bedrijven van relatief veelvoorkomende delicten zoals diefstal, inbraak, vernieling en geweld. Daarnaast wordt er aandacht besteed aan melding- en aangiftegedrag en preventieve maatregelen van burgers en bedrijven. In de Veiligheidsmonitor Rijk worden bovendien vragen gesteld over overlast en verloedering. Ook wordt de Recidivemonitor van het WODC gebruikt om periodiek cijfers aan te leveren over de recidive van verschillende doelgroepen. Echter, delicten die vallen in de eerdergenoemde categorie "ernstige vormen van criminaliteit", worden niet of impliciet vastgelegd, terwijl de behoefte om meer te weten over de aard en omvang vanuit VbbV wel aanwezig is.

Ernstige criminaliteit bestaat uit drie deelgebieden, zoals ook aangegeven in onderstaande figuur: georganiseerde misdaad, financieel-economische criminaliteit en cybercrime.



Bron: Willemsen (2008)

Uit de figuur blijkt dat voor de meeste onderdelen een monitor bestaat waarmee de VbbV-kentallen gemeten kunnen worden. Voor financieel-economische criminaliteit en cybercrime is dit nog niet het geval. Het zijn in belangrijke mate misdaadgebieden in opkomst, waarvoor in Nederland nog geen instrument bestaat waarmee de gevolgen voor de samenleving worden gemeten. In het buitenland is de ervaring weliswaar niet geheel afwezig, maar wel zeer beperkt.

Het hier beschreven project heeft ten doel om een meetinstrument op het gebied van financieel-economische criminaliteit en cybercrime te ontwikkelen. Het bestaat uit de volgende onderdelen:

- Afbakening. Allereerst wordt expliciet gemaakt welke doelstellingen de monitor zou kunnen dienen. Dit gebeurt in hoofdstuk 2. Daarna is de vraag wat onder cybercrime en financieel-economische criminaliteit wordt verstaan: welke delicten vallen hieronder en hoe verhouden ze zich tot elkaar? Dit gebeurt in hoofdstuk 3.
- Inventarisatie van binnen- en buitenlandse meetinstrumenten om slachtofferschap van financieel-economische delicten en cybercrime vast te leggen. Deze inventarisatie, binnen voornamelijk Engelstalige landen, staat in hoofdstuk 4.
- Inventarisatie van prevalenties en incidenties van delicten die onder financieel-economische criminaliteit en cybercrime vallen. Deze worden eveneens in hoofdstuk 4 gepresenteerd in samenhang met de meetinstrumenten waarmee de schattingen tot stand zijn gekomen.
- Evaluatie van de kwaliteit van de meetinstrumenten. Hierop wordt ingegaan in hoofdstuk 5.

- Het maken van een onderzoeksopzet voor de monitor onder burgers en bedrijven, met name wijze van steekproeftrekking en dataverzameling. Dit wordt beschreven in hoofdstuk 6.
- Ontwikkeling van vragenlijsten voor burgers en bedrijven. De resultaten hiervan zijn als bijlagen bijgevoegd.

In termen van doelstellingen van de enquêtes is er strikt genomen geen sprake van afbakening, want er worden geen beperkende keuzes gemaakt, maar er wordt toegewerkt naar een meetinstrument met maximale reikwijdte. Later kan men desgewenst besluiten doelstellingen te laten vallen en de corresponderende vragen te schrappen.

2. Mogelijke doelstellingen van de enquête

In dit rapport wordt een voorstel voor een tweetal enquêtes gedaan waarin slachtofferschap van financieel-economische criminaliteit en computercriminaliteit wordt gemeten onder burgers, bedrijven en instellingen. Beide enquêtes kunnen voor verschillende doeleinden worden gebruikt. Vanuit VbbV is het van belang dat er jaarlijks cijfers beschikbaar zijn waarmee bepaald kan worden of de hoofddoelstellingen van dit programma zijn behaald (of behaald kunnen worden in de loop der tijd). Meer algemeen gesproken is inzicht in de aard en omvang van criminaliteit en de ontwikkeling ervan door de tijd, belangrijk om tot juiste keuzes te komen in de bestrijding hiervan. Kennis over delicttypen, kenmerken van slachtoffers en van mogelijke daders, melding- en aangiftegedrag van slachtoffers en de reactie hierop van de politie zijn belangrijke elementen. Criminaliteitsbestrijding kost geld; het vaststellen van de materiële en immateriële schade die het gevolg is van criminaliteit kan een rationale bieden om prioriteiten te stellen in de aanpak van criminaliteit. Daarom is het meten van verschillende vormen van schade een tweede mogelijke doelstelling van de enquête. De derde brede doelstelling is voorlichting en preventie, het voorkomen van slachtofferschap. Kennis over het feitelijke preventiegedrag van burgers en bedrijven kan bijvoorbeeld helpen bij het vormgeven van voorlichtingscampagnes op dit terrein. Daarnaast is het zinnig om vast te stellen of suboptimaal preventiegedrag de oorzaak is van slachtofferschappen, met als alternatieve mogelijkheid dat slachtoffers in rede niet hadden kunnen verhinderen wat hen is overkomen. Deze doelstellingen leiden tot de volgende globale indeling van vragen:

1. ***Aard en omvang***
   a. ***delictvormen***: welke delicten komen voor, hoe vaak worden deze gepleegd en wie (bedrijven & burgers) zijn de slachtoffers?
   b. ***risicokenmerken***: welke kenmerken hangen samen met slachtofferschap.
2. **Melding- en aangiftegedrag en reactie:** van welke delicten wordt melding of aangifte gedaan en hoe vaak. Hoe reageren de politie en eventueel andere belanghebbenden (bijvoorbeeld banken) op een incident?
3. ***Schade***
   a. ***economische schade:*** in termen van geld en downtime;
   b. ***psychologische schade:*** in termen van leed;
   c. ***gedragschade:*** welke is de weerslag van beide vormen van schade in het gedrag van burgers en bedrijven in termen van preventie of vermijding, en wat zijn daarvan de kosten?

4. ***Preventieve maatregelen:*** wat is in het algemeen het preventiegedrag bij burgers en bedrijven (ook bij niet-slachtoffers)?

Verderop in dit rapport wordt een veelheid enquêtegegevens en andere data besproken. Daarbij zal steeds deze classificatie worden aangehouden.

3. Vormen van criminaliteit

In een zeer uitvoerige literatuurstudie hebben Van der Hulst en Neve (2008) een overzicht gemaakt van de verschillende soorten criminaliteit waarbij ICT een rol speelt. Het rapport heeft vooral ten doel om de daders van cybercrime te karakteriseren. Zij delen de criminaliteit in in twee grote terreinen.

1. *cybercrime in bredere zin*. Dit zijn vormen van criminaliteit die ook zonder tussenkomst van ICT gepleegd kunnen worden, maar die door het gebruik van ICT nieuwe gedaanten hebben aangenomen. Dit wordt door Van der Hulst en Neve cybercriminaliteit genoemd.

2. *cybercrime in engere zin*. Deze vormen van criminaliteit zijn gericht op computers en kunnen niet bestaan zonder computers. Van der Hulst en Neve noemen dit computercriminaliteit.

Bij de opzet van de enquêtes conformeren wij ons aan deze indeling. Er is echter wel een derde groot terrein van criminaliteit, namelijk de vormen van financieel-economische criminaliteit waarin ICT geen of slechts een ondergeschikte rol speelt. Over de definitie van dit soort criminaliteit is weinig overeenstemming, zoals verwoord in McCarthy en Cohen (2008):

> "There is no widely accepted definition of economic crime, and it is impossible to enumerate briefly the various definitions, theories, and offenses included in this category."

In het kader van het project VbbV is gekozen om onder financieel-economische criminaliteit te verstaan corruptie, het witwassen van geld en fraude (Willemsen, 2008). Corruptie, het betalen van personen die daar geen recht op hebben om goederen of diensten te verkrijgen en witwassen, het aan het zicht onttrekken van criminele winsten en ze vervolgens schijnbaar legaal weer te herinvesteren, staan vrijwel los van cybercrime. Over de definitie van fraude bestaat in de literatuur geen overeenstemming. Het woord is afkomstig van het Latijnse *fraus*. Het woordenboek (Mallinckrodt, 1980) geeft de betekenissen: bedrog, list, ontduiking, bedrieglijkheid, dwaling, dwaalspoor, schade, misdaad. Podgor (1999) geeft een aantal citaten waaruit de moeilijkheid blijkt om het begrip te definiëren. Twee voorbeelden:

> "I shall not attempt to construct a definition which will meet every case which might be suggested, but there is little danger in saying that whenever the words "fraud" or "intent to defraud" or "fraudulently" occur in the definition of a crime two elements at least are essential to the commission of the crime: namely, first, deceit or an intention to deceive or in some cases

> mere secrecy; and secondly, either actual injury or possible injury or an intent to expose some person either to actual injury or to a risk of possible injury by means of that deceit or secrecy."
>
> James Fitzjames Stephen, *History of Criminal Law*

> "In much of the judicial discussion of fraud it is assumed as self-evident that the reader knows what fraud is, so why bother to define it? However, when in the actual decision of a case it becomes necessary to frame a definition of fraud the courts encounter difficulty. Sometimes they meet it by saying that fraud is so various in its manifestations that it would be fruitless to attempt a definition, and that each case must be determined as it arises according to its own circumstances. Following the same tack, some text-writers have also refused to attempt the formulation of a definition. Others, of more venturesome disposition, have constructed definitions, although there is not complete agreement among them."
>
> Milton D. Green, Fraud, *Undue Influence and Mental Incompetency*

Ten aanzien van het verwante begrip "oplichting" werd ook in een rapport van CentERdata (Oudejans en Vis, 2008) geconstateerd: "Een vast categoriesysteem voor vormen van oplichting wordt in de literatuur niet aangetroffen. Een reden hiervoor is dat de modus operandi steeds wijzigt". In het CentERdata onderzoek werd dit probleem opgelost door de respondenten een aantal brede terreinen voor te leggen (producten, diensten, geld, de kans op winst of rendement of anders) en verder open vragen te stellen. Levi e.a. (2007) kiezen in een studie naar de economische impact van fraude in het Verenigd Koninkrijk een andere pragmatische oplossing.

> "The issue of defining which activities constitute fraud is the subject of considerable debate. Resolving this debate is outside the remit of the present research. To avoid confusion, for the purposes of this study, fraud is defined as follows:
> *Fraud is the obtaining of financial advantage or causing of loss by implicit or explicit deception; it is the mechanism through which the fraudster gains an unlawful advantage or causes unlawful loss."*

Dezelfde pragmatische aanpak kiezen we hier, en beschouwen fraude als het opzettelijk iemand misleiden om zo geld, goederen of diensten te verkrijgen waar men geen recht op heeft. De lijst van mogelijke vormen van fraude is schier onuitputtelijk. Er zijn vormen van fraude waarin cybercrime een hoofdrol speelt; dit is bijvoorbeeld het geval bij voorschotfraude, waarin slachtoffers via e-mail wordt gevraagd om geld over te maken voor een product of dienst die nooit wordt geleverd. Dit soort fraude is onder verschillende noemers ook gerapporteerd in Oudejans en Vis (2008). Een voorbeeld waarbij het internet partieel een rol speelt is cv-fraude. Zo worden op het internet valse diploma's aangeboden die een rol kunnen spelen in cv-fraude.

In de tabellen 1a, 1b en 1c wordt een overzicht gegeven van de verschillende vormen van criminaliteit en de wijze waarop burgers en bedrijven hier slachtoffer van kunnen worden. Bij de onderdelen cybercrime in bredere en engere zin hebben we ons weer geconformeerd aan de beschrijving van Van der Hulst en Neve (2008). Het is in het kader van de instrumentontwikkeling belangrijker om de uitingsvorm van delicten in de ogen van slachtoffers (burger of bedrijf) te beschrijven dan de delicten in juridische zin juist te definiëren.

Tabel 1a. Relatie cybercrime in bredere zin en slachtofferschap (classificatie gebaseerd op Van der Hulst en Neve (2008))

Cybercriminaliteit	Slachtoffers en uitingsvormen
Legale communicatie en afscherming	
Radicalisering en extremisme	Personen: beïnvloeding en onder druk zetten (van gezinsleden) via websites en chatrooms, werving van medestanders en -strijders
Terrorisme, ideologisch gemotiveerde misdaad	Bedrijven, instellingen en personen: bedreiging , afpersing, je bedreigd voelen (subjectief)
Afscherming (onzichtbaar voor anderen communiceren)	Niet geschikt voor slachtofferenquête
Illegale handel	
Drugs	Personen (gezinsleden): aanbieden of kopen van drugs(grondstoffen)
Geneesmiddelen	Personen (gezinsleden): niet werkzame of schadelijke geneesmiddelen gebruiken aanbieden
Vuurwapens en explosieven	Niet geschikt voor slachtofferenquête
Kinderporno	Personen: werving van kinderen, toevallige confrontatie met kinderporno
Heling	Personen en bedrijven: eigen spullen terugvinden op het internet
Mensenhandel, -smokkel	Niet geschikt voor slachtofferenquête
Software piraterij	Bedrijven: diefstal van muziek, dvd's, software met auteursrechten
Illegale kansspelen	Personen: gokverslaving, opgelicht worden
Financieel-economische criminaliteit	
Internetfraude	Verzamelnaam voor voorschotfraude en identiteitsfraude
Voorschotfraude	Personen en bedrijven: voorschotten betalen voor producten of diensten die men niet krijgt
Identiteitsfraude	Personen en bedrijven: je voordoen als een ander en dan kopen op andermans kosten, plunderen van rekeningen*
Marktmanipulatie (verspreiden geruchten)	Bedrijven, personen die aandeelhouder zijn zien hun aandelen kelderen Bedrijven worden aangetast in hun goede naam of gepercipieerde kredietwaardigheid
Afpersing, chantage	Personen (bijvoorbeeld dreiging opnames seks op internet zetten), bedrijven (bijvoorbeeld dreiging dDoS)
Witwassen	Bedrijven: ongewild met uit criminaliteit verkregen gelden worden betaald
Illegale communicatie	
Cyberstalking	Personen: boodschappen sturen, roddelen op sociale sites, mensen publiek te schande maken

Cybercriminaliteit	Slachtoffers en uitingsvormen
Discriminatie	Personen, mogelijk ook kleine bedrijven: bedreiging, intimidatie, laster, haat zaaien
Grooming	Personen: benaderen van minderjarige kinderen door volwassenen die zich als kinderen voordoen
Spionage	Bedrijven: bedrijfsspionage

Wanneer personen het slachtoffer zijn, kan het ook om gezinsleden gaan van degenen die als doelgroep voor de criminelen fungeren. Zo kunnen de ouders zich ook het slachtoffer voelen wanneer hun kinderen via het internet aan drugs kunnen komen. Voor al deze misdrijven geldt dat de computer strikt genomen niet noodzakelijk is om ze te plegen. In de slachtofferenquête zal expliciet gevraagd moeten worden of en hoe de computer (of eventuele andere elektronica) hier een rol speelde. Voor identiteitsfraude, zoals gedefinieerd in tabel 1a, bestaat een veelheid aan ICT-technieken:

- spam om via trucs aan persoonsgegevens te komen, phishing;
- bekijken sociale netwerk sites;
- malware, omleiden naar nepwebsite, pharming;
- skimmen, het lezen van bankpassen en pincodes terwijl er gepind wordt,

maar uiteraard is ook ‘eenvoudige’ diefstal van een paspoort, rijbewijs, mobiele telefoon of laptop een stap op weg naar identiteitsfraude.

Tabel 1b. Relatie cybercrime in engere zin en slachtofferschap (klassificatie gebaseerd op Van der Hulst en Neve (2008))

Computercriminaliteit	Slachtoffers en uitingsvormen
Ongeautoriseerde toegang	
Hacking	personen, bedrijven: computer werkt traag of niet; bedrijven: gevoelige informatie op straat
Botnets	personen, bedrijven: computer werkt traag of niet
ICT-storing door gegevensverkeer	
dDoS (Denial of Service)	bedrijven: door spam raakt systeem overbelast waardoor communicatie met relaties onmogelijk wordt
Spam	personen, bedrijven: irritatie vanwege ongewenste e-mails en vol raken mailbox
ICT-storing door manipulatie van data en systeem	
Malware in systemen (virussen, wormen, Trojaanse paarden)	personen, bedrijven: computer werkt anders of niet
Defacing	bedrijven en hun klanten: veranderen website die daardoor lelijk wordt of onbedoelde functionaliteit krijgt, omleiden bezoekers
Hacktivism	bedrijven: hacking, inbreken in systemen uit ideologische motieven

Computercriminaliteit	Slachtoffers en uitingsvormen
Cyberterrorisme	bedrijven en overheid: lam leggen van vitale infrastructuren (politiek gemotiveerd)
ICT Dienstverleners en high-tech crime	
Corruptie	bedrijven
Infiltratie	bedrijven
Inhuur expertise door criminelen	bedrijven

Hacking en het installeren van software voor botnets is een vorm van criminaliteit waarbij de kans bestaat dat de eigenaar van de geïnfecteerde computer het nooit zal opmerken; een slachtofferenquête zal daardoor altijd een onderschatting van deze vorm van cybercrime geven. Bij corruptie en infiltratie gaat het in tabel 1b specifiek om misdrijven van deskundigen op ICT-gebied. In andere gevallen valt dit onder financieel-economische misdrijven.

In tabel 1c worden alle vormen van financieel-economische criminaliteit beschreven waarin de computer hoogstens een beperkte instrumentele rol speelt, maar niet essentieel is. Het zijn alle vormen van fraude waar het slachtoffer op basis van misleiding of illegale handelingen geld afhandig wordt gemaakt.

Tabel 1c. Relatie financieel-economische criminaliteit en slachtofferschap

Niet computer-gerelateerde financieel-economische fraude	Potentiële slachtoffers
Identiteitsfraude door diefstal/vervalsing documenten en creditcards	personen, bedrijven
Verzekeringsfraude	(verzekerings)bedrijven
Faillissementsfraude (ten onrechte winsten, goederen buiten faillissement houden)	bedrijven
Piramidespel	personen, bedrijven
Spooknota's	bedrijven, personen
Kredietfraude (lening afsluiten terwijl onderpand minder waard is dan beweerd)	bedrijven
Jaarrekeningfraude	bedrijven, personen (aandeelhouders)
Bouwfraude	bedrijven, personen
Verduistering	bedrijven
Taxatiefraude (bewust objecten verkeerd taxeren)	bedrijven, personen
Acquisitiefraude (met name advertenties die dan niet worden geplaatst als afgesproken)	bedrijven
Diplomafraude, cv-fraude	bedrijven
Corruptie	personen, bedrijven

De indeling is gebaseerd op de inhoud van een aantal enquêtes die in de volgende hoofdstukken worden besproken, de inhoud van diverse websites met betrekking tot fraude (bijvoorbeeld www.fraud.org, www.fbi.gov/majcases/fraud/fraudschemes.htm,

http://www.lectlaw.com/def/f079.htm, e.d.) en Levi e.a. (2007). Uit dit soort bronnen blijkt een zeer grote variëteit aan benamingen, maar ook verschillen in gedetailleerdheid waarmee de fraudevormen worden beschreven. Zo kan identiteitsfraude worden onderverdeeld in paspoortfraude, credit card fraude, bankpasfraude etc. Voor piramidespelen geldt iets dergelijks: de algemene vorm is gebaseerd op het werven van nieuwe deelnemers aan een activiteit die een inleg moeten betalen, maar dit kan zich uiten in kettingbrieven, beleggingen, participaties in time-sharing appartementen etc. De lijst in tabel 1c is op een niveau samengesteld dat het aantal vormen enigszins beperkt blijft. Omdat dit project valt onder de noemer “ernstige vormen van criminaliteit” laten we kleine vormen van consumentenfraude, zoals die veelvuldig in Oudejans en Vis (2008) zijn genoemd buiten beschouwing (bijvoorbeeld: “Pizzabezorger die me 50 cent teruggaf wat 2 Euro had moeten zijn”, “Er stond een veel te hoog bedrag op de pomp; is ook van mijn bankrekening afgehouden”). Daarnaast zijn er nog vormen van fraude die er specifiek op gericht zijn om de overheid op te lichten, zoals belastingfraude, uitkeringsfraude, zwart werken, witwassen en milieufraude. Deze vormen staan bekend onder de naam “verticale fraude”. Ze blijven buiten beschouwing omdat ze niet passen in een slachtofferenquête.

4. Statistische gegevens en trends

Op het internet is veel materiaal op het gebied van cybercrime, en de daarmee gepaard gaande vormen van fraude en oplichting te vinden. De meeste cijfers zijn echter niet representatief voor een bepaalde welomschreven populatie. ICT-bedrijven die zelf beveiliging als dienst leveren beschikken over veel technische kennis, zitten dicht bij de bron van het kwaad en zien de gevolgen van cybercriminaliteit voor hun klanten. De door hen verzamelde gegevens zijn interessant, maar niet gebaseerd op een nette steekproefopzet en mogelijk gekleurd door eigenbelang. Wie beveiliging verkoopt kan in de verleiding komen het gevaar te overdrijven. Hetzelfde geldt voor non-profit instanties die in het leven geroepen zijn om computercriminaliteit te bestrijden. Daarnaast is er mogelijk sprake van beroepsdeformatie, een gekleurde perceptie van de werkelijkheid. Het is denkbaar dat het aantal vormen van computercriminaliteit groeit zonder dat het aantal slachtofferschappen mee groeit, al was het maar omdat de professionele bestrijders goed hun werk doen. Dat neemt niet weg dat de vragen die commerciële ICT-beveiligers in hun enquêtes stellen van inzicht in de materie getuigen en goed als voorbeelden voor een Nederlandse slachtofferenquête kunnen dienen.

De nationale statistische bureaus houden zich nog slechts in beperkte mate met economische delicten en computer criminaliteit bezig. Slechts in een aantal Engelstalige landen wordt er op de websites van de overheid of de statistische bureaus melding gemaakt van slachtofferenquêtes waarin dit onderwerp aan bod komt. Onder burgers gaat het dan vaak slechts om enkele deelonderwerpen, zoals identiteitsfraude. Daar waar bedrijfsenquêtes worden gehouden zijn de enquêtes diepgravender, en komt een heel scala aan onderwerpen aan bod. Scans bij Franstalige en Duitstalige websites hebben weinig opgeleverd. Het weinige dat aan materiaal werd aangetroffen heeft geen toegevoegde waarde ten opzichte van de Engelstalige landen (Verenigd Koninkrijk, Verenigde Staten, Canada, Australië en Nieuw Zeeland). Daarom wordt de bespreking van de huidige status quo tot deze landen beperkt. Als eerste komt echter het internationale onderzoek aan bod.

4.1 Landen overstijgend

Een weinig verrassende constatering is dat het internetgebruik de afgelopen jaren met sprongen is toegenomen. Uit tabel 2 blijkt dat met name in ontwikkelingsgebieden met relatief lage penetraties zoals het Midden Oosten en Afrika de groei het hoogst is. Binnen Europa heeft Nederland de hoogste internetpenetratie, gevolgd door een aantal Scandinavische landen en Portugal. In economische grootmachten als het Verenigd Koninkrijk, Duitsland en Frankrijk is de penetratie aanzienlijk lager. Dit zou de Nederlander relatief kwetsbaar kunnen maken als slachtoffer van cybercrime.

Tabel 2. Internetgebruik in de wereld en in Europa, gesorteerd op penetratie in 2008.
Bron: http://www.internetworldstats.com/

	populatie in 2008	internet-gebruikers in 2008	penetratie (thuis) %	gebruikers (thuis) %	groei 2001-2008 %
Werelddelen				basis: wereld	
Noord Amerika	337,167,248	248,241,969	73.6	17.0	129.6
Oceanië / Australië	33,981,562	20,204,331	59.5	1.4	165.1
Europa	800,401,065	384,633,765	48.1	26.3	266.0
Latijns Amerika/Caraïbisch gebied	576,091,673	139,009,209	24.1	9.5	669.3
Midden Oosten	197,090,443	41,939,200	21.3	2.9	1176.8
Azië	3,776,181,949	578,538,257	15.3	39.5	406.1
Afrika	955,206,348	51,065,630	5.3	3.5	1031.2
Totaal wereld	**6,676,120,288**	**1,463,632,361**	**21.9**	**100.0**	**305.5**
Geselecteerde landen Europa				basis: Europa	
Nederland	16,645,313	15,000,000	90.1	3.9	284.6
Noorwegen	4,644,457	4,074,100	87.7	1.1	85.2
IJsland	304,367	258,000	84.8	0.1	53.6
Zweden	9,045,389	7,000,000	77.4	1.8	72.9
Portugal	10,676,910	7,782,760	72.9	2.0	211.3
Luxemburg	486,006	345,000	71.0	0.1	245.0
Faroer Eilanden	48,668	34,000	69.9	0.0	1033.3
Zwitserland	7,581,520	5,230,351	69.0	1.4	145.1
Denemarken	5,484,723	3,762,500	68.6	1.0	92.9
Finland	5,244,749	3,600,000	68.6	0.9	86.8
Verenigd Koninkrijk	60,943,912	41,817,847	68.6	10.9	171.5
Liechtenstein	34,498	23,000	66.7	0.0	155.6
Slowenië	2,007,711	1,300,000	64.8	0.3	333.3
Duitsland	82,369,548	52,533,914	63.8	13.7	118.9
Spanje	40,491,051	25,623,329	63.3	6.7	375.6
Wit Rusland	9,685,768	6,000,000	61.9	1.6	3233.3
Monaco	32,796	20,000	61.0	0.0	185.7
Estland	1,307,605	780,000	59.7	0.2	112.8

	populatie in 2008	internet-gebruikers in 2008	penetratie (thuis) %	gebruikers (thuis) %	groei 2001-2008 %
Italië	58,145,321	34,708,144	59.7	9.0	162.9
Frankrijk	62,177,676	36,153,327	58.1	9.4	325.3
Rusland	140,702,094	32,700,000	23.2	8.5	954.8
Albanië	3,619,778	471,200	13.0	0.1	18748.0
Totaal Europa	**800,401,065**	**384,633,765**	**48.1**	**100.0**	**266.0**

Er zijn twee grote internationale slachtofferenquêtes:

- de ICVS, the International Crime Victim Survey, in een aantal landen verspreid over de wereld
- de EU-ICS, the European Crime and Safety Survey, in een aantal landen in Europa

In beide enquêtes is een beperkt aantal vragen over oplichting en computercriminaliteit opgenomen (Van Dijk e.a. 2007). Er wordt gevraagd naar

1. ***Aard en omvang***
   a. ***delictvormen:*** typen oplichting; via internet shoppen; credit card fraude.
2. ***Melding- en aangiftegedrag en reactie:*** melden aan de politie.

Op basis hiervan kan een beperkte vergelijking van landen worden gemaakt. Zo hoog als Nederland staat op de ranglijst van internetpenetratie, zo laag staat Nederland op de lijst van fraude bij internet winkelen en credit cards. Deze cijfers suggereren dat Nederlanders voorzichtig met deze zaken omgaan, maar waar dat precies in zit wordt uit de gegevens niet duidelijk; mogelijk ligt het aan het feit dat in Nederland vergeleken met bijvoorbeeld de VS minder gebruik wordt gemaakt van credit cards.

Tabel 3. Percentages slachtofferschappen van fraude in diverse landen en steden (totale bevolking) gedurende een jaar in 2003/2004; bron: Van Dijk e.a. (2007).

Landen	Internet winkelen	credit card	Steden	Internet winkelen	credit card
USA	3.3	4.0	Berlijn	3.8	
Polen	3.0		New York	3.7	4.3
Duitsland	2.7		Londen	3.2	7.5
Bulgarije	2.6		Parijs	2.7	2.4
Engeland, Wales	2.2	1.7	Kopenhagen	1.5	0.1
Noorwegen	1.5		Edinburgh	1.0	1.9
Denemarken	1.4	0.3	Madrid	1.0	1.3
Nieuw Zeeland	1.3		Wenen	0.9	0.4
Zweden*	1.2	0.3	Hong Kong	0.9	
Noord Ierland	1.2	1.3	Amsterdam	0.9	0.3
Oostenrijk	1.1	0.4	Dublin	0.7	1.6

Landen	Internet winkelen	credit card	Steden	Internet winkelen	credit card
Schotland	1.0	1.4	Stockholm	0.7	0.2
Spanje	0.7	0.9	Brussel	0.6	1.1
Ierland	0.7	1.3	Tallinn	0.6	
Canada	0.7		Belfast	0.5	1.4
Estland	0.6		Athene	0.4	1.4
Portugal	0.5	0.4	Oslo	0.4	
Luxemburg	0.5	0.3	Reykjavik	0.3	
IJsland	0.4		Lissabon	0.2	0.0
Frankrijk	0.4	0.3	Helsinki	0.0	0.1
België	0.4	0.4	Boedapest	0.0	0.1
Nederland	0.3	0.4	Rome	0.0	
Mexico	0.2	0.6			
Griekenland	0.1	1.4			
Finland	0.1	0.0			
Italië	0.0	0.1			
Gemiddeld	1.1	0.9	Gemiddeld	1.1	1.5

4.2 Nederland

Binnen Nederland bestaat al enige ervaring met het onderzoeken van computercriminaliteit. Een interessant project is een pilot studie in het MKB (Syntens, 2006). Bij 50 bedrijven is door adviseurs van Syntens onderzocht hoe het in de praktijk is gesteld met de beveiliging van de computernetwerken en de gegevens van ondernemers, welke schade zij hebben opgelopen en aan welke risico's ze bewust of onbewust bloot staan. Het gaat dan niet alleen om het gevaar via internet maar ook om uitval van systemen door andere oorzaken. Geconstateerd is dat beleid op het gebied van informatiebeveiliging meestal ontbreekt. De belangrijkste conclusies waren:

1. ondernemers zijn sterk afhankelijk van informatiesystemen maar nemen geen adequate maatregelen om de beschikbaarheid te borgen;
2. informatiebeveiliging heeft meer met organisatie en cultuur dan met technologie te maken;
3. mensen zijn de zwakste schakel;
4. ondernemers schuiven de verantwoordelijkheid af naar hun ICT-toeleveranciers.

Het grootste deel van de pilotstudie bestond uit demonstraties, simulaties van wat er fout kan gaan. Hieraan voorafgaand werd een vragenlijst voorgelegd, waarin met name nuttige vragen over risico's en preventie staan.

1. ***Aarde en omvang***
   a. ***risicokenmerken: c***omputerbezit; type internetverbinding; inrichting email; telewerken; draadloze netwerken; website; online verkoop; betaalwijze; beveiligde verbinding; subjectieve veiligheid.
2. ***Delictvormen:*** geen.
3. ***Schade***
   a. ***economische schade:*** storingen.

4. ***Preventieve maatregelen:*** fysieke beveiliging apparatuur; firewall; anti-virus software; anti-spyware; online inkoop; privileges medewerkers; versturen (ongevraagde) email; bescherming klantgegevens (intern en extern); maken backups; beheer website; encryptie; beleid wachtwoorden; beleid beveiliging en bekendheid hiervan; vastleggen procedures.

De website 'waarschuwingsdienst.nl' is een dienst van GOVCERT.nl – het Computer Emergency Response Team van de Nederlandse overheid. GOVCERT is een onderdeel van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. De Waarschuwingsdienst is een van de langstlopende initiatieven op het terrein van voorlichting en 'high tech crime'. Het 'Security Team' van GOVCERT scant verschillende bronnen – zowel publieke als vertrouwelijke – naar potentiële gevaren op het internet en de oplossingen daarvoor. Indien deze informatie relevant is voor de beoogde doelgroepen, wordt een 'alert' geschreven en op de website geplaatst. De technisch georiënteerde rapportage van deze dienst is voornamelijk in woorden en niet in tabellen. Eén van de redenen hiervoor is de voortdurende gedaanteverandering van de dreigingen, waardoor er in de loop van de tijd geen vaste definities beschikbaar zijn waarop longitudinale statistieken gebaseerd kunnen worden. De rapportage van GOVCERT is dan ook bedoeld voor gebruikers die geïnteresseerd zijn in de technische ontwikkelingen van cybercrime. Als longitudinaal georiënteerde monitor van slachtofferschappen is de rapportage minder geschikt.

Tenslotte voert Ernst & Young jaarlijks onderzoek naar Cybercrime uit (Ernst & Young, 2009). Hierin ligt de nadruk zeer sterk op beveiliging. Het gaat om een internet-onderzoek onder 600 Nederlandse directeuren, managers en professionals uit het bedrijfsleven.

1. ***Aarde en omvang***
   a***. delictvormen:*** computervirussen; computerinbraak; aanbod illegale diensten; phishing; denial of service; spyware; diefstal intellectueel eigendom; internet stalking; vermogensdelicten; identiteitsdiefstal;
   b. ***risicokenmerken:*** afhankelijkheid van ICT, risico nieuwe technologieën.
2. ***Melding- en aangiftegedrag en reactie:*** ondernomen acties bij cybercrime; redenen voor geen aangifte; vertrouwen in politie en justitie.
3. ***Schade:*** geen.
4. ***Preventieve maatregelen***
   a. ***preventie vooraf:*** aanwezigheid noodplan; vertrouwen in eigen beveiliging; technische maatregelen; beveiligingsbewustzijn eigen medewerkers.

Over de wijze van steekproeftrekking en de generaliseerbaarheid van de uitkomsten is het rapport onduidelijk, al claimt men wel 'representativiteit'. Een aantrekkelijk punt is de relatief lange consistente tijdreeks vanaf 2003, waaruit onder meer blijkt dat de kosten voor ICT-beveiliging jaarlijks bij gemiddeld 30% van de bedrijven stijgen. Het meest opvallende cijfer is dat bij slechts 10% van de bedrijven in geval van cybercrime aangifte wordt gedaan bij de politie.

4.3 Verenigd Koninkrijk

In het Verenigd Koninkrijk zijn vanuit de overheid drie verschillende instrumenten beschikbaar om het criminaliteitsniveau te meten:

- de Commercial Victimization Survey (CVS)
- de Offending Crime and Justice Survey (OCJS)
- de British Crime Survey (BCS)

De CVS is een slachtofferenquête onder bedrijven. Deze is voor het eerst gehouden in 1994, de tweede en vooralsnog laatste meting was in 2002. Met name de meting in 2002 was zeer uitgebreid op zowel het gebied van cybercrime als financieel-economische criminaliteit.

1. ***Aard en omvang***
   a. ***delictvormen:*** computervirus; hacking; defacing; informatiediefstal dDOS; verduistering, afpersing; diefstal door eigen personeel; omkoping ambtenaren en private personen in binnen- en buitenland; omkoping eigen personeel; samenzwering om te verhinderen dat men contracten krijgt; smokkel (en zo goedkoop kunnen inkopen); verzoek tot heling;
   b. ***risicokenmerken:*** ligging bedrijf; computerbezit credit card, kopen via internet.
2. ***Melding- en aangiftegedrag en reactie:*** informeren politie; reden niet informeren; informeren andere bedrijven in de branche; koepelorganisatie; claim bij verzekeraar; informeren service provider; informeren host website.
3. ***Schade***
   a***. economische schade:*** waarde verduisterde gelden of goederen.
4. ***Preventieve maatregelen***: firewall; antivirus software; beperking emailgebruik; beperking gebruik floppy disk; gedragscode; rampenplan.

Het onderzoek is gehouden op basis van een netto steekproef van 6516 bedrijven; de steekproef is getrokken uit de database van Yell Data, het voormalige bedrijfsregister van British Telecom. Er is gestratificeerd naar bedrijfsgrootte, sector en al dan niet ligging in een sociaal zwakke regio. De interviews zijn telefonisch afgenomen. Van de 10660 getrokken bedrijven hebben er 6516 gerespondeerd, een respons van 61%. De gemiddelde interviewduur was 20 minuten.

De OCJS is een vragenlijst naar daderschap, die in 2003 onder de bevolking tot 65 jaar is gehouden; daarna is de jaarlijkse meting beperkt tot jongeren van 10 tot 25 jaar. Hoewel computercriminaliteit hierin voorkomt is dit instrument niet bruikbaar voor dit project omdat het is gericht op daderschap in plaats van slachtofferschap.

De British Crime Survey (BCS) is een slachtofferenquête onder personen van 16 jaar en ouder. Jaarlijks worden hierin 51.000 personen face to face ondervraagd. De respons in 2007 bedroeg 76% (Kershaw e.a., 2008). Het onderzoek bevat drie relevante modules.

BCS Mobiele telefoons

1. ***Aard en omvang***
   a. ***delictvormen:*** diefstallen en omstandigheden;
   b. ***risicokenmerken:*** bezit mobiele telefoons in huishouden.

2. ***Melding- en aangiftegedrag en reactie:*** rapporteren aan politie en service provider.

BCS Technologie

1. ***Aard en omvang***
   a. ***delictvormen:*** fraude of slechte dienstverlening bij aankoop via het internet; schade door virus; hacking; kwetsend materiaal via internet of email;
   b. ***risicokenmerken:*** gebruik van internet; gebruik van credit cards.
2. ***Melding- en aangiftegedrag en reactie:*** rapporteren virus, hacking; kwetsend materiaal aan politie of andere partijen.
3. ***Schade***
   c. ***gedragschade:*** preventief gedrag als reactie op kwetsend materiaal.

BCS Identiteitsfraude

1. **Aard en omvang**
   a. ***delictvormen:*** diefstal identiteitspapieren; gebruik mijn identiteit voor aankopen of diensten;
   b. ***risicokenmerken:*** bezit identiteitpapieren (paspoort, rijbewijs).
2. ***Melding- en aangiftegedrag en reactie:*** tijd totdat probleem is opgelost.

In de BCS rapporteerde 4% van de huishoudens in 2005 een diefstal van een mobiele telefoon. De helft hiervan werd gerapporteerd aan de politie, drie kwart aan de netwerk service provider. Van de houders van credit cards is 4% het slachtoffer geweest van fraude. Credit card fraude is een type misdrijf waar men relatief zeer bezorgd over is (19% zegt zeer bezorgd te zijn) vergeleken met autodiefstal, inbraak en fysiek geweld.

Meer recente en uitgebreide cijfers over het Verenigd Koninkrijk staan in Fafinsky en Minassian (2008). Hierin wordt een overzicht gegeven van de computercriminaliteit uit verschillende bronnen. Het rapport is van beveiligingsbedrijf Garlik, de tweede in een serie. De voornaamste uitkomsten zijn weergegeven in tabel 4.

Tabel 4. Gevallen van cybercrime in 2006 en 2007; bron: Fafinsky en Minassian (2008)

	2007	**2006**	**verandering**
Identiteitsdiefstal en -fraude	84,700	92,000	-8%
Financiële fraude	255,800	207,000	24%
Kwetsen van personen	2,240,000	1,944,000	15%
Computer misbruik (exclusief virussen)	132,800	144,500	-8%
Ongewenste sexuele benaderingen online (waaronder grooming)	830,000	850,000	-2%
Totaal	3,543,300	3,237,500	9%

Hierbij wordt het misbruiken van credit card gegevens niet gerekend onder identiteitsfraude maar onder financiële fraude. Bij financiële fraude is het verlies door plastic kaart fraude £535 miljoen op een totaalbedrag aan betalingen van £568 miljard. Met name het kwetsen van personen en asociaal cybergedrag hebben dankzij de opkomst van sociale netwerk sites grote vormen aangenomen: 2,24 miljoen gevallen op 61 miljoen Britten. Deze cijfers geven geen informatie over aantallen individuele slachtoffers en hoe zij de criminaliteit ervaren.

4.4 Verenigde Staten

In de Verenigde staten zijn er vanuit de officiële statistieken twee belangrijke bronnen

- de National Computer Security Survey (NCSS)
- de National Crime Victim Survey (NCVS)

De NCSS is een grootschalige enquête in opdracht van het Justice Department door RAND Corporation onder 7818 bedrijven. De steekproef is gebaseerd op een bedrijfsregister en gestratificeerd naar bedrijfsomvang, sector en risiconiveau (een classificatie van het Department of Homeland Security). De enquête is gehouden in 2006, de data betreffen het voorafgaande kalenderjaar. De gegevens zijn deels verzameld via het internet en deels middels een schriftelijke enquête. De respons bedroeg 23%.

Inhoud NCSS

1. ***Aard en omvang***
   a. ***delictvormen:*** virussen, Trojaanse paarden, wormen; denial of service; vandalisme en sabotage; verduistering; fraude (identiteitsfraude en meer in het algemeen: de waarheid verkeerd voorstellen); diefstal intellectueel eigendom; diefstal van persoonlijke of financiële informatie; overig (hacking, spoofing, phishing, sniffing, pinging, scanning, spyware, keylogging, adware); diefstal van laptops;
   b. ***risicokenmerken:*** ICT Infrastructuur.
2. ***Melding- en aangiftegedrag en reactie:*** rapporteren bij politie en organisaties; redenen waarom niet; mogelijke daders.
3. ***Schade***
   a. ***economische schade:*** schade in geld en downtime.
4. ***Preventieve maatregelen:*** belangrijkste zorgen; perceptie belangrijkste bedreigingen; veiligheidstechnologie nu en in de toekomst; procedures; uitbesteden veiligheid, testen; kosten; effectiviteit (wat is voorkomen?).

Het onderzoek is een vervolg op een pilot die in 2001 is gehouden. Toen is ook de basis structuur van de vragenlijst ontwikkeld. De vragenlijst is in 2006 aangepast aan de technologische stand van zaken (RAND, 2008). Hiervoor is uitvoerig cognitief onderzoek gedaan naar de validiteit en de begrijpelijkheid van de vragenlijst. Uit het globale methodologisch verslag van RAND komen de volgende punten naar voren:

- De vraagvolgorde is belangrijk om te zorgen dat categorieën goed worden ingevuld. Zo is verduistering een speciaal geval van fraude; om te zorgen dat verduistering als aparte

categorie wordt gezien moeten de vragen over verduistering voorafgaan aan de vragen over fraude.

- Verschillende onderdelen van de vragenlijst moeten soms door verschillende personen worden beantwoord. Vragen over virussen, denial of service, elektronisch vandalisme en sabotage kunnen het best door technische mensen worden beantwoord, terwijl anderen meer weten over verduistering, fraude en identiteitsdiefstal. Wanneer een vragenlijst in wordt opgedeeld om door verschillende personen te worden beantwoord moet hierop worden gelet.
- De wijze waarop ICT in grote bedrijven is georganiseerd varieert zeer sterk, van een centrale afdeling die alles bestiert tot een structuur waarin betrekkelijk kleine eenheden autonoom kunnen functioneren. Dit maakt dat het moeilijk is om voor een bedrijf complete informatie te krijgen. Het is in ieder geval een argument om de enquête in te steken op vestigingsniveau, en pas als blijkt dat het niet anders kan over te gaan op bedrijfsniveau.

Het onderzoek is zeer gedetailleerd en doorwrocht opgezet en kan zeer goed als vertrekpunt fungeren voor een bedrijfsenquête binnen Nederland. De specifieke analyses per vraag zijn een goede checklist bij het construeren van een Nederlandse vragenlijst.

Tabel 5. Prevalentie van incidenten: bedrijven die in 2005 incidenten hebben meegemaakt.
Bron: NCSS 2005

	alle bedrijven*	**aantal**	**%**
Alle incidenten	7,636	5,081	67
Cyber aanval	7,626	4,398	58
Computer virus	7,538	3,937	52
Denial of service	7,517	1,215	16
Vandalisme, sabotage	7,500	350	5
Cyber diefstal	7,561	839	11
Verduistering	7,492	251	3
Fraude	7,488	364	5
Diefstal intellectueel eigendom	7,492	227	3
Diefstal persoonlijke of financiële gegevens	7,476	249	3
Andere incidenten	7,492	1,792	24

*: alle bedrijven die antwoord gaven op de vraag of ze een incident van het betreffende type hadden opgemerkt

Uit tabel 5 blijkt dat twee derde van de bedrijven in 2005 incidenten heeft meegemaakt. De meest voorkomende daarvan zijn besmettingen met virussen. Echter, alle in de NCSS behandelde vormen van criminaliteit komen met (enige) regelmaat voor. Tabel 6 laat zien dat er binnen bepaalde delictvormen ook nog grote variëteit bestaat.

Tabel 6. Uitsplitsing enkele typen incidenten; bron: NCSS 2005

	%	n
Intellectueel eigendom (3% in tabel 5)		
Bedrijfsgeheimen	70	
Copyrighted material	47	
Gepatenteerd material	14	
Trademarks	8	
Aantal bedrijven*		198
Persoonlijke of financiële informatie (3%)		
Namen of geboortedata	60	
Sociale zekerheids nummers	49	
Credit card nummers	34	
PIN codes of rekeningnummers	27	
Nummers bank- of betaalpassen	14	
Anders	21	
Aantal bedrijven*		235
Andere veiligheidsincidenten (24%)		
Adware en andere malware	77	
Spyware, keystroke logging	58	
Phishing, spoofing	53	
Scanning, pinging of sniffing	33	
Hacking	16	
Diefstal van andere informatie	3	
Anders	8	
Aantal bedrijven*		1762

*: alle bedrijven die gedetailleerde informatie over de incidenten hebben verstrekt.

In tabel 7 wordt duidelijk dat 91% van de ondervraagde bedrijven een of andere vorm van schade leden, hetzij direct financieel, hetzij in downtime. Uit tabel 8 blijkt dat het om aanzienlijke schadeposten gaat. Bij de 3247 bedrijven die de vragen hebben beantwoord ging het om $866,600,600, bijna een miljard. Hierbij kan het met name bij diefstal om grote bedragen gaan. De bedragen hebben betrekking op de totale kosten: diagnose, herstel, vervanging van hard- en software, arbeidskosten, de waarde van verloren informatie, gestolen producten, gemiste verkoop en productiviteit en juridische kosten. Slechts de kosten van toekomstige preventie zijn niet meegeteld.

Tabel 7. Schade in geld en downtime*. Bron: NCSS 2005

	%
Geen schade	9
Wel schade	91
Alleen schade in geld	38
Alleen schade in downtime	12
Schade in beide	41

*: gebaseerd op 4083 bedrijven die tenminste een vraag naar schade in geld of downtime hebben beantwoord.

Tabel 8. Schade in dollars en downtime in uren, naar type incident. Bron: NCSS 2005

	aantal incidenten		verlies in 1000 $		uren downtime	
	totaal	mediaan	totaal	mediaan	totaal	mediaan
Alle incidenten	22,138,250	6	866,600	6	323,900	16
Cyber aanval	1,582,913	4	313,900	5	219,600	12
Computer virus	1,460,242	3	280,700	5	193,000	12
Denial of service	121,652	3	21,100	5	19,200	7
Vandalisme of sabotage	1,019	1	12,200	5	7,300	10
Cyber diefstal	130,970	2	450,000	29		
Verduistering	1,565	1	158,700	50		
Fraude	125,510	3	103,100	20		
Diefstal van intellectueel eigendom	607	1	159,400	43		
Diefstal van persoonlijke of financiële gegevens	3,288	1	28,800	20		
Andere veiligheidsincidenten	20,424,367	20	102,700	5	104,300	23
Aantal bedrijven	**4,433**		**3,247**		**2,157**	

Uit de numerieke uitkomsten blijkt dat alle vormen van computer criminaliteit voldoende vaak voorkomen om ook in Nederland opname in een enquête te rechtvaardigen; de aantallen zullen in de regel groot genoeg zijn om tot betrouwbare schattingen te komen van prevalenties; dit geldt ook voor incidenties en schade, mits ingedeeld in klassen, zie ook hoofdstuk 6.

Een onderzoek naar cybercrime dat al 13 jaar loopt, is dat van CSI (Computer Security Institute; Richardson, 2008). Hierin worden computerveiligheidsprofessionals uit het bedrijfsleven ondervraagd. Dit is geen representatief onderzoek voor het gehele bedrijfsleven. Bovendien speelt mogelijk het eigenbelang van de onderzoekende partij mee. Er is echter wel een lange ervaring met de gestelde vragen. Aan de versie van 2008 namen 512 respondenten deel, een respons van ruim 10%. De vragen betreffen

1. ***Aard en omvang***
   a. ***delictvormen:*** aantal incidenten; type incidenten; aantal aanvallen.
2. ***Melding- en aangiftegedrag en reactie:*** geen.
3. ***Schade***
   a. ***economische schade:*** verlies in dollars; percentage verlies door eigen personeel.

4. ***Preventieve maatregelen:*** het veiligheidsbudget als percentage van het IT-budget; kosten voor beveiligingsbewustwording als percentage van IT-budget; percentage dat normen hanteert als return of investment voor beveiliging; uitbesteden; soort beveiliging; technieken om de beveiliging te evalueren; aangiftegedrag; soort actie na incident; redenen om geen aangifte te doen; status van het beveiligingsbeleid (formeel, informeel e.d.); beleid t.a.v. data opslag; processen t.a.v. software ontwikkeling.

Hoewel de cijfers uit de enquête niet representatief zijn, bevat de vragenlijst interessante concepten die elders niet worden aangetroffen. Deze hebben vooral te maken met organisatie en ICT-beleid binnen bedrijven.

De NCVS wordt gehouden onder burgers, en is in de VS de reguliere slachtofferenquête. Het gaat om een gestratificeerde meertraps-clustersteekproef. De primary sampling units (PSU's) zijn counties (onderdelen van staten) en stedelijke gebieden. Grote PSU's (in termen van inwoners) vallen automatisch bij de eerste trap in de steekproef, kleine PSU's worden gegroepeerd in strata en met kans evenredig aan de omvang getrokken. In de tweede trap wordt een PSU verdeeld in vier niet overlappende frames. Uit elk hiervan worden door middel van area sampling huishoudens getrokken. Binnen een huishouden wordt elke persoon van 12 jaar en ouder ondervraagd. Dit is een face to face enquête, waarin de interviewer vragen stelt, maar ook formulieren aanreikt die de respondent zelf moet invullen. De respons in 2006 bedroeg 91% op huishoudniveau en 86% op persoonsniveau.
Hierin is vanaf 2005 een module opgenomen over identiteitsfraude.

Inhoud NCVS

1. ***Aard en omvang***
   a. ***delictvormen:*** gebruik bestaande rekeningen; openen nieuwe rekeningen; verkrijgen van diensten of een baan; gebruik identiteit voor verkrijgen uitkeringen; type rekeningen; wijze en tijdstip waarop ontdekt; duur misbruik; wijze waarop de dader aan de informatie kwam; mislukte pogingen.
2. ***Melding- en aangiftegedrag en reactie:*** rapportage aan relevante instanties, politie; reactie politie; aangiftebewijs; redenen om niet aan te geven; daderkennis.
3. ***Schade***
   a. ***economische schade:*** kosten in dollars; kosten in tijd; kosten in weigering kredietverstrekking; baanverlies etc.;
   b. ***psychologische schade:*** reactie op behandeling door credit card maatschappij; reactie op behandeling door politie; problemen met mensen die je niet meer vertrouwt; mate van stress; professionele hulp; fysieke symptomen.
4. ***Preventieve maatregelen:*** preventie door regelmatig financiën checken; software; kopen online.

Verder worden specifiek over cybercrime in de NCVS geen vragen gesteld.

Het Bureau of the Census (het Amerikaanse CBS) test in hun cognitieve laboratorium de vragen die in de belangrijke surveys worden gesteld. Zo is ook de module over identiteitsfraude getest (Hughes, 2004). Algemene opmerking is dat de precieze omschrijvingen voor de interviewer soms lastig zijn om voor te lezen. Ze kan erover struikelen. Desondanks leek dit niet tot problemen te leiden omdat

de respondenten zelf goed genoeg wisten wat hen was overkomen en daar graag over rapporteerden. Andere problemen bleken:

- Een identiteitsdiefstal kan meerdere gevolgen hebben; wanneer gesproken wordt over een incident, dan kan het onduidelijk zijn of hier de diefstal of één van de gevolgen wordt bedoeld.
- De tijdsduur die verliep tussen ontdekking van de diefstal en het stoppen van misbruik was moeilijk aan te geven en een bron van verwarring. Deze vraag is in de definitieve versie weggelaten.
- Kosten als gevolg van de diefstal waren voor de respondenten moeilijk in te schatten. Postzegels, telefoonkosten, maar ook gedwongen vrij nemen van het werk en advocaatkosten werden door de ene respondent wel en door de andere niet meegeteld. Daarbij komt dat mensen hun uurloon vaak niet kennen, waardoor ze gemiste uren niet in geld kunnen omrekenen.
- Daderkennis. Dit is een onduidelijk begrip. Gaat het om het kennen van de naam, het uiterlijk, of om persoonlijk kennen? De vraag is in de definitieve versie weggelaten.

Voor de overgrote meerderheid bleken echter de oorspronkelijk voorgestelde vragen goed te worden begrepen.

In de VS is als aanvulling op de slachtofferenquête ook een module ontwikkeld over grooming en het aanbieden van pornografisch materiaal, voor jongeren tussen 10 en 17 jaar. Deze module is getest in het cognitieve laboratorium (Beck en DeMaio, 2007), waarna is besloten deze vooralsnog niet in de enquête op te nemen maar eerst verder te testen. Problemen waren onder andere:

- geen duidelijk onderscheid tussen grooming en andere vormen van sexuele delicten in de slachtofferenquête;
- in het geval dat er sprake was van een delict werd er in sterke mate buiten de referentieperiode van 6 maanden gerapporteerd (telescoping). Men wil kennelijk te graag zijn verhaal kwijt;
- aan de andere kant was er sprake van gêne en zorg om vertrouwelijkheid;
- moeite met definities van wat online zijn betekent en de activiteiten die daaronder vallen; verschil tussen email en instant messaging werd niet gemaakt.

Het feit dat in de VS zulke analyses tegenwoordig standaard worden uitgevoerd bij nieuwe (onderdelen van) vragenlijsten geeft vertrouwen in de validiteit van de definitieve versies. Daarnaast geven de beide besproken rapporten over de cognitieve analyses een goed beeld van wat er mis kan gaan.

Tabel 9. Identiteitsdiefstal bij huishoudens in de VS. Bron: NCVS 2005

	aantal huishoudens	**%**
identiteitsdiefstal	6,426,200	5.5
bestaande credit card	2,966,500	2.5
andere bestaande rekeningen	1,586,500	1.4
persoonlijke informatie	1,083,100	0.9
meerdere typen gedurende één periode	790,200	0.7
geen identiteitsdiefstal	109,206,700	93.3
onbekend	1,477,800	1.3
totaal	117,110,800	100.0

De schatting van het aantal huishoudens in de VS dat in 2005 met identiteitsdiefstal te maken kreeg is bijna 6,5 miljoen (tabel 9). Credit cards zijn hierbij het voornaamste doelwit, maar dit betreft wel minder dan de helft van het aantal cases. De manier waarop dit wordt opgemerkt varieert (tabel 10). Het gemiddelde verlies per diefstal bedraagt $1620, maar blijkens tabel 11 kan het soms om grote bedragen gaan. Het gemiddelde is aanzienlijk groter dan de mediaan, wat past bij een scheve verdeling.

Tabel 10. Manier waarop identiteitsdiefstal werd opgemerkt; kolompercentages. Bron: NCVS 2005

	totaal	**bestaande creditcard**	**andere bestaande rekeningen**	**persoonlijke informatie**	**verschillende typen gedurende één periode**
ontbrak geld, onbekende afschrijvingen op rekening	30.8	33.5	43.5	5.2	30.6
er werd contact opgenomen over laat of niet betaalde rekeningen	20.6	26.8	6.4	23.3	22.4
problemen met bankieren	13.1	10.4	17.7	9.1	19.7
foutieve kredietmelding	5.6	4.8	3.5	10.0	6.2
credit card/chequeboek verdwenen	5.3	6.7	5.4	1.1	5.3
rekening geblokkeerd bij instelling	4.3	4.9	4.1	1.6	5.9
anders	29.6	20.1	30.8	52.2	32.0

Tabel 11. Schade als gevolg van identiteitsdiefstal; kolompercentages. Bron: NCVS 2005

	totaal	**bestaande creditcard**	**andere bestaande rekeningen**	**persoonlijke informatie**	**verschillende typen gedurende één periode**
$0	18.3	13.3	16.8	37.3	14.8
$1-99	16.7	21.2	18.8	5.6	10.6
$100-249	12	12.4	14.8	7.8	10.1
$250-499	10.8	11.8	12.2	4.5	12.2
$500-999	10.8	11.3	11.7	6.2	13.2

	totaal	bestaande creditcard	andere bestaande rekeningen	persoonlijke informatie	verschillende typen gedurende één periode
$1,000-2,499	10.2	10	10.8	7.6	13.1
$2,500-4,999	3.6	4.2	2.3	2.5	5.5
$5,000 of meer	4.7	3.8	3.2	6.6	8.7
weet niet	12.9	11.9	9.4	21.8	11.8
gemiddelde	$1,620	$980	$1,220	$4,850	$2,460
mediaan	$300	$300	$300	$500	$540

4.5 Australië

Australië is in 2007 gestart met een Personal Fraud Survey, als module in de arbeidskrachtentelling. De enquête is gehouden onder personen van 15 jaar en ouder (22.800 huishoudens). De vragenlijst is niet online beschikbaar; wel is er een rapport dat een goed beeld van de inhoud van de enquête geeft en waarmee de vragenlijst gemakkelijk kan worden gereconstrueerd. Computercriminaliteit is een onderdeel van de vragenlijst, maar het onderwerp is breder.

1. ***Aard en omvang***
   a. ***delictvormen:*** misbruik credit card of bank card; identiteitsdiefstal; loterijen; pyramidespel; phishing; financieel advies; kettingbrief; voorschotfraude; methode.
2. ***Melding- en aangiftegedrag en reactie:*** aan wie gerapporteerd.
3. ***Schade***
   a. ***economische schade:*** verlies aan geld en tijd;
   c. ***gedragschade:*** gedragsverandering.

Deze karakteristieken zijn gevraagd voor het meest recente incident. Daardoor zijn de uitkomsten niet representatief op incidentniveau; incidenten bij mensen met veel incidenten zijn ondervertegenwoordigd. Hier is niet door weging voor gecorrigeerd (dit kan door op case-niveau naar het aantal incidenten te wegen). Bij credit card fraude en identiteitsdiefstal was de meeteenheid de ‘episode’, de periode waarin alle gevolgen van de diefstal aan het licht kwamen, en niet één apart gevolg.

Uit een overzichtstabel (tabel 12) blijkt dat de verschillende vormen van computercriminaliteit bij elkaar voor een miljard Australische dollar (0,7 miljard Euro) aan schade.

Tabel 12. Prevalentie computercriminaliteit en financiële schade. Bron: Personal Fraud Survey(2007)

	slachtoffers x 1000			niet-slachtoffers	ratio
	man	vrouw	allen	x 1000	%
Identiteitsfraude					
credit card fraude	203	180	383	15842	2.4
identiteitsdiefstal	69	55	124	16101	0.8
totaal	269	231	500	15726	3.1
Vormen van oplichting					
loterijen	45	39	84	16141	0.5
pyramidespel	39	32	71	16154	0.4
phishing en verwante vormen	30	28	58	16167	0.4
financieel advies	18	11	29	16197	0.2
kettingbrieven	13	14	27	16199	0.2
voorschotfraude	9	7	16	16209	0.1
anders	38	31	69	16156	0.4
totaal	181	148	329	15896	2.0
alle typen fraude	438	368	806	15419	5.0
totale financiële schade					
totaal aantal slachtoffers met financiële schade	235	218	453	15732	
totale schade (miljoen $)	518	459	977		
gemiddelde schade per persoon ($)	2207	2101	2156		
mediane schade per persoon ($)	445	489	450		

Een bedrijvenenquête is gehouden door een consortium van verschillende partijen en uitgevoerd door AC Nielsen: de Australian Crime and Computer Security Survey (ACCSS; zie AusCERT, 2006). Vragen zijn

1. ***Aard en omvang***
   a. ***delictvormen:*** groei aanvallen; aantallen; van buitenaf of van binnenuit; motief aanvaller; aard aanval (misbruik internet door insider; ongeoorloofde toegang informatie); systeempenetratie van buiten; diefstal laptop; diefstal handhelds; diefstal andere hardware; Trojaans paard; virus/worm; onderschepping telecommunicatie; degradatie netwerk performance; denial of service; website defacement; sabotage data of netwerken; fraude telecommunicatie; identiteitsfraude; financiële fraude; ongeoorloofde privileges; diefstal vertrouwelijke informatie.
2. ***Melding- en aangiftegedrag en reactie:*** aan wie gerapporteerd; resultaat.
3. ***Schade***
   a. ***economische schade:*** financieel verlies per incident; totale kosten als gevolg van electronische aanvallen; criminaliteit en ongeoorloofd gebruik;

c. ***gedragschade:*** factoren die bijdragen aan kwetsbaarheid (in bedrijfsmanagement); meest problematische managementaspecten.

4. ***Preventieve maatregelen:*** vormen van veiligheidstechnologie; veiligheidbeleidsmaatregelen; gebruik van standaarden; uitgaven aan veiligheid: groei, beoordeling of het genoeg is; training en certificering.

De vragenlijst kon schriftelijk of via het internet worden ingevuld. De vragenlijst is verstuurd aan 2024 IT managers; de respons bedroeg 389, ofwel 17%. Tabel 13 geeft een overzicht van de aantallen vormen van computercriminaliteit die zijn gerapporteerd. Hieruit kan worden opgemaakt dat voor dit detailniveau van rapporteren het aantal respondenten van de enquête te laag was. Het beeld van de ontwikkeling in de schadeposten tussen 2003 en 2006 dat gegeven wordt in tabel 14 is dan ook voor de individuele schadebedragen zeer onbetrouwbaar. De uitbijter voor diefstal/inbraak vertrouwelijke gegevens in 2006 is voornamelijk toe te schrijven aan slechts één waarneming (op een totaal van 14) van $40.000.000. De trend van de oplopende gemiddelde schade per bedrijf is echter gebaseerd op grotere aantallen en daarmee wel geloofwaardig. De bedragen hebben betrekking op de bedrijven die gerapporteerd hebben en zijn niet noodzakelijk representatief voor Australië.

Tabel 13. Vormen van computercriminaliteit bij bedrijven 2003-2006, aantallen in de steekproef; bron: AusCERT(2006)

	2003	**2004**	**2005**	**2006**
Diefstal inbraak vertrouwelijke gegevens	7	8	1	14
Ongeautoriseerde toegang	10	7	3	14
Computer-gefaciliteerde financiele fraude	8	8	5	9
Diefstal en misbruik van klantgegevens	-	-	4	8
Telecommunicatiefraude	6	6	3	9
Sabotage van data of netwerken	3	3	2	7
Website defacement	8	2	5	13
Denial of service	16	15	15	15
Degradatie van netwerk performance	14	24	9	12
Onderscheppen telecommunicatie	1	1	1	0
Infectie virus, worm, trojaans paard	66	93	53	-
Virus, worm (self-progagating)	-	-	-	52
Trojaans paard, rootkit infectie (niet self propagating)	-	-	-	23
Diefstal laptop	82	84	56	142
Diefstal held-held computers	-	12	5	19
Diefstal van hardware of onderdelen	-	30	25	49
Binnendringen systeem door buitenstaander	7	6	0	10
Ongeautoriseerde toegang door insider	3	3	1	3
Insider misbruik van internet, e-mail of interne hulpbronnen	30	1	29	55

Tabel 14. Geschatte schadebedragen in de steekproef voor Australië ten gevolge van computercriminaliteit bij bedrijven 2003-2006, per jaar in AUS $; bron: AusCERT(2006).

	2003	2004	2005	2006
Diefstal/inbraak vertrouwelijke gegevens	258,000	1,340,000	50,000	40,126,100
Ongeautoriseerde toegang	322,000	68,000	3,200	161,003
Computer-gefaciliteerde financiële fraude	3,525,000	2,457,000	581,000	941,602
Diefstal en misbruik van klantgegevens	-	-	62,000	215,103
Telecommunicatiefraude	415,200	218,220	13,000	551,327
Sabotage van data of netwerken	125,000	134,000	3,050	22,001
Website defacement	58,500	3,000	112,000	74,702
Denial of service	397,300	378,000	8,943,000	120,503
Degradatie van netwerk performance	528,200	1,709,000	408,600	62,512
Onderscheppen telecommunicatie	4,000	5,000	1,500	0
Infectie virus, worm, trojaans paard	2,223,900	7,097,100	2,684,750	-
Virus, worm (self-progagating)	-	-	-	992,793
Trojaans paard, rootkit infectie (niet self propagating)	-	-	-	248,102
Diefstal laptop	2,258,183	1,484,244	1,220,500	2,267,203
Diefstal held-held computers	-	56,500	31,000	355,600
Diefstal van hardware of onderdelen	-	430,000	326,200	653,602
Binnendringen systeem door buitenstaander	151,000	311,000	0	313,002
Ongeautoriseerde toegang door insider	262,000	210,000	5,000	56,000
Insider misbruik van internet, e-mail of interne hulpbronnen	1,272,500	20,000	2,412,100	1,310,053
Totale jaarlijkse schade	11,800,783	15,921,064	16,856,900	48,471,208
Gemiddelde jaarlijkse schade	93,657	116,212	153,245	241,150

4.6 Nieuw Zeeland

In 2006 is in Nieuw Zeeland als onderdeel van de New Zealand Crime and Safety Survey (NZCASS) aan burgers een beperkt aantal vragen over criminaliteit gesteld via de computer of mobiele telefoon (Mayhew en Reilly, 2007). Het zijn

1. ***Aard en omvang***
   a. ***delictvormen:*** virussen, wormen of spyware; hacking; fraude bij kopen; confrontatie met een kwetsende internetpagina; bedreigende email; gebruik mobiele telefoon door ander; kwetsende telefoontjes of teksten; kwetsende plaatjes; diefstal of ongeoorloofd gebruik credit card of bank pas, ook leeghalen rekeningen en nieuwe rekeningen, leningen openen;
   b. ***risicokenmerken:*** bezit en frequentie gebruik computer en mobiele telefoon; gebruik credit card, bank pas.
2. ***Melding- en aangiftegedrag en reactie***: geen.
3. ***Schade***
   b. ***psychologische schade:*** zorgen over elektronische misdaad.

De vragen zijn face to face gesteld. Door de beperktheid van de vragenlijst riepen de antwoorden veel nieuwe vragen op. De validiteit van de vragen is niet gecheckt; daardoor was bijvoorbeeld onduidelijk of computers daadwerkelijk geïnfecteerd waren, of dat het beperkt bleef tot een melding van een virusscanner

Tabel 15. Slachtofferschappen burgers van 1 januari 2005 tot april 2006. Bron: NZCASS

slachtoffer van	**%**
Computer misbruik	
Computer is aangetast door een virus, een worm of spyware	53.1
In de computer is ingebroken zonder uw toestemming	5.9
Ik kwam onbedoeld materiaal op een webpagina tegen dat ik zeer kwetsend vond	15.2
Ik kreeg email waarin kwetsende of bedreigende dingen werden gezegd	10.4
U hebt via internet of per email iets gekocht waarbij u gelooft dat u het slachtoffer van fraude bent geworden	1.7
Misbruik mobiele telefoon	
Ik heb een telefoontje of tekstbericht gekregen waarin zeer kwetsende dingen werden gezegd	8.0
Ik heb een telefoontje of tekstbericht gekregen dat ik pesterig of bedreigend vond	5.3
Telefoongebruik door een ander voor een kwetsend doel	2.5
Ik kreeg een plaatje dat zeer kwetsend was	1.3
Tenminste één van bovenstaande	12.1

slachtoffer van	%
Identiteitsdiefstal	
Iemand heeft een credit card of bank card of rekeningnummer zonder toestemming met het doel te stelen	2.3
Iemand heeft zonder toestemming persoonlijke informatie gebruikt om credits cards of leningen te krijgen, een nieuwe rekening te openen of op een andere manier te frauderen	1.1
Tenminste één van bovenstaande	2.8

Een bedrijfsenquête is gehouden door de Alpha-Omega Group (Quinn, 2005). Hierin kwamen aan de orde:

1. ***Aard en omvang***
   a. ***delictvormen:*** aantal incidenten ongeautoriseerd gebruik; aard incidenten; insider misbruik; diefstal hardware; identiteitsdiefstal telecommunicatiefraude; denial of service; ongeautoriseerde toegang; hacking; informatiediefstal; financiële fraude; intellectuele diefstal, namaak.
2. ***Melding- en aangiftegedrag en reactie:*** acties n.a.v. incidenten: advocaten; politie; verandering proces; redenen om niet aan politie te rapporteren; follow up (strafrechtelijk); interne persoon aan wie incidenten gerapporteerd.
3. ***Schade***
   a***. economische schade:*** kosten per incident.
4. ***Preventieve maatregelen:*** IT budget dat aan veiligheid wordt besteed, als percentage, per werknemer; per organisatie; als uitkomst van een kosten-baten analyse; outsourcing; verzekering; beleidsplannen en actualiseren van deze plannen; niveau training veiligheidbewustzijn; veiligheidstechnologie in gebruik; procedures en beleid.

De respons bedroeg 218 personen. Hieronder volgt een selectie uit de rapportage.

Tabel 16. Aantallen gerapporteerde incidenten in de Nieuw-Zeelandse bedrijfsenquête

Incident	Aantal
Misbruik door insiders	235
Diefstal hardware	155
Indentiteitsdiefstal	85
Telecommunicatiefraude	72
Denial of service	38
Ongeautoriseerd gebruik/toegang	37
Hacking	36
Informatiediefstal	23
Financiele fraude	19
Product piraterij en vervalsing	16

Uit tabel 16 blijkt dat de Nieuw Zeelandse bedrijven vooral worden bedreigd door insiders. Misbruik staat bovenaan, en het ligt voor de hand dat insiders ook de meeste gelegenheid hebben tot diefstal. De aanvallen van buitenaf staan lager in de orde. Tabel 17 geeft een uitsplitsing per bedrijfstak naar de investering en de operationele kosten per werknemer in computerbeveiliging. Merk op dat bij een dergelijke fijne uitsplitsing de gegevens (bij slechts 156 respondenten) wel onbetrouwbaar moeten zijn. Desondanks ligt het voor de hand dat deze kosten in de financiële en technologische sector het hoogst zijn. De investering in de retailbranche is ook relatief hoog.

Tabel 17. Investering en kosten per werknemer aan computer veiligheid in NZ $

	Investering per werknemer	**Kosten per werknemer**
Financieel	94	272
Technologie	75	237
Nationale regering	51	114
Retail	94	51
Transport	11	46
Locaal bestuur	34	44
Anders	13	41
Onderwijs	93	31
Entertainment/media	31	26
Industrie	11	21
Medisch	9	8
Telecommunicatie	72	3

Tabel 18 laat zien dat veiligheidsbeleid vaak niet serieus wordt uitgevoerd en onderhouden. Net als in Nederland blijkt hier dat computerveiligheid mensenwerk is. Veel instrumenten bestaan niet bij de bedrijven, en als ze bestaan worden ze vaak niet serieus ingezet.

Tabel 18. Beleid en risico management instrumenten; percentages

	wordt gemonitord	**wordt regelmatig beoordeeld**	**wordt de hand aan gehouden**	**bestaat**
Risico management strategie	20	31	25	49
Business continuiteitsplan	35	51	40	75
Incident respons plan	17	22	23	38
Gebruik informatie management standards	13	20	27	38
Informatie veiligheid strategie	17	29	29	50
Strategisch informatie plan	23	59	40	81

4.7 Canada

In Canada is recentelijk een gedetailleerde enquête onder bedrijven opgestart, met een aanzienlijke nadruk op het omgaan met klanten die, bewust of onbewust, fraude plegen, de Survey of Fraud against Businesses. Er zijn aparte enquêtes voor banken, gezondheids- en invaliditeitsverzekering, schade- en ongevallenverzekering en retail. De inhoud van de vragenlijst voor retail is globaal:

1. ***Aard en omvang***
   a. ***delictvormen:*** fraude door niet-personeel (credit card, private label card; cheques; valse identiteit; valse informatie; vals geld; return fraude; valse rekeningen); fraude door personeel (misbruik van eigendommen, valse declaraties, financiële misleiding); phishing.
2. ***Melding- en aangiftegedrag en reactie:*** ondernomen acties; frequentie inschakelen politie; redenen om wel/niet politie in te schakelen; juridische actie.
3. ***Schade***
   a. ***economische schade:*** financiële schade; schade aan relaties; reputatie;
   b. ***psychologische schade:*** moraal bij personeel.
4. ***Preventieve maatregelen:*** preventieve maatregelen; mogelijke verbeteringen.

Van dit onderzoek zijn nog geen resultaten bekend. Ook zijn er geen publiek toegankelijke cijfers over slachtoffers van cybercrime bij burgers.

4.8 Conclusies

Er zijn fundamentele verschillen in ambitieniveau tussen de enquêtes in de verschillende landen. Deze hebben vooral te maken met het feit dat de meeste enquêtes onderdeel uitmaken van een reguliere slachtofferenquête, en daarin slechts een beperkte ruimte mogen innemen. Dit geldt met name voor de enquêtes onder burgers. De verschillen in inhoud zijn echter niet groot. Daarom ligt het voor de hand om de inhoud van een enquête in Nederland zo veel mogelijk te laten aansluiten bij wat er internationaal aan vragen beschikbaar is, waarbij zowel voor huishoudens als bedrijven de Verenigde Staten de kwalitatief meest hoogstaande basis vormen. Een probleem is echter dat de structuur en benamingen van het financiële systeem in de Verenigde Staten afwijken van die Nederland. Zo is het in de VS bijvoorbeeld mogelijk om iemands identiteit te misbruiken om aan een medische behandeling te komen.

De problematiek voor bedrijven is het meest complex, niet alleen omdat de ICT-systemen en de manieren van financieel-economische criminaliteit het meest geavanceerd zijn, maar ook omdat het probleem van beveiliging en bedrijfscultuur hier het meest lastig in kaart te brengen is. Een mogelijke oplossing hiervoor is om dit probleem dan maar te negeren, maar Syntens (2006) laat op overtuigende wijze zien dat hierin de bron van veel criminaliteit en de kostbare gevolgen ervan schuilt. De wijze waarop in de VS de vragenlijst is opgebouwd voor de bedrijvenenquête leidt ertoe dat veel relevante informatie toch boven tafel komt. Dit is een extra reden om de bedrijfsenquête in de VS als uitgangspunt voor Nederland te nemen.

5. Kwaliteit

Over de kwaliteit van de buitenlandse enquêtes in psychometrische zin is weinig bekend; betrouwbaarheden in termen van coëfficiënten (bijvoorbeeld Cronbach's alpha) zijn niet gemeten. Er zijn geen test-hertest experimenten uitgevoerd, dus kennen we ook geen test-hertest correlaties. Evenmin is er op bedrijfsniveau gekeken naar de plausibiliteit van longitudinale uitkomsten of zijn er andere toetsen uitgevoerd om de validiteit van gemeten uitkomsten te checken. In de Verenigde Staten is echter wel op een andere manier gekeken naar de validiteit van de vragen, namelijk door de enquête voorafgaand aan het veldwerk cognitief te testen. We geven twee voorbeelden, één uit de module voor identiteitsdiefstal uit de slachtofferenquête bij personen en één uit de bedrijfsenquête

Meest recente episode of identiteitsdiefstal
Drie versies van deze vraag zijn getest. In de eerste versie werd alleen vraag 45d gesteld.

45d. Welk type identiteitsdiefstal werd het meest recent ontdekt?
Vier respondenten waren met deze vraagversie geïnterviewd. Drie van de vier respondenten hadden problemen met de betekenis van de vraag. Toen hen gevraagd werd wat ze dachten dat de vraag betekende antwoordden drie van hen dat de vraag was welk incident het eerst gebeurde. Eén respondent antwoordde: geen diefstal gebeurde het eerst, het gebeurde allemaal omstreeks dezelfde tijd. De respondenten waren niet in staat om de vraag te beantwoorden in termen van "type identiteitsdiefstal". Ze antwoordden in termen van wat hen gedurende de diefstal was overkomen. Een respondent had (1) haar naam en (2) haar SOFI-nummer gebruikt om een nieuwe mobiele telefoonrekening te openen. Een ander had (1) geld gehaald van haar bankrekening en (2) een nieuwe credit kaart op haar naam geopend. In beide gevallen waren deze incidenten technisch twee verschillende "typen" identiteitsdiefstal. Maar voor beide respondenten waren de twee incidenten gerelateerd aan één specifieke gebeurtenis. Omdat de twee "typen" of incidenten vervlochten waren, konden de respondenten ze niet uit elkaar halen en aangeven wat als eerste gebeurde.

Mede op basis van de ervaringen met de twee andere versies werd de vraag uiteindelijk geherformuleerd als
45d. Was het misbruik van
- **de credit kaard rekening(en)**
- **andere bestaande rekeningen**
- **persoonlijke informatie of nieuwe rekeningen**

één identiteitsdiefstal of meer dan één identiteitsdiefstal
45e. Gebeurden deze diefstallen apart, of op hetzelfde moment?
45f. Welke identiteitsdiefstal werd als laatste ontdekt?

Hughes (2004)

Zijn in dit bedrijf incidenten ontdekt waarin een computer werd gebruikt voor verduistering tegen het bedrijf in 2004?
1 □ Ja **Hoe veel incidenten zijn ontdekt?**
_____ aantal
2 □ Nee

Commentaar:

> In het algemeen waren de definitie en de verwoording van de vraag geen probleem. Een grote verzekeringsmaatschappij was onzeker over de vraag of manipulatie van prijzen hieronder viel. De respondent kon zich de details van de gebeurtenis herinneren en dacht dat het onder de definitie van verduistering viel, maar wist het niet zeker. Uiteindelijk zei hij 'ja'. De enige andere respondent die 'ja' zei refereerde aan een frauduleuze order van 120 laptops. Hier stuurde de werknemer de laptops naar een opslagruimte waar hij ze vervolgens kon verkopen. De overige respondenten zeiden 'nee'. Er was onzekerheid of dit wel klopte. Acht van de 16 respondenten zeiden dat ze 'vermoedden van niet' of 'dat ze het nooit hadden gehoord'. Vijf bedrijven zeiden dat als het zou gebeuren ze dit niet in een onderzoek zouden zeggen.
>
> *Aanbevelingen:*
> Veel bedrijven kunnen zich ongemakkelijk voelen bij het rapporteren van dit soort informatie in een survey. Het lijkt erop dat de respondenten met de meeste IT-kennis niet op de hoogte zijn van dit soort zaken (verduistering en fraude). Een idee is om aparte vertrouwelijke websites met wachtwoord te creëren om dit soort informatie te verzamelen, maar daardoor zal het aantal onvolledig ingevulde vragenlijsten vermoedelijk toenemen. We bevelen in ieder geval aan om dit type vragen pas aan het eind van de vragenlijst te stellen omdat ze het meest gevoelig zijn.

(Sand e.a., 2005)

Beide geciteerde rapporten kunnen goed worden gebruikt als check bij het opstellen van de concrete vragenlijst. Daarnaast zijn voor de bedrijfsenquête uiteraard de ervaringen met de MCB (Monitor Criminaliteit Bedrijfsleven) relevant. Op een aantal vragen waar de ervaringen met MCB en een recent terrorisme-onderzoek relevant kunnen zijn gaf projectleider Robbert Zandvliet (TNS NIPO) de volgende antwoorden.

1. Kunnen we een voor dit onderwerp selectieve non respons verwachten? *Bij de MCB was dit nauwelijks het geval (non-respons brengt iets lagere schattingen voor delicten met zich mee). Zie paragraaf 4.1 in het handboek MCB 2007 (Zandvliet e.a., 2008).*

2. De kennis is zowel technisch als beleidsmatig. Kunnen we verwachten dat we daar meerdere personen in een bedrijf voor nodig hebben? Levert dat extra non respons op? Vereist dat extra doorlooptijd? *Bij MCB en genoemd terrorisme-onderzoek was deze kennis in voldoende mate voorhanden. Zaak is wel de juiste persoon aan de telefoon te krijgen. Bij de MCB vragen we naar degene die binnen de vestiging op de hoogte is van criminaliteit en veiligheid. Bij het terrorisme-onderzoek naar degene meest verantwoordelijk voor het veiligheidsbeleid.*

Dus extra non-respons niet zozeer, veel afspraken om de juiste persoon aan de telefoon te krijgen des te meer. Wat betreft technische kennis: dat ligt er natuurlijk maar net aan hoe technisch. Van een directeur mag je denk ik niet verwachten dat hij alle technische ins en outs op softwaregebied kent, maar wel genomen maatregelen tegen criminaliteit op een meer algemeen niveau.

3. Je vraagt om nogal wat vuile was buiten te hangen (bij de meeste bedrijven is de beveiliging, zeker waar het om menselijk gedrag gaat, bar en boos). Is men daartoe bereid? Hoe kun je de enquête het best 'verkopen' naar de respondenten? *Een brief vooraf helpt zeker (is gebleken bij MCB --> hogere respons). Daarin veel aandacht voor doel en privacywaarborging. Sporadisch hebben we te maken met geïrriteerde respondenten. Een helpdesk voor vragen van respondenten is ook een goed idee. Verder is men verrassend openhartig, zelfs over zaken als interne criminaliteit.*

4. Ik neem aan dat je deze enquête het beste op vestigingsniveau (i.p.v. bedrijfsniveau) kunt afnemen. Klopt dat*? In principe wel (MCB is op vestigingsniveau), ware het niet dat ik bij cybercrime*

mijn twijfels heb. MCB inventariseert veel maatregelen op vestigingsniveau (bijv. cameratoezicht, alarm etc. etc.), maar ik vermoed dat cybercrime en het bestrijden daarvan ingrepen op vestigingoverschrijdend niveau met zich meebrengt. Iets om rekening mee te houden

De conclusies van de overwegingen ten aanzien van kwaliteit zijn dat

- het voor personen lastig is om technisch de juiste antwoorden te geven
- de gevraagde informatie bij bedrijven zo heterogeen is dat deze bij grotere bedrijven vermoedelijk door meerdere personen moet worden gegeven; dit leidt veeleer tot vertraging dan tot verhoging van de non respons
- bereidheid om 'de vuile was buiten te hangen' in Nederland groter lijkt dan in de VS, maar het blijft wel een belangrijk aandachtspunt

Om tot een valide enquête te komen is een cognitieve test zeer waardevol. Vanwege het cultuurverschil, maar ook vanwege het verschil in idioom, is het niet te verwachten dat de resultaten uit de VS in dit opzicht volledig voorspellend zijn voor Nederland.

6. Opzet enquêtes

Voor het houden van een monitor bij burgers en bedrijven staan in beginsel meerdere methoden open. We bespreken hier vier mogelijke methoden en de implicaties voor de details van de dataverzameling. We gaan er daarbij van uit dat de bedrijvensteekproef steeds is gebaseerd op een gestratificeerde trekking uit het bedrijvenregister van de Kamer van Koophandel. De steekproef onder burgers hangt af van de gekozen methode.

a. *Face to face interviews*. Bij burgers kan het onderzoek gebaseerd zijn op een personensteekproef, bijvoorbeeld op basis van het bestand van Cendris, eventueel verrijkt door Experian met extra huishoudenkenmerken of een steekproef uit GBA verrijkt met kenmerken uit het SSB van het CBS Deze laatste methode wordt gebruikt bij de Veiligheidsmonitor Rijk (CBS, 2009). Zeker bij burgers garandeert de aanwezigheid van een interviewer de hoogste validiteit. De interviewer kan zich vergewissen dat de vragen goed worden begrepen (Loosveldt, 2008), iets dat bij het technische onderwerp niet vanzelfsprekend is. Bij de bedrijfsenquête is er het belangrijke nadeel dat, zeker bij grotere bedrijven, het nodig kan zijn dat verschillende personen elk voor een deel van de vragenlijst als respondent optreden. Wanneer deze niet volgtijdelijk beschikbaar zijn moet een interviewer meer dan één keer het bedrijf bezoeken. De kosten van deze aanpak zijn zowel bij bedrijven als burgers zeer hoog. De Veiligheidsmonitor Rijk wordt door het CBS voor een deel op deze manier uitgevoerd.

b. *Telefonische interviews*. Het trekken van een steekproef van burgers komt hier neer op het trekken van telefoonnummers. Hierbij worden reiskosten vermeden en wordt het management van afspraken softwarematig afgehandeld. De Veiligheidsmonitor Rijk wordt deels ook op deze manier uitgevoerd; ook de MCB wordt telefonisch gehouden. Telefonisch interviewen heeft dan ook aantrekkelijke kanten. Probleem is echter dat de vragen, of liever de lijsten met mogelijke antwoorden, voor computercriminaliteit en financieel-economische criminaliteit zo complex zijn dat ze via de telefoon niet voor te leggen zijn. Het is zeer

waarschijnlijk dat daardoor het eerst voorgelegde of het laatst voorgelegde alternatief relatief vaak wordt gekozen (Sykes en Collins, 1988). De complexiteit van de enquête maakt het wenselijk dat de respondent de mogelijke antwoorden voor zich ziet.

c. *Schriftelijk*. De steekproef van burgers is hier weer een adressensteekproef. Voordeel van een schriftelijke vragenlijst is dat het eerste contact maken met de respondent (via de post) weinig moeite kost. Schriftelijke vragenlijsten hebben echter een lage respons en de gelegenheid ontbreekt om aan non-respondenten een enkele vraag te stellen die kan worden gebruikt bij herweging. Daarnaast kan een hoge partiële non respons (niet of niet leesbaar ingevulde vragen) en een groot aantal routefouten worden verwacht (De Leeuw en Hox, 2008). Nadat de vragenlijsten zijn binnengekomen volgt bovendien een moeizame data-entry fase.

d. *Internet*. Voor burgers kan gebruik worden gemaakt van access panels. Dit zijn grote panels van respondenten die door marktonderzoekbureaus zijn geworven. Het grote nadeel van deze panels is dat ze niet op een steekproeftechnisch traceerbare manier zijn geworven en er dus getwijfeld kan worden aan de representativiteit van de uitkomsten. Daar staan echter wel voordelen tegenover. Van de panelleden is al veel informatie bekend, ook variabelen waarvan de landelijke verdeling bekend is en waar naar herwogen kan worden. Bedrijven zitten niet in zo'n access panel. Zij kunnen schriftelijk en telefonisch (eerst brief, dan nabellen) worden geworven, waarna ze via een toegangscode de vragenlijst kunnen invullen.

In onderstaande tabel worden de belangrijkste voor- en nadelen van de verschillende methoden opgesomd.

Methode	Voordelen	Nadelen
Face to face	Validiteit	Kosten; probleem indien meerdere personen respondent
Telefonisch	Steekproef management	Vragen ongeschikt
Schriftelijk	Organisatorische eenvoud	Kwaliteit invullen, hoge (partiële) non respons, data entry
Internet	Kosten	Representatief maken vergt inspanning

De kwalitatief beste methode is ongetwijfeld face to face onderzoek. Mogelijk loont het de moeite om aan onderzoekbureaus wel een offerte voor deze variant te vragen, maar de kans is zeer groot dat dit tot prohibitief hoge kosten leidt. De verwachting is daarom dat gekozen zal moeten worden voor methode d, het internet. De drie belangrijkste argumenten zijn

- prijs
- zichtbaarheid van lange lijsten met antwoordcategorieën
- automatische route

Voor burgers is de selectie eenvoudig, maar het zorgen voor de representativiteit van de uitkomsten, of voor een benadering daarvan, vergt ervaring en vakmanschap. Herwegen naar demografie zoals

leeftijd en geslacht zal eenvoudig zijn, maar dat maakt schattingen op basis van een access panel niet noodzakelijk representatief voor slachtofferschap van cybercrime. Verondersteld kan worden dat de vatbaarheid hiervoor voor leden van een access panel afwijkt van dat van de Nederlandse bevolking, bijvoorbeeld omdat ze meer online zijn. De crux is waarschijnlijk het toepassen van een weegfactor die samenhangt met het gebruik van de computer. Het is in de offertefase aan de bureaus om hiervoor met een passende oplossing te komen. Een uitweg die altijd werkt is het houden van een beperkte telefonische enquête die wel representatief is voor PC-gebruik, om zo aan enkele verdelingen te komen van cruciale variabelen om naar te herwegen. Voor een eerste meting ligt het voor de hand een steekproefomvang te kiezen die vergelijkbaar is met dat gedeelte van de Veiligheidsmonitor Rijk dat face to face wordt afgenomen (er wordt ook een gedeelte telefonisch afgenomen), dus een netto respons van bij benadering 5000. Daarbij wordt de eerstjarige van 15 jaar of ouder in een huishouden geïnterviewd.

Voor de bedrijfsenquête ligt de vergelijking met de Monitor Criminaliteit Bedrijfsleven voor de hand. Deze is echter telefonisch, op vestigingsniveau, afgenomen. In dit geval is telefonische afname onaantrekkelijk vanwege de complexiteit van de vragen en met name de antwoordcategorieën, maar ook vanwege het feit dat vaak meerdere respondenten binnen een bedrijf nodig zullen zijn om de enquête compleet in te vullen; het kan gaan om zowel ICT-specialisten als financiële specialisten als het algemeen management. Daarom stellen wij voor om voor de enquête zowel schriftelijk (een brief) als telefonisch uit te nodigen, en vervolgens per bedrijf een internetenquête aan te bieden. In beginsel wordt deze enquête op vestigingsniveau afgenomen. Er moet echter rekening mee worden gehouden dat met name ICT-informatie niet altijd per vestiging beschikbaar is. Daarom moet de mogelijkheid worden ingebouwd om ook informatie te geven over alle vestigingen heen. Om in de goede verhoudingen te kunnen wegen is dan wel de informatie nodig hoeveel vestigingen een bedrijf heeft.

Het is met name van belang de steekproef van bedrijven representatief te trekken naar omvang van het bedrijf, bijvoorbeeld door middel van stratificatie naar grootteklasse. De resultaten van de Amerikaanse NCSS suggereren dat prevalentie en incidentie niet sterk varieert per bedrijfstak. Telecommunicatie en IT bedrijven hebben de hoogste prevalentie (82%), bos- en landbouwbedrijven de laagste (44%), zie tabel 20. Ter vergelijking: de percentages bedrijven in de MCB die met diefstal te maken hadden liepen uiteen van 4% voor dienstverlening tot 27% voor detailhandel (Zandvliet e.a., 2008). De NCSS had een netto respons van 8079 bedrijven; bij de MCB was de netto respons 38.000. Gezien de veel minder extreme verdelingen van prevalenties die zich in de NCSS voordoen vergeleken met de MCB ligt het voor de hand om een respons van 8000 voor een eerste enquête als richtinggevend te beschouwen. Alleen met betrekking tot schadebedragen is er dan een zeker risico dat de varianties hoog zijn. Dit probleem kan worden omzeild door schadebedragen in klassen te presenteren (geen schade, tot €10.000, €10.000-€100.000, meer dan €100.000) , en niet een totaalbedrag te schatten.

Tabel 20. Prevalenties in de NCSS 2005.

	bedrijven		alle incidenten	
	n	% met computers	n	% met incidenten
Alle bedrijven	8,079	97%	7,636	67%
Kritieke infrastructuur	2,719	98%	2,610	67%
Landbouw	175	82	142	51
Chemie en farmaceutisch	201	98	192	73
Computer systeem design	170	100	167	79
Financieel	323	100	317	67
Gezondheid, zorg	423	100	410	67
Internet	135	100	132	66
Petroleum, mijnen	126	98	124	56
Media	218	100	212	71
Onroerend goed	175	97	167	65
Telecommunications	134	100	130	82
Transport	303	98	294	64
Nutsbedrijven	336	98	323	64
Hoogwaardig	1,737	97%	1,656	71%
Duurzame goederen	503	97	479	75
Niet duurzame goederen	327	99	319	72
Opname beeld en geluid	88	99	84	67
Retail	316	94	293	67
Wetensch. onderzoek	219	99	210	70
Groothandel	284	98	271	67
Midden	1,184	99%	1,140	67%
Accounting	176	100	173	55
Advertising	154	99	149	67
Architecture	214	97	204	70
MBO, HBO	190	95	177	72
Verzekeringen	269	100	263	69
Juridisch	181	99	174	69
Laag	2,439	94%	2,230	63%
Accommodaties	143	96	134	60
Administratief	255	98	239	65
Kunst en entertainment	198	96	181	62
Bouw	241	97	223	70
Voeding	212	88	186	54
Bosbouw, visserij, jacht	152	88	131	44
Management	190	93	150	59
Mijnen	272	94	170	65
Andere diensten	159	97	249	68
Verhuur	317	96	151	64
Sociale dienstverlening	132	92	299	66
Opslag	168	90	117	60

Bronnen

AusCERT, 2006, 2006 Australian computer crime and security survey.
http://www.auscert.org.au/images/ACCSS2006.pdf

Australian Bureau of Statistics, 2008, Personal Fraud.
http://www.ausstats.abs.gov.au/ausstats/subscriber.nsf/0/866E0EF22EFC4608CA2574740015D234/$File/45280_2007.pdf

Beck, J. en T. DeMaio, 2007, First Round Cognitive Pretesting on the Proposed Internet Predation Questions for the National Crime Victimization Survey: Results and Recommendations. Statistical Research Division, U.S. Bureau of the Census.
http://www.census.gov/srd/papers/pdf/ssm2007-20.pdf

British Crime Survey 2005/2006. Final Questionnaire
http://qb.soc.surrey.ac.uk/surveys/bcs/05mainqbcs.pdf

CBS, 2009, Veiligheidsmonitor Rijk, landelijke rapportage.
http://www.veiligheidbegintbijvoorkomen.nl/images/Veiligheidsmonitor%20Rijk%202008%20Landelijke%20rapportage_tcm62-172357.pdf

Van Dijk, J., J. van Kesteren en P. Smit, 2007, Criminal Victimisation in International Perspective. Key Findings from the 2004-2005 ICVS and EU-ICS. Onderzoek en Beleid nr. 257. Boom/WODC, Den Haag.
http://www.wodc.nl/onderzoeksdatabase/icvs-2005-survey.aspx?cp=44&cs=6798

Ernst & Young, 2009, ICT Barometer over ICT-beveiliging en cybercrime http://www.ict-barometer.nl/onderzoeksonderwerpen.php

EU-ICS (2005) European Crime and Safety SurveyFINAL DUTCH VERSION, 2005
http://www.europeansafetyobservatory.eu/files/EUICS_qfinalNL.pdf

Fafinsky, S. en N. Minassian, 2008, UK Cybercrime Report 2008. Garlik,
http://www.garlik.com/static_pdfs/cybercrime_report_2008.pdf

Flatley, J., 2007, Mobile phone theft, plastic card and identity fraud: Findings from the 2005/06 British Crime Survey. Home Office Statistical Bulletin 10/7.
http://www.homeoffice.gov.uk/rds/pdfs07/hosb1007.pdf

Hughes, K., 2004, Final Report of Cognitive Research on the New Identity Theft Questions for the 2004 National Crime Victimization Survey. Statistical Research Division, U.S. Bureau of the Census. http://www.census.gov/srd/papers/pdf/ssm2004-02.pdf

van der Hulst, R.C. en R.J.M. Neve, 2007, High-tech crime, soorten criminaliteit en hun daders, een literatuurinventarisatie. Onderzoek en Beleid 264, WODC, Den Haag.
http://www.wodc.nl/onderzoeksdatabase/1477a-high-tech-crime.aspx?cp=44&cs=6798

Kershaw, C., S. Nicholas en A. Walker, 2008, Crime in England and Wales 2007/08. Findings from the British Crime Survey and police recorded crime. http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/17_07_08_crime_statistics_200708.pdf

De Leeuw, E.D. en J.J. Hox, 2008, Self-Administered Questionnaires: Mail Surveys and Other Applications. In: E.D. de Leeuw, J.J. Hox en D.A. Dillman (eds.), International Handbook of Survey Methodology., blz. 239-262. Lawrence Erlbaum Associates, London

Levi, M., J. Burrows, M.H. Fleming en M. Hopkins, 2007, The Nature, Extent and Economic Impact of Fraud in the UK. Report for the Association of Chief Police Officers' Economic Crime Portfolio. http://www.acpo.police.uk/asp/policies/Data/Fraud%20in%20the%20UK.pdf

Loosveldt, G., 2008, Face-To-Face Interviews. In: E.D. de Leeuw, J.J. Hox en D.A. Dillman (eds.), International Handbook of Survey Methodology., blz. 201-220. Lawrence Erlbaum Associates, London

Mallinckrodt, H.H., 1980, Latijns-Nederlands woordenboek. Het Spectrum, Utrecht.

Mayhew, P. en J. Reilly, 2007, The experience of e-crime. Findings from the New Zealand Crime & Safety Survey 2006. New Zealand Ministry of Justice. http://www.justice.govt.nz/pubs/reports/2007/crime-safety-survey-2006/experience-of-e-crime/e-crime.pdf

McCarthy, B. en L.E. Cohen, 2008, Economic Crime: Theory - Classical Approach To Crime, Neoclassical Or Economic Approach, Advantages Of The Neoclassical Approach, Problems With The Neoclassical Approach. http://law.jrank.org/pages/1055/Economic-Crime-Theory.html#ixzz0LyoxuSNq

Newman, G.R. en M.M. McNally, 2005, Identity theft literature review. Paper Prepared for presentation and discussion at the National Institute of Justice Focus Group Meeting to develop a research agenda to identify the most effective avenues of research that will impact on prevention, harm reduction and enforcement. http://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf

Oudejans, M. en C. Vis, 2008, Slachtoffers van (poging tot) oplichting. Onderzoek onder burgers in Nederland. CentERdata, Tilburg. http://www.wodc.nl/onderzoeksdatabase/onderzoek-naar-slachtoffers-van-oplichting-onder-personen.aspx

Podgor, E.S., 1999, Criminal Fraud, American Universities Law Review 48 no. 4, blz. 729-768.

Quinn, K.J.S., 2005, New Zealand Computer Crime and Security Survey. Alpha-Omega Group, Dunedin. http://eprints.otago.ac.nz/342/1/2005_CC%26SS_Report_Distributiuon_Version.pdf

RAND, 2005, The National Computer Security Survey (NCSS). Final Methodology http://www.rand.org/pubs/technical_reports/2008/RAND_TR544.pdf

Richardson, R., 2008, CSI Computer Crime & Security Survey. http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf

Sand, K.L., S.J. Cotton, R. Anderson, D. Golinelli, R. Lewis en L. Davis, 2005, The National Computer Security Cognitive Interviewing Report. RAND Corporation.

Statistics Canada, 2007a, Vragenlijst Survey of Fraud against Businesses, banken.
http://www.statcan.gc.ca/imdb-bmdi/instrument/5133_Q1_V2-eng.pdf

Statistics Canada, 2007b, Vragenlijst Survey of Fraud against Businesses, gezondheids- en invaliditeitsverzekering
http://www.statcan.gc.ca/imdb-bmdi/instrument/5133_Q3_V1-eng.pdf

Statistics Canada, 2007c, Vragenlijst Survey of Fraud against Businesses, schade- en ongevallenverzekering
http://www.statcan.gc.ca/imdb-bmdi/instrument/5133_Q4_V1-eng.pdf

Statistics Canada, 2007d, Vragenlijst Survey of Fraud against Businesses, retail
http://www.statcan.gc.ca/imdb-bmdi/instrument/5133_Q2_V1-eng.pdf

Sykes, W. en M. Collins, 1988, Effects of mode of interview: experiments in the UK. In: R.M. Groves, P.P. Biemer, L.E. Lyberg, J.T. Massey, W.L. Nicholls en J. Waksberg (eds.), Telephone Survey Methodology, blz. 301-320. Wiley, New York.

Syntens, 2006, Eindrapportage nulmeting in het kader van het MKB-experiment van het Nationaal Project Aanpak Cybercrime, uitgevoerd door Syntens in opdracht van Digibewust.
http://www.samentegencybercrime.nl/UserFiles/File/Eindrapport%20nulmeting%20NPAC%20MKB%20experiment%20definitief.doc

Willemsen, F, 2008, Startnotitie Voorbereiding nulmeting FINEC & CYBER. WODC, Den Haag.

Wilson, D, A. Patterson, G. Powell en R Hembury, 2006, Fraud and technology crimes. Findings from the 2003/04 British Crime Survey, the 2004 Offending, Crime and Justice Survey and administrative sources. Home Office Online Repost 09/06.
http://www.homeoffice.gov.uk/rds/pdfs06/rdsolr0906.pdf

Zandvliet, R., E. van de Loo en T. van Dijk, 2008, Handboek MCB 2007. TNS NIPO, Amsterdam,

*www.wodc.nl/images/**Handboek**%20**MCB**%20**2007**_tcm44-112925.pdf*

BIJLAGE 1. VRAGENLIJST BURGERS

Voor de huishoudenenquête Finec & Cyber bestaat er geen goed buitenlands voorbeeld. Wanneer er naar (onderdelen van) Finec & Cyber wordt gevraagd betreft dit steeds modules uit een vragenlijst die groter is, bijvoorbeeld een algemene slachtofferenquête of een arbeidskrachtentelling. De hier beschreven vragenlijst is daarom grotendeels nieuw ontworpen; voor een beperkt aantal vragen is gebruik gemaakt van Amerikaanse voorbeelden uit de vragenlijst over identiteitsdiefstal. Deze vragen zijn aangegeven met **[VS]**.
In de huidige vragenlijst zijn sommige bekende consumentenklachten niet meegenomen:

- oplichting als toerist, wisseltrucs
- namaakproducten, -merken
- bewust verkeerde voorlichting in winkels
- ondeugdelijke reparaties, gebruik ondeugdelijke materialen

Demografie: wordt bekend verondersteld (uitgaande van ondervraging van internetpanel)

- samenstelling huishouden
    - aantal personen in het huishouden (uitwonenende kinderen niet meerekenen)
    - gezinssituatie (alleenstaand, gehuwd, samenwonend, eenoudergezin, overig)
- per lid huishouden (indien van toepassing: ook kinderen)
    - leeftijd
    - geslacht
    - bezigheid (school, betaald werk, gepensioneerd, anders)
- opleiding hoofd huishouden
- inkomen huishouden
- provincie, stedelijkheid en urbanisatiegraad

Als respondent wordt gekozen de eerstjarige van 15 jaar of ouder

Indien het aantal personen in het huishoudenouder dan 11 jaar > 1

In het vervolg worden soms ook vragen gesteld over andere personen in het huishouden dan u. Kunt u invullen met welke namen we deze personen moeten aangeven
persoon 1: uzelf (ingevuld)
persoon 2 (<geslacht><leeftijd>: …
persoon 3 (<geslacht><leeftijd>: …
……..

Subjectieve veiligheid

p1. Hieronder volgt een aantal uitspraken over de veiligheid van omgaan met computers en elektronisch betalen. Kunt u aangeven in hoeverre u het met deze uitspraken eens bent.

1. Ik maak me vaak zorgen dat ik een door virus op mijn PC schade oploop
2. Soms ben ik bang dat indringers via het internet mijn PC misbruiken

3. Ik vind het eng om via de PC betalingen te doen
4. Ik vind betalen met een credit card via de PC niet veilig
5. Ik vind betalen met een credit card in een restaurant of winkel niet veilig
6. Ik probeer zo veel mogelijk te vermijden dat anderen via het internet kunnen zien wie ik ben
7. Zonder het internet zou mijn leven nu een stuk moeilijker zijn
8. Ik vind het een griezelig idee dat ik zo afhankelijk ben van het internet.

Antwoordcategorieën: helemaal niet mee eens, niet mee eens, niet mee oneens niet mee eens, mee eens, helemaal mee eens

Bezit, gedrag

In deze enquête wordt een groot aantal vragen gesteld over het gebruik en de risico's van computers. Al deze vragen gaan over privégebruik.

p2. Hoeveel desktop computers zijn in uw huishouden aanwezig? …
p3. Hoeveel laptop computers zijn in uw huishouden aanwezig? …
p4. Met hoeveel van deze computers maken u of uw huisgenoten verbinding met het internet? …
p5. Beschikt u thuis over een draadloos netwerk? ja/nee
Indien ja
p6. Kunnen anderen zonder wachtwoord gebruik maken van dit netwerk? ja/nee

p7. In onderstaande tabel staat een aantal dingen genoemd die mensen op de computer kunnen doen. Kunt u aangeven hoe vaak u en uw huisgenoten deze dingen doen. Als u het van uw huisgenoten niet precies weet, schat u het dan zo goed mogelijk in. De antwoordmogelijkheden zijn: 0: nooit; 1: incidenteel; 2: minstens 1 x per maand; 3: minstens 1 x per week; 4: dagelijks

	uzelf	persoon 2	persoon 3	.....
mailen				
chatten				
informatie zoeken				
nieuwsgroepen				
[VS] via de computer kopen				
internetbankieren				
bezoeken van sociale websites zoals Hyves, MySpace, Facebook of LindedIn				
spelletjes				
downloaden van tekst				
downloaden van software				
downloaden van audio/videobestanden				
afspelen van audio/videobestanden				
telewerken op het netwerk van uw werkgever				
eigen website bewerken				
eigen weblog schrijven				

Indien 'uzelf via de computer kopen'=0: naar p9

p8. Welke methoden van betalen gebruikt u als u iets online koopt (meer dan één antwoord mogelijk)?

- Ideal
- Credit card
- Paypal
- Anders, namelijk …

p9. Maakt u wel eens gebruik van een credit card om buiten het internet om dingen te betalen? ja/nee

Indien p9=ja:

p10. Hoe vaak gebruikt u uw credit card buiten het internet om? incidenteel/wekelijks/dagelijks

Aard en omvang

Er zijn verschillende manieren waarop criminelen en andere kwaadwillende mensen misbruik kunnen maken van uw computer. Hieronder volgt een lijst met een aantal mogelijke problemen. Aan u de vraag of u deze de afgelopen 12 maanden heeft ervaren.

Bij elk van de genoemde incidenten: ja/nee

Zo ja: hoe vaak (in de afgelopen12 maanden).

m1. U bent bestanden op uw computer kwijtgeraakt door virussen (alleen invullen wanneer de virusscanner alarm sloeg)

m2. Uw computer werkte ongewoon traag door ingrijpen door onbekenden vanaf het internet

m3. Uw programma's werken niet meer als gevolg van virussen(alleen invullen wanneer de virusscanner alarm sloeg)

m4. Iemand gebruikte zonder uw toestemming via het internet uw computer

m5. U kreeg zo veel spam (ongewenste e-mail) dat uw mailbox onbruikbaar werd

m6. Na een verzoek per e-mail hebt u een voorschot betaald en daar niets voor terug gehad

m7. U hebt een aankoop via het internet gedaan en het product niet gekregen

m8. U bent op het internet op een andere niet legale manier geld kwijtgeraakt

Indien m8<>ja: naar m9

m8a. Welke manier? (open)

m9. U hebt per e-mail drugs aangeboden gekregen.

Indien m9<>ja: naar m10

m9a. Bent u daarop ingegaan? ja/nee

m10. U hebt per e-mail andere verboden artikelen (dan drugs) aangeboden gekregen

Indien m10<>ja: naar m11

m10a. Bent u daarop ingegaan? ja/nee

m11. U hebt per e-mail medicijnen aangeboden gekregen.

Indien m11<>ja: naar m12

m11a. Bent u daarop ingegaan? ja/nee

Indien m11a<> ja: naar m12

m11b. Werkten de medicijnen? ja/nee

m12. Men heeft u via het internet proberen te werven voor een terroristische of extremistische organisatie

m13. Men heeft geprobeerd u af te persen door te dreigen compromitterende foto's of teksten via het web te verspreiden

m14. Men heeft geprobeerd via het internet u te discrimineren of haat tegen u te zaaien

m15. Men belasterde u en roddelde over u via het internet (zonder u persoonlijk aan te spreken)

De volgende vragen gaan niet alleen over problemen via het internet, maar ook per SMS of mobiele telefoon. Is het volgende het afgelopen 12 maanden in uw huishouden gebeurd?

m16. U of een van uw huisgenoten werd bedreigd via het internet, e-mail, SMS of mobiele telefoon.

m17. U of een van uw huisgenoten werd gepest via het internet, e-mail, SMS of mobiele telefoon.

m18. U of een van uw huisgenoten werd gestalkt (achtervolgd) via het internet, e-mail, SMS of mobiele telefoon.

m19. Iemand in uw huishouden heeft via het internet, e-mail, SMS of mobiele telefoon contact gehad met een volwassene die zich veel jonger voordoet dan hij/zij is.

m20. U of een van uw huisgenoten werd onvrijwillig geconfronteerd met kinderporno via het internet, e-mail, SMS of mobiele telefoon.

m21. U of een van uw huisgenoten werd onvrijwillig geconfronteerd met ander kwetsend materiaal (dan kinderporno) via het internet, e-mail, SMS of mobiele telefoon.

Dan volgt nu een aantal vragen over misdrijven die via het internet, maar ook op een andere manier kunnen plaatsvinden.

m22. Men heeft iemand uit uw huishouden de afgelopen 12 maanden geprobeerd te werven voor kinderporno

m23. Men heeft iemand uit uw huishouden de afgelopen 12 maanden geprobeerd te werven voor illegale loterijen

m24. Men heeft iemand uit uw huishouden de afgelopen 12 maanden geprobeerd te werven voor een piramidespel

m25. Men heeft iemand uit uw huishouden de afgelopen 12 maanden geprobeerd te werven voor kettingbrief

m26. Men heeft geprobeerd u een financieel advies aan te praten(bijvoorbeeld om bepaalde aandelen te kopen)

m27. Men heeft aan u spooknota's verstuurd (rekeningen voor producten die u nooit heeft gekocht)

m28. Bouw-, taxatiefraude: men heeft geprobeerd u te veel laten betalen voor onroerend goed door malafide praktijken

m29. Corruptie in Nederland: u moest mensen die daar geen recht op hebben geld geven om iets gedaan te krijgen: overheid, douane, politie, anderen (NB. corruptie in het buitenland telt hier niet mee).

De volgende vragen gaan over het misbruiken van uw identiteit, uw persoonlijke gegevens.

m30. Heeft iemand de afgelopen 12 maanden per e-mail wel eens om persoonlijke gegevens gevraagd zoals rekeningnummers, PIN-codes en wachtwoorden?
Indien m30<>ja: naar m31

m30a. Bent u daar wel eens op ingegaan? ja/nee

m31. Bent u op een website de afgelopen 12 maanden wel eens om persoonlijke gegevens gevraagd zoals rekeningnummers, PIN-codes en wachtwoorden (die niet bedoeld waren om tot die website toegang te krijgen)?

Indien m31<>ja: naar m32

m31a. Bent u daar wel eens op ingegaan? ja/nee

m32. Heeft iemand de afgelopen 12 maanden zonder uw toestemming uw credit card gegevens gebruikt om betalingen te doen?

m33. Heeft iemand de afgelopen 12 maanden zonder uw toestemming geld van uw bankrekening afgehaald?

m34. Heeft iemand de afgelopen 12 maanden uw persoonlijke informatie gebruikt om daarmee een nieuwe rekening te openen, bijvoorbeeld voor een lening, een credit card of een mobiele telefoon?

Indien m34<>ja: naar m35

m34a. Wat voor rekening? (open)

m35. Heeft iemand de afgelopen 12 maanden uw persoonlijke informatie gebruikt voor andere frauduleuze doelen, zoals het krijgen van een uitkering, het huren van een huis of het geven van valse informatie aan de politie.

Indien m35<>ja: naar m36

m35a. Wat voor doelen? (open)

m36. Is van u de afgelopen 12 maanden wel eens een laptop computer gestolen?

m37. Is van u de afgelopen 12 maanden wel eens een mobiele telefoon gestolen?

m38. Is de afgelopen 12 maanden wel eens uw rijbewijs gestolen?

m39. Is de afgelopen 12 maanden wel eens uw paspoort gestolen?

Tekstvariabele

@de laatste keer = <leeg> indien het incident 1 maal heeft plaatsgehad
"de laatste keer" indien het incident meerdere malen heeft plaatsgehad

Indien m32=ja (credit card fraude)

p11. Op welke manier is men *@de laatste keer* aan de gegevens van uw credit card gekomen?

- ik weet het niet
- door mijn credit card te stelen
- door bij een betaling via het internet mijn gegevens te kopiëren
- door bij een fysieke betaling met mijn credit card mijn gegevens te kopiëren
- doordat de dader een bekende was die toegang tot mijn gegevens had
- anders, namelijk ...

Indien m33=ja (bankrekeningfraude)

p12. Op welke manier is men *@de laatste keer* aan de benodigde gegevens van uw bankrekening gekomen?

- ik weet het niet
- door de gegevens van mijn PINpas bij een PINautomaat te lezen (skimmen)
- door mij via het internet te bespioneren of op mijn computer in te breken
- doordat de dader een bekende was die toegang tot mijn gegevens had

- anders, namelijk …

Indien m34=ja of m35=ja (misbruik persoonlijke informatie)
p13. Op welke manier is men *@de laatste keer* aan uw persoonlijke informatie gekomen die vervolgens is misbruikt?

- ik weet het niet
- doordat mijn paspoort of rijbewijs is gestolen
- door mij via het internet te bespioneren of op mijn computer in te breken
- doordat de dader een bekende was die toegang tot mijn gegevens had
- anders, namelijk …

Aangiftegedrag (alleen voorgevallen misdrijven)

Voor verschillende vormen zijn ook verschillende soorten reacties van toepassing. Dus niet alle vragen worden bij alle vormen gesteld; @de laatste keer is een tekstvariabele die leeg is wanneer het misdrijf de afgelopen 12 maanden slechts één keer is voorgevallen.

Voor alle ondervonden misdrijven (m1 t/m m39)

p14. **[VS]** Hebt u *@de laatste keer* hiervan aangifte gedaan bij de politie? ja/nee

Indien p14=nee:

p15. **[VS]** Waarom hebt u geen aangifte gedaan? (*meer dan één antwoord mogelijk*)

- ik wist niet dat ik dit bij de politie kon aangeven
- ik heb geen schade geleden
- ik heb het ergens anders aangegeven
- ik heb het zelf afgehandeld
- ik dacht niet dat de politie iets zou doen
- ik wilde de politie er niet mee lastig vallen/niet belangrijk genoeg
- ik ontdekte het misdrijf te laat nadat het gebeurde
- ik kon de politie geen nuttige informatie geven
- ik was bang om het aan te geven
- de dader was een vriend of familielid die ik niet in moeilijkheden wilde brengen
- ik geneerde me
- kwam slecht uit/ik wilde de tijd er niet voor nemen
- anders namelijk …

naar p23

Indien p14= ja:

p16. Vond de politie het een zaak voor hen? ja/nee

Indien p16<>ja: naar p23

Indienp16= ja:

p17. **[VS]** Heeft de politie rapport opgemaakt? ja/nee

p18. Heeft de politie voor u merkbare pogingen gedaan de dader op te sporen? ja/nee

p19. Heeft de politie de dader opgespoord? ja/nee/de dader is wel opgespoord maar niet door de politie
Indien p19=nee: naar p22

Indien p19<>nee:
p20. **[VS]** Was de dader een bekende van u? ja/nee
Indien p20<>ja: naar p22
Indien p22=ja:
p21. **[VS]** Wat is uw relatie tot de dader?
- (ex-)partner
- (stief-)ouder
- broer of zus
- (stief-)kind
- ander familielid
- (ex-)vriend of vriendin
- buren
- collega
- iemand die in mijn huis werkt (oppas, schoonmaker, elektriciën e.d.)
- een verkoper
- een andere bekende

p22. **[VS]** Hoe tevreden bent u met de afhandeling door de politie?
- zeer ontevreden
- ontevreden
- niet tevreden, niet ontevreden
- tevreden
- zeer tevreden

Oplossen problemen

Voor de misdrijven m1, m2, m3, m4, m5, (virussen, malware):

p23. Welke stappen heeft u *@de laatste keer* gezet om het probleem op te lossen? (*meer dan één antwoord mogelijk*)
- contact opgenomen met uw internetprovider
- contact opgenomen met uw computerleverancier
- een computer reparatiebedrijf ingeschakeld
- van internet software gekocht/gedownload
- geen van deze

Voor elk van de gekozen opties:
p24. Heeft …. voor een duurzame oplossing van het probleem kunnen zorgen? ja/nee

p25. Hoe lang duurde het voordat de schade was hersteld?
- 1 dag
- 2-7 dagen

- tussen een week en een maand
- langer dan een maand

Voor de misdrijven m32, m33, m34 (identiteitsdiefstal met financiële consequenties)
p26. Hebt u *@de laatste keer* contact opgenomen met de betrokken bank? ja/nee
p27. Is alle opgelopen schade door de bank vergoed

- nee, helemaal niet, de schade is voor mij
- nee, maar ik ben tegen de schade verzekerd
- ja, gedeeltelijk
- ja, helemaal

p28. Heeft de bank een rol gespeeld bij het opsporen van de dader

- nee, de dader is niet opgespoord
- nee, de dader is opgespoord, maar de bank staat daarbuiten
- ja, de bank heeft een rol gespeeld

Voor alle ondervonden misdrijven (m1 t/m m39)
p29. Hebt u gebruik gemaakt van juridische bijstand?

- nee
- ja, een onbetaald bureau voor rechtshulp
- ja, betaalde juridische bijstand

Schade (alleen voorgevallen misdrijven)

Voor verschillende vormen zijn ook verschillende soorten schade van toepassing. Dus niet alle vragen worden bij alle vormen gesteld.

a. economische schade

p30. **[VS]** Welke kosten hebt u *@de laatste keer* als gevolg van … gemaakt aan

1. betalingen aan personen die daar geen recht op hadden of die u misleid hebben
   (m6, m11, m13, m23, m24, m25, m26, m27, m28, m29)
2. diefstal (die niet is vergoed)
   (m32, m33, m34, m35, m36, m37, m38, m39)
3. herstel computer door een betaalde professional
   (m1, m2, m3, m4, m5, m32, m33)
4. kopen van nieuwe hardware of software
   (m1, m2, m3, m4, m5, m32, m33)
   - niets
   - een bedrag, namelijk … Euro

Voor m1, m2, m3, m4, m5, m16, m17, m18, m19, m20, m21 (virussen, malware, onvrijwillige confrontatie)
p31. **[VS]** Welke extra kosten hebt u *@de laatste keer* gemaakt voor de beveiliging van uw computer in de toekomst?

- niets

- een bedrag, namelijk … Euro

Voor m1, m2, m3, m4, m5, m16, m17, m18, m19, m20, m21
p32. Heeft *@de laatste keer* … ertoe geleid dat u dagen van uw werk vrij moest nemen? ja/nee
Zo ja:
p33. Hoeveel dagen?

Voor m13, m14, m15 (chantage, haat zaaien, roddelen)
p34. Heeft *@de laatste keer* … geleid tot problemen op uw werk? ja/nee
Zo ja:
p35. Wat voor problemen? (open)

b. psychologische schade

Voor alle misdrijven

p36. Heeft *@de laatste keer* … uw gevoel van welbevinden aangetast, of deed het u niets?
- ja, ik voelde me er minder prettig onder
- nee, het deed me weinig of niets

Indien p36<>ja: naar p38

Indien p36= ja:
p37. **[VS]** Waarin uitte zich dat? (*meer dan één antwoord mogelijk*)
- bezorgd, ongerust zijn
- woede
- depressief/verdrietig zijn
- je kwetsbaar voelen
- je in je privacy aangetast voelen
- het gevoel dat je anderen niet kunt vertrouwen
- slecht slapen
- hoofdpijn
- snel afgeleid zijn, slecht functioneren
- geïrriteerd zijn, snel ruzie krijgen
- je onveilig voelen
- gebruik van medicijnen
- professionele medische of psychologische hulp

c. subjectieve veiligheid

Voor m1 t/m m5, m12 t/m m21, m30 t/m m35.

p38. Is … voor u een reden geweest om
1. het internet minder te gaan gebruiken? ja/nee

2. niet naar sites gaan waar u vroeger graag kwam? ja/nee

p39. Heeft … ertoe geleid
1. dat er nu meer spanningen in uw privéleven zijn? ja/nee
2. dat u slechter functioneert op uw werk? ja/nee

Voorlichting en preventie

p40. Over welke beveiligsingssoftware beschikt uw huishouden?

	nee	sommige computers	alle computers	weet niet
spamfilter (tegen ongewenste e-mail)				
firewall (tegen hackers, inbrekers)				
virusbeveiliging (tegen programma's die gegevens wissen of veranderen, of die uw gedrag op de computer bespioneren)				

indien spamfilter op sommige computers:
@op de computers waarop een spamfilter is geïnstalleerd=' op de computers waarop een spamfilter is geïnstalleerd'
anders: @op de computers waarop een spamfilter is geïnstalleerd=leeg

indien firewall op sommige computers:
@op de computers waarop een firewall is geïnstalleerd=' op de computers waarop een firewall is geïnstalleerd'
anders: @op de computers waarop een firewall is geïnstalleerd=leeg

indien virusbeveiliging op sommige computers:
@op de computers waarop een virusbeveiliging is geïnstalleerd=' op de computers waarop een virusbeveiliging is geïnstalleerd'
anders: @op de computers waarop eenvirusbeveiliging is geïnstalleerd=leeg

Indien spamfilter aanwezig
p41. Staat het spamfilter altijd aan *@op de computers waarop een spamfilter is geïnstalleerd?*
- altijd
- meestal
- meestal niet
- nooit

Indien firewall aanwezig
p42. Staat de firewall altijd aan *@op de computers waarop een firewall is geïnstalleerd?*
- altijd
- meestal
- meestal niet
- nooit

Indien virusbeveiliging aanwezig

p43. Staat de virusbeveiliger altijd aan *@op de computers waarop een virusbeveiliging is geïnstalleerd?*

- altijd
- meestal
- meestal niet
- nooit

p44. Worden op de computers in uw huishouden regelmatig systeemscans uitgevoerd? (dan checkt een programma alle files en bekijkt of alles nog naar behoren functioneert)

- nee, op geen enkele computer
- op sommige computers
- op alle computers

p45. Worden binnen uw huishouden regelmatig back-ups (reservekopieën) van de gegevensbestanden gemaakt?

- nee
- van sommige computers
- van alle computers

Indien p45=nee: naar p47

Indien p45<> nee:

p46. Waar worden de back-ups (reservekopieën) bewaard? (*meer dan één antwoord mogelijk*)

- op het internet
- op een externe harde schijf
- op een daarvoor bestemde computer
- anders, namelijk …

p47. Verandert u met enige regelmaat uw wachtwoorden bij websites waar u moet inloggen, zoals banken, sociale websites, de belastingdienst, betaalde websites e.d.

- nee, ik verander mijn wachtwoorden nooit, tenzij ik ertoe wordt gedwongen
- incidenteel, maar ik denk er vaak niet aan
- ja, ik verander bewust regelmatig mijn wachtwoorden

p48. Gebruikt u op websites waar u moet inloggen steeds dezelfde wachtwoorden

- nee, voor elke website kies ik een ander wachtwoord
- soms, voor een aantal websites kies ik hetzelfde wachtwoord, maar niet voor alle websites
- ja, als dat kan kies ik altijd hetzelfde wachtwoord

p49. Hebt u een computer waarbij u met een wachtwoord moet inloggen? ja/nee/weet niet

Indien p49= ja:

p50. Wanneer u inlogt doet u dat dan gewoonlijk als gewoon gebruiker of als administrator? gebruiker/administrator/weet niet

Indien meerpersoonshuishouden: naar p52
Indien eenpersoonshuishouden:

p51. Zijn er anderen die het wachtwoord kennen waarmee u op uw computer inlogt? ja/nee

naar p57

Indien meerpersoonshuishouden:

p52. Hebben anderen in uw huishouden computers waarbij met een wachtwoord moet worden ingelogd? ja/nee
Indien p52=nee en p49=nee: naar p55

Indien p52=ja of p49=ja:

p53. Kent u binnen het huishouden elkaars wachtwoorden? ja/nee/ten dele

p54. Zijn er mensen buiten het huishouden die wachtwoorden van computers binnen het huishouden kennen? ja/nee/weet niet

p55. Is beveiliging van computers een gespreksonderwerp binnen het huishouden?
- nee, daar hebben we het nooit over
- ja, incidenteel
- ja, daar denken we samen goed over na

p56. Is veilig gedrag op het internet een gespreksonderwerp binnen het huishouden?
- nee, daar hebben we het nooit over
- ja, incidenteel
- ja, daar denken we samen goed over na

p57. Hoe komt u aan kennis over beveiliging van computers?
(meer dan één antwoord mogelijk)
- van de computerleverancier
- van de internetprovider
- uit de krant
- van het internet
- van familie, vrienden en kennissen
- van collega's op het werk
- van professionele deskundigen
- anders, namelijk …

p58. Hoe komt u aan kennis over veilig gedrag op het internet?
(meer dan één antwoord mogelijk)
- van de computerleverancier
- van de internetprovider
- uit de krant
- van het internet
- van familie, vrienden en kennissen

- van collega's op het werk
- van professionele deskundigen
- anders, namelijk …

Voor de incidenten m1 t/m m5, m16 t/m m21

p59. Wat had … kunnen voorkomen? (*meer dan één antwoord mogelijk*)

- virusscanner (beter) gebruiken
- meer discipline bij systeemscan
- meer discipline bij maken back-ups
- meer discipline bij gebruik wachtwoorden
- wachtwoorden niet aan derden vertellen
- meer kennis over wat cybercriminelen doen
- minder blootgeven op sociale netwerk sites als Hyves, Myspace, Facebook en LinkedIn
- een deskundige inschakelen bij beveiliging
- anders, namelijk …

Ter vergelijking: aangiftemodule in het slachtofferonderdeel in POLS

Deze module is onderdeel van de 'reguliere' slachtofferenquête, maar staat zo ver van het onderwerp Finec & Cyber af dat besloten is deze niet over te nemen.

```
1 Is dit voorval bij de politie bekend ?
   - ja 1 -> 2
   - nee 2 -> einde onderwerp
   - weigert / weet niet 8/9 -> einde onderwerp

2 Heeft U zelf of iemand anders het voorval bij de politie gemeld of is het
door de politie zelf ontdekt ?
   - O.P. heeft melding gedaan 1 -> 3
   - iemand anders heeft melding gedaan 2 -> 3
   - het is door de politie zelf ontdekt 3 -> 5
   - weigert / weet niet 8/9 -> einde onderwerp

3.Hoe heeft U of die persoon toen contact opgenomen met de politie:
Was dat telefonisch, op het politiebureau of bij een agent op straat ?
   - telefonisch 1
   - op het politiebureau 2
   - bij een agent op straat 3
   - anders 4
   - weigert / weet niet 8/9

4 Heeft U of die persoon contact opgenomen met de politie in Uw eigen buurt
of woonplaats of was dat elders ?
   - eigen buurt of wijk 1
   - elders in de woongemeente 2
   - elders in Nederland 3
   - in het buitenland 4
   - weigert / weet niet 8/9
5 Heeft u (of degene die het heeft gemeld) een document getekend, zoals een
aangifteformulier, aangiftekaart of een procesverbaal ?
```

- ja 1 -> 6
- nee 2 -> einde onderwerp
- weigert / weet niet 8/9 -> einde onderwerp

6 Bent u of is iemand anders voor die aangifte op het politiebureau geweest ?
- op zelf 1
- iemand anders 2
- weigert / weet niet 8/9

7 >> ENQ.: Kaart 10 (REM) / Kaart 12 (REP), drie antwoorden mogelijk <<
Wat heeft de politie voor zover u weet aan de zaak gedaan ?
- informatie of advies gegeven 1
- schriftelijke verklaring of
- proces verbaal opgemaakt 2
- verwezen naar andere instellingen 3
- onderhandeld/bemiddeld 4
- iemand meegenomen naar het bureau 5
- de openbare weg vrijgemaakt/vrijgehouden 6
- brandweer, ziekenauto of dokter gewaarschuwd 7
- heeft zich ter plekke op de hoogte gesteld 8
- iets anders 9
- niets gedaan 10
- weigert / weet niet 98/99 -> einde onderwerp

8 *Als bij 'afhandeling' (zie 7) meer dan een mogelijkheid genoemd is -> 9*
anders -> einde onderwerp

9 >> ENQ.: Kaart 10 (REM) / Kaart 12 (REP) <<
Wat was daarvan het belangrijkste ?
- informatie of advies gegeven 1
- schriftelijke verklaring of
- proces verbaal opgemaakt 2
- verwezen naar andere instellingen 3
- onderhandeld/bemiddeld 4
- iemand meegenomen naar het bureau 5
- de openbare weg vrijgemaakt/vrijgehouden 6
- brandweer, ziekenauto of dokter gewaarschuwd 7
- heeft zich ter plekke op de hoogte gesteld 8
- iets anders 9
- niets gedaan 10
- weigert / weet niet 98/99

BIJLAGE 2. VRAGENLIJST BEDRIJVEN

Bedrijfskenmerken

Er wordt uitgegaan van een steekproef uit het bedrijvenregister van de Kamer van Koophandel, waardoor kenmerken als bedrijfstak, aantal vestigingen en omvang reeds bekend zijn. Deze worden wel opnieuw gecheckt. De introductie is grotendeels overgenomen uit de MCB; de betrokken vragen zijn aangegeven met **[MCB]**. Voor cybercrime is de bedrijfsenquête uit de VS als basis gebruikt; de vragen hieruit zijn aangegeven met **[VS]**. Voor financieel economische criminaliteit is geen goed internationaal voorbeeld voorhanden. Dit gedeelte van de vragenlijst is nieuw ontworpen, zo veel mogelijk naar analogie van de modules over cybercrime.

Het is waarschijnlijk dat bij grotere bedrijven de input van meerdere personen als respondent wordt gevraagd. De constructie waarmee dit gebeurt is hier niet expliciet aangegeven, maar onderzoekbureaus dienen in hun offerte duidelijk te maken op welke manier zij de respons van meer dan één persoon faciliteren.

We beginnen met enkele algemene vragen.
i1. Kunt u mij zeggen hoeveel personen er op dit moment gewoonlijk 15 uur of meer per week bij deze vestiging werkzaam zijn? De eigenaars/directeuren en eventuele meewerkende gezinsleden, mits 15 uur of meer per week werkzaam, dienen ook meegerekend te worden.

- geen
- 1 persoon
- 2 - 4 personen
- 5 - 9 personen
- 10 - 19 personen
- 20 - 49 personen
- 50 - 99 personen
- 100 en meer personen
- weet niet
- geen opgave

i2. Hoeveel vestigingen telt dit bedrijf? …

De volgende vragen zijn gebaseerd op de huidige indeling in sector en subsector van de Kamer van Koophandel, en wijken daardoor af van de vragen in de MCB

Indien bouwnijverheid
i3. Wat is de belangrijkste activiteit die wordt uitgeoefend in of vanuit deze vestiging? Is dat ...

- afwerking gebouwen
- bouwrijp maken
- installatie
- utiliteitsbouw
- verhuur
- geen van deze

Indien detailhandel
i4. Wat is de belangrijkste activiteit die wordt uitgeoefend in of vanuit deze vestiging? Is dat ...

- auto en motorfietsen
- colportage

- food + genotmiddelen
- markthandel
- non-food
- reparatie
- straathandel
- via postorder & internet
- geen van deze

Indien financieel

i5. Wat is de belangrijkste activiteit die wordt uitgeoefend in of vanuit deze vestiging? Is dat ...

- banken
- diensten
- verzekeren en pensioen
- geen van deze

Indien groothandel

i6. Wat is de belangrijkste activiteit die wordt uitgeoefend in of vanuit deze vestiging? Is dat ...

- consument non-food
- gespecialiseerd
- handelsbemiddeling
- ICT
- landbouw
- machines & apparaten
- voeding + genotmiddelen
- overig

Indien horeca

i7. Wat is de belangrijkste activiteit die wordt uitgeoefend in of vanuit deze vestiging? Is dat ...

- drinkgelegenheden
- eetgelegenheden
- hotels
- kantine & catering
- vakantieverblijven
- geen van deze

Indien industrie

i8. Wat is de belangrijkste activiteit die wordt uitgeoefend in of vanuit deze vestiging? Is dat ...

- bouwmaterialen + glas
- chemisch
- delfstofwinning
- hout + papier
- machines & apparaten
- metaal
- textiel
- transportmiddelen
- overig

Indien landbouw, bosbouw, visserij

i9. Wat is de belangrijkste activiteit die wordt uitgeoefend in of vanuit deze vestiging? Is dat ...

- akkerbouw
- bosbouw (ook diensten)
- dienstverlening

- dieren fokken en houden
- fruitteelt
- gemengd bedrijf
- hoveniers
- jacht
- tuinbouw

Indien persoonlijke diensten

i10. Wat is de belangrijkste activiteit die wordt uitgeoefend in of vanuit deze vestiging? Is dat ...

- crematoria
- fitness
- haarverzorging
- reinigen kleding + textiel
- sauna, solaria, baden
- schoonheidsverzorging
- uitvaart
- overig

Indien vervoer en communicatie

i11. Wat is de belangrijkste activiteit die wordt uitgeoefend in of vanuit deze vestiging? Is dat ...

- dienstverlening
- expeditie
- lucht- en ruimtevaart
- post en telecom
- spoor
- toerisme
- water
- weg
- geen van deze

Indien zakelijke dienstverlening

i12. Wat is de belangrijkste activiteit die wordt uitgeoefend in of vanuit deze vestiging? Is dat ...

- architect + ingenieur
- bedrijfadvies
- financieel administratief
- ICT
- keuring + controle
- rechtskundig/juridisch
- reclame
- reiniging
- overig

Indien sector overig

i13. Wat is de belangrijkste activiteit die wordt uitgeoefend in of vanuit deze vestiging? Is dat ...

- gezondheidszorg
- kunst, cultuur, amusement
- milieudienstverlening
- onderwijs
- onroerend goed
- sport + recreatie
- welzijnszorg
- geen van deze

i14. **[MCB]** Wat is uw functie in deze vestiging?
(bij meerdere respondenten meer dan één antwoord mogelijk)

- eigenaar
- directeur
- echtgeno(o)t(e) van de directeur
- financieel directeur
- hoofd financiële afdeling
- financiële controleur
- bedrijfsleider
- hoofd ICT [*niet in MCB*]
- medewerker ICT [*niet in MCB*]
- nog anders, namelijk .....
- geen opgave

i15. **[MCB]** Kunt u aangeven hoeveel uw omzet over 2008 bedroeg, exclusief BTW? Als u het niet precies weet, kunt u dan een zo goed mogelijke schatting
geven?

- weet exacte omzet
- geeft schatting
- nee
- weet niet
- wil niet zeggen

Indien i15=nee, weet niet of wil niet zeggen:naar i17

i16. **[MCB]** Wat is de totale omzet in 2008 in euro's? .....
Ga naar i19

Indien i15= nee, weet niet of wil niet zeggen:
i17. **[MCB]** Kunt u het misschien dan bij benadering aangeven?
Is de omzet hoger of lager dan 250 miljoen euro?

- hoger
- lager
- exact
- weet de exacte omzet
- wil niet (meer) zeggen
- weet niet (exacter)

Indien i17<>Lager: ga naar i20

Indien i17=lager
i18. **[MCB]** Is de omzet hoger of lager dan 50 miljoen euro?

- hoger
- lager
- exact
- weet de exacte omzet
- wil niet (meer) zeggen
- weet niet (exacter)

Ga naar i20

Indien i16<50.000 euro:
i19. **[MCB]** Is dit daadwerkelijk een bedrijf?

- ja

- nee

[NB. De volgende vier vragen uit de MCB lijken niet erg relevant voor FINEC & Cyber. Uit oogpunt van vergelijkbaarheid toch handhaven?]

i20. **[MCB]** Kunt u de aard van de huidige locatie van deze vestiging aanduiden? Ik lees u een aantal mogelijkheden op. Is dit een .....
Enq.: Lees op
- kantorencomplex
- handelscentrum of bedrijfsverzamelgebouw
- winkelcentrum
- bedrijfs- of industrieterrein
- afzonderlijk kantoorgebouw of bedrijfspand
- bedrijf in woonhuis
- anders, namelijk .....
- weet niet
- wil niet zeggen

i20. **[MCB]** Is deze vestiging gevestigd in het centrum van een stedelijke agglomeratie, aan de rand van een stedelijke agglomeratie of buiten een stedelijke agglomeratie?
- in het centrum van een stedelijke agglomeratie
- aan de rand van een stedelijke agglomeratie
- buiten een stedelijke agglomeratie (bijvoorbeeld dorp, platteland)
- anders, namelijk .....
- weet niet
- wil niet zeggen

i22. **[MCB]** Beschikt de vestiging over een eigen, van de openbare weg afgescheiden terrein \ bedrijfsterrein? We bedoelen daarmee ook bijvoorbeeld parkeerterreinen?
- ja
- nee
- weet niet
- wil niet zeggen

i23. **[MCB]** Heeft de vestiging eigen bedrijfswagens of wagens die namens het bedrijf zijn geleased of andere transportmiddelen?
Enq. shovels, heftrucks en schepen behoren ook tot andere transportmiddelen.
- ja
- nee
- weet niet
- geen antwoord

Zorgen over computerveiligheid

i24. **[VS]** Wat zijn de top 3 veiligheidsproblemen voor dit bedrijf?
- computer virus, worm of trojaans paard
- denial of service (van buitenaf platleggen communicatie)
- elektronisch vandalisme of sabotage
- verduistering
- fraude

- diefstal van intellectueel eigendom (copy rights, patenten, geheimen, handelsmerken)
- ongeoorloofd gebruik of kopiëren van digitale producten die ontwikkeld zijn voor de verkoop, zoals software, muziek of film
- diefstal van persoonlijke of financiële informatie, zoals namen, geboortedata, sofi-nummers, credit card nummers of PIN-codes
- andere computer incidenten zoals hacken, spoofing, phishing, sniffing, pinging, scanning, spyware, adware of andere malware
- misbruik van computers door werknemers (internet, e-mail etc.)
- misbruik van informatie op gestolen laptops
- iets anders, namelijk …

i25. **[VS]** Wat zijn de drie belangrijkste bronnen die de computerveiligheid bedreigen?
- de huidige werknemers
- huidige opdrachtnemers, verkopers, uitzendkrachten etc.
- vroegere werknemers, opdrachtnemers, verkopers, uitzendkrachten etc.
- binnenlandse concurrenten
- buitenlandse concurrenten
- binnenlandse hackers
- buitenlandse hackers
- anders, namelijk …

Infrastructuur en beveiliging

i26. **[VS]** Wat voor apparatuur en infrastructuur gebruikte dit bedrijf de afgelopen 12 maanden?
(*meer dan één antwoord mogelijk*)
- local area network (LAN)
- wide area network (WAN)
- process control network (PCN)
- virtual private network (VPN)
- draadloos netwerk
- electronic data interchange (EDI)
- intranet
- extranet
- stand-alone PC's (niet op een LAN)
- laptop die eigendom zijn van het bedrijf
- laptops die geen eigendom zijn van het bedrijf
- anders, namelijk …

i27. **[VS]** Welke vormen van toegang tot het netwerk werden de afgelopen 12 maanden door dit bedrijf ondersteund?
(*meer dan één antwoord mogelijk*)
- hard wired telecommunicatielijnen
- inbel-toegang via telecommunicatielijnen
- toegang tot de netwerken van het bedrijf of e-mail via het internet
- draadloze toegang tot e-mail

- draadloze toegang tot het internet
- draadloze toegang tot de gegevens van het bedrijf of andere netwerken
- publiek toegankelijke website ZONDER e-commerce mogelijkheden
- publiek toegankelijke website MET e-commerce mogelijkheden
- anders, namelijk …

i28. **[VS]** Welke vormen van beveiligingstechnologie heeft het bedrijf de afgelopen 12 maanden gebruikt?
(*meer dan één antwoord mogelijk*)

- anti-virus software
- anti spyware/adware software
- biometrie
- eenmalige wachtwoord generatoren (smartcards, tokens, etc.)
- wachtwoorden die periodiek moeten worden veranderd
- digitale certificaten
- firewall
- DMZ-Host
- indringers ontdekkingssyteem (Intrusion Detection System)
- indringers beveiligingssysteem (Intrusion Protection System)
- e-mail logs of filters
- administratieve systeem logs
- versleutelen, encryptie
- anders, namelijk …

i29. **[VS]** Hoeveel Euro heeft het bedrijf de afgelopen 12 maanden besteed aan de zojuist genoemde beveiligingstechnologie (als u het niet precies weet, kunt u dan een schatting geven)?
Personeelskosten tellen niet mee.
…… Euro

i30. **[VS]** Welk percentage van het totale ICT budget van het bedrijf is de afgelopen 12 maanden besteed aan beveiligingstechnologie (als u het niet precies weet, kunt u dan een schatting geven)?
Personeelskosten tellen niet mee.
… %

i31. **[VS]** Wat voor soort veiligheidstechnologie is het bedrijf van plan de komende 12 maanden toe te voegen aan wat het al heeft?
(*meer dan één antwoord mogelijk*)

- anti-virus software
- anti spyware/adware software
- biometrie
- eenmalige wachtwoord generatoren (smartcards, tokens, etc.)
- wachtwoorden die periodiek moeten worden veranderd
- digitale certificaten
- firewall
- DMZ-Host

- indringers ontdekkingssyteem (Intrusion Detection System)
- indringers beveiligingssysteem (Intrusion Protection System)
- e-mail logs of filters
- administratieve systeem logs
- versleutelen, encryptie
- anders, namelijk …
- het bedrijf gaat geen nieuwe technologie toevoegen

i32. **[VS]** Wat voor beleid en procedures had het bedrijf ten aanzien van computerveiligheid?

- business continuïteitsplan voor computersystemen
- rampen herstelplan voor computer systemen
- een bedrijfsbeleid voor computer veiligheid
- identificatie van de kritieke onderdelen van het bedrijf
- kwetsbaarheid/risico assessment
- testen van indringen in het bedrijf
- een computer/netwerk bewakingscentrum
- configuratie management
- regelmatig bekijken van de systeem-/veiligheidsadministratie logboeken
- periodieke computer veiligheidscontrole
- hebben van formele computer veiligheidsstandaards
- fysieke veiligheid (bijvoorbeeld beperkte fysieke toegang)
- personeelsbeleid (antecedentenonderzoek, overplaatsing, ontslag)
- training van personeel in computer veiligheidsprocedures
- vervanging/modernisering van apparatuur
- anders, namelijk …

i33. **[VS]** Welke computer veiligheidsfuncties heeft het bedrijf uitbesteed? Geef zowel de compleet als gedeeltelijk uitbestede activiteiten aan.
(*meer dan één antwoord mogelijk*)

- business continuïteitsplan voor computersystemen
- rampen herstelplan voor computer systemen
- een bedrijfsbeleid voor computer veiligheid
- identificatie van de kritieke onderdelen van het bedrijf
- kwetsbaarheid/risico assessment
- testen van indringen in het bedrijf
- een computer/netwerk bewakingscentrum
- configuratie management
- regelmatig bekijken van de systeem-/veiligheidsadministratie logboeken
- periodieke computer veiligheidscontrole
- hebben van formele computer veiligheidsstandaards
- fysieke veiligheid (bijvoorbeeld beperkte fysieke toegang)
- personeelsbeleid (antecedentenonderzoek, overplaatsing, ontslag)
- training van personeel in computer veiligheidsprocedures
- vervanging/modernisering van apparatuur
- anders, namelijk …

- alle activiteiten zijn geheel binnen het bedrijf uitgevoerd

i34. **[VS]** Als het bedrijf een business continuïteitsplan of een rampen herstelplan heeft, was dit dan de afgelopen 12 maanden getest, gebruikt in een noodsituatie of een nieuwe versie van geïnstalleerd?
(*meer dan één antwoord mogelijk*)

- de afgelopen 12 maanden getest
- de afgelopen 12 maanden in een noodsituatie gebruikt
- de afgelopen 12 maanden een nieuwe versie
- wel plannen, maar niet getest, gebruikt of nieuwe versie
- anders, namelijk …
- nee; had de afgelopen 12 maanden geen plannen

i35. **[VS]** Hoe vaak heeft dit bedrijf de afgelopen 12 maanden formele kwetsbaarheids/risico-assessments uitgevoerd voordat nieuwe applicaties, systemen of programma's werden geïmplementeerd?
(*meer dan één antwoord mogelijk*)

- altijd
- meer dan de helft van het aantal keren
- minder dan de helft van het aantal keren
- wanneer dit wettelijk vereist was
- anders, namelijk …
- nooit
- Er zijn geen nieuwe applicaties, systemen of programma's geïmplementeerd

i36. **[VS]** Heeft het bedrijf de afgelopen 12 maanden de downtime bijgehouden die het gevolg was van computer veiligheidsincidenten?

- ja
- nee

Computer virussen

Een computer virus is een verborgen stukje computer code dat zichzelf voortplant door zich in software te nestelen. Hieronder rekenen we ook wormen en Trojaanse paarden, maar **niet** adware, spyware en andere vormen van malware.

cv1. **[VS]** Zijn de afgelopen 12 maanden virussen ontdekt die een computer, een deel van het systeem of een totaal systeem geïnfecteerd hebben?

- ja
- nee

Indien cv1=<>ja: naar ds1

Indien cv1=ja

cv2. **[VS]** Om hoe veel incidenten met virussen gaat het?
(Wanneer een virus tegelijkertijd een server en één of meer PC's geïnfecteerd heeft dit als één incident tellen)
…. incidenten

cv3. **[VS]** Welke van de volgende vormen van veiligheidstechnologie of –procedures faalden bij het voorkomen van deze incidenten?
(*meer dan één antwoord mogelijk*)

- interne computer bescherming
- externe computer bescherming
- anti-virus software
- anti-spyware/adware software
- biometrie
- unieke wachtwoord generator
- wachtwoorden die periodiek veranderd moeten worden
- digitale certificaten
- firewall
- DMZ-Host
- indringers ontdekkingssyteem (Intrusion Detection System)
- indringers beveiligingssysteem (Intrusion Protection System)
- versleutelen, encryptie
- kwetsbaarheid software/buffer overload
- e-mail logs of filters
- computer/netwerk bewakingssysteem
- configuratie management
- fysieke/omgevingsbeveiliging
- personeelsbeleid
- misbruik van geautoriseerde toegang
- anders, namelijk …
- weet niet

cv4. **[VS]** Via welke kanalen zijn de virussen het bedrijf binnengekomen?
(*meer dan één antwoord mogelijk*)
- e-mail bijlagen
- installeren software
- files op USB-sticks, DVD's, CD's of andere draagbare media
- files die gedownload zijn van het internet
- anders, namelijk …
- weet niet

cv5. **[VS]** Aan welke van de volgende organisaties zijn deze incidenten gerapporteerd?
(*meer dan één antwoord mogelijk*)
- de politie
- GOVCERT.nl
- computerleverancier
- gespecialiseerd computerbeveiligingsbedrijf
- anders, namelijk …

cv6. **[VS]** Hoeveel van de … incidenten met virussen zijn gerapporteerd bij de politie? …
Indien alle incidenten gerapporteerd zijn bij de politie: naar cv8

Indien incidenten niet gerapporteerd zijn bij de politie

cv7. **[VS]** Wat zijn de redenen dat incidenten niet gerapporteerd zijn bij de politie?
(*meer dan één antwoord mogelijk*)
- intern afgehandeld
- aan een andere organisatie gerapporteerd, namelijk …
- negatieve publiciteit
- verlaagt vertrouwen van klanten of investeerders
- concurrentie overwegingen
- wilde niet dat de hardware als bewijsmateriaal in beslag werd genomen
- hier gaat de politie niet over
- niet aan gedacht
- viel niets mee te winnen
- anders, namelijk …

Indien incidenten wel gerapporteerd zijn bij de politie

cv8. Is de politie erin geslaagd de daders op te sporen?
- ja, in alle gevallen
- ja, in sommige gevallen
- de daders zijn wel bekend, maar nooit dankzij de politie
- de daders zijn in geen van de incidenten bekend

Indien geen daders bekend: naar cv10

Indien daders bekend

cv9. **[VS]** Wat was de relatie tussen de dader(s) en het bedrijf toen de incidenten met virussen plaatsvonden?

(*meer dan één antwoord mogelijk*)

- medewerker
- opdrachtnemer, verkoper, uitzendkracht
- vroegere medewerker, opdrachtnemer, verkoper, uitzendkracht
- buitenstaander, iemand die nooit voor het bedrijf heeft gewerkt
- binnenlandse concurrent
- buitenlandse concurrent
- binnenlandse hacker
- buitenlandse hacker
- andere hacker (land onbekend)
- anders, namelijk …
- weet niet

cv10. **[VS]** Wat was de gemiddelde downtime (in uren) per virusinfectie; wilt u de tijd nodig voor reparatie meetellen? (als u het niet precies weet, geeft u dan een schatting)

- voor de servers, routers en switches …. uur
- voor de individuele PC's/werkstations …. uur

cv11. **[VS]** Hoeveel is de afgelopen 12 maanden uitgegeven aan het herstel als gevolg van computervirussen? (als u het niet precies weet, geeft u dan een schatting)

…. Euro

cv12. **[VS]** Tot welke verliezen en kosten hebben de virusinfecties de afgelopen 12 maanden geleid? (als u het niet precies weet, geeft u dan een schatting). Tel daarbij mee de waarde van de verloren informatie, gemiste verkopen, juridische kosten etc.

…. Euro

Denial of service

Denial of service is de verbreking, aantasting of uitputting van een internetverbinding; dit heeft een onderbreking van de normale informatiestroom tot gevolg. Denial of service wordt meestal veroorzaakt door ping aanvallen, grote hoeveelheid binnenkomende gegevens etc. NB. Geef hier **geen** incidenten op die al bij virussen zijn vermeld.

ds1. **[VS]** Zijn er de afgelopen 12 maanden denial of service incidenten geweest?

- ja
- nee

Indien ds1<>ja: naar ev1

Indien ds1=ja

ds2. **[VS]** Om hoe veel denial of service incidenten gaat het?

…. incidenten

ds3. **[VS]** Welke van de volgende vormen van veiligheidstechnologie of –procedures faalden bij het voorkomen van deze incidenten?

(*meer dan één antwoord mogelijk*)

- interne computer bescherming
- externe computer bescherming
- anti-virus software
- anti-spyware/adware software
- biometrie
- unieke wachtwoord generator
- wachtwoorden die periodiek veranderd moeten worden
- digitale certificaten
- firewall
- DMZ-Host
- indringers ontdekkingssyteem (Intrusion Detection System)
- indringers beveiligingssysteem (Intrusion Protection System)
- versleutelen, encryptie
- kwetsbaarheid software/buffer overload
- e-mail logs of filters
- computer/netwerk bewakingssysteem
- configuratie management
- fysieke/omgevings beveiliging
- personeelsbeleid
- misbruik van geautoriseerde toegang
- anders, namelijk …
- weet niet

ds4. **[VS]** Welke van de volgende onderdelen werden aangetast door deze denial of service incidenten?

(*meer dan één antwoord mogelijk*)
- local area network (LAN)
- wide area network (WAN)
- process control network (PCN)
- virtual private network (VPN)
- draadloos netwerk
- electronic data interchange (EDI)
- intranet
- extranet
- stand-alone PC's (niet op een LAN)
- laptop die eigendom zijn van het bedrijf
- laptops die geen eigendom zijn van het bedrijf
- anders, namelijk …
- weet niet

ds5. **[VS]** Aan welke van de volgende organisaties zijn deze incidenten gerapporteerd?
(*meer dan één antwoord mogelijk*)
- de politie
- GOVCERT.nl
- computerleverancier
- gespecialiseerd computerbeveiligingsbedrijf
- anders, namelijk …

ds6. **[VS]** Hoeveel van de … denial of service incidenten zijn gerapporteerd bij de politie? …
Indien alle incidenten gerapporteerd zijn bij de politie: naar ds8

Indien incidenten niet gerapporteerd zijn bij de politie

ds7. **[VS]** Wat zijn de redenen dat incidenten niet gerapporteerd zijn bij de politie?
(*meer dan één antwoord mogelijk*)
- intern afgehandeld
- aan een andere organisatie gerapporteerd, namelijk …
- negatieve publiciteit
- verlaagt vertrouwen van klanten of investeerders
- concurrentie overwegingen
- wilde niet dat de hardware als bewijsmateriaal in beslag werd genomen
- hier gaat de politie niet over
- niet aan gedacht
- viel niets mee te winnen
- anders, namelijk …

Indien incidenten wel gerapporteerd zijn bij de politie

ds8. Is de politie erin geslaagd de daders op te sporen?
- ja, in alle gevallen
- ja, in sommige gevallen
- de daders zijn wel bekend, maar nooit dankzij de politie

- de daders zijn in geen van de incidenten bekend

Indien geen daders bekend: naar ds10

Indien daders bekend

ds9. **[VS]** Wat was de relatie tussen de dader(s) en het bedrijf toen de incidenten plaatsvonden?
(*meer dan één antwoord mogelijk*)

- medewerker
- opdrachtnemer, verkoper, uitzendkracht
- vroegere medewerker, opdrachtnemer, verkoper, uitzendkracht
- buitenstaander, iemand die nooit voor het bedrijf heeft gewerkt
- binnenlandse concurrent
- buitenlandse concurrent
- binnenlandse hacker
- buitenlandse hacker
- andere hacker (land onbekend)
- anders, namelijk …
- weet niet

ds10. **[VS]** Wat was de totale duur (in uren) van de denial of service incidenten? (als u het niet precies weet, geeft u dan een schatting). De tijd nodig voor reparatie meetellen.
…. uur

ds11. **[VS]** Hoeveel is de afgelopen 12 maanden uitgegeven aan het herstel als gevolg van denial of service incidenten (als u het niet precies weet, geeft u dan een schatting)
…. Euro

ds12. **[VS]** Tot welke verliezen en kosten hebben de denial ofservice incidenten de afgelopen 12 maanden geleid? (als u het niet precies weet, geeft u dan een schatting). Tel daarbij mee de waarde van de verloren informatie,verloren productiviteit, gemiste verkopen, juridische kosten etc.
…. Euro

Electronisch vandalisme of sabotage

Electronisch vandalisme of sabotage is het bewust of kwaadwillig schade toebrengen, electronisch bekladden, kapot maken of op andere manieren veranderen van files, data, web pagina's programma's etc.

NB.

- Geef hier **geen** incidenten op die al bij virussen zijn vermeld.
- Incidenten die uitmondden in fraude komen later in deze vragenlijst aan bod; wilt u die hier **niet** vermelden

ev1. **[VS]** Heeft dit bedrijf de afgelopen 12 maanden incidenten ontdekt waarin files, data, web pagina's of delen van het computer systeem electronisch beschadigd of gesaboteerd is?

- ja
- nee

Indien ev1<>ja: naar vd1

Indien ev1=ja

ev2. **[VS]** Om hoe veel incidenten van electronisch vandalisme of sabotage gaat het?

…. incidenten

ev3. **[VS]** Welke van de volgende vormen van veiligheidstechnologie of –procedures faalden bij het voorkomen van deze incidenten?

(*meer dan één antwoord mogelijk*)

- interne computer bescherming
- externe computer bescherming
- anti-virus software
- anti-spyware/adware software
- biometrie
- unieke wachtwoord generator
- wachtwoorden die periodiek veranderd moeten worden
- digitale certificaten
- firewall
- DMZ-Host
- indringers ontdekkingssyteem (Intrusion Detection System)
- indringers beveiligingssysteem (Intrusion Protection System)
- versleutelen, encryptie
- kwetsbaarheid software/buffer overload
- e-mail logs of filters
- computer/netwerk bewakingssysteem
- configuratie management
- fysieke/omgevings beveiliging
- personeelsbeleid
- misbruik van geautoriseerde toegang

- anders, namelijk …
- weet niet

ev4. **[VS]** Welke van de volgende onderdelen werden aangetast door deze vandalisme of sabotage incidenten?
(*meer dan één antwoord mogelijk*)
- local area network (LAN)
- wide area network (WAN)
- process control network (PCN)
- virtual private network (VPN)
- draadloos netwerk
- electronic data interchange (EDI)
- intranet
- extranet
- stand-alone PC's (niet op een LAN)
- laptop die eigendom zijn van het bedrijf
- laptops die geen eigendom zijn van het bedrijf
- anders, namelijk …
- weet niet

ev5. **[VS]** Aan welke van de volgende organisaties zijn deze incidenten gerapporteerd?
(*meer dan één antwoord mogelijk*)
- de politie
- GOVCERT.nl
- computerleverancier
- gespecialiseerd computerbeveiligingsbedrijf
- anders, namelijk …

ev6. **[VS]** Hoeveel van de … vandalisme of sabotage incidenten zijn gerapporteerd bij de politie?
…
Indien alle incidenten gerapporteerd zijn bij de politie: naar ev8

Indien incidenten niet gerapporteerd zijn bij de politie

ev7. **[VS]** Wat zijn de redenen dat incidenten niet gerapporteerd zijn bij de politie?
(*meer dan één antwoord mogelijk*)
- intern afgehandeld
- aan een andere organisatie gerapporteerd, namelijk …
- negatieve publiciteit
- verlaagt vertrouwen van klanten of investeerders
- concurrentie overwegingen
- wilde niet dat de hardware als bewijsmateriaal in beslag werd genomen
- hier gaat de politie niet over
- niet aan gedacht
- viel niets mee te winnen
- anders, namelijk …

Indien incidenten wel gerapporteerd zijn bij de politie

ev8. Is de politie erin geslaagd de daders op te sporen?

- ja, in alle gevallen
- ja, in sommige gevallen
- de daders zijn wel bekend, maar nooit dankzij de politie
- de daders zijn in geen van de incidenten bekend

Indien geen daders bekend: naar ev10

Indien daders bekend

ev9. **[VS]** Wat was de relatie tussen de dader(s) en het bedrijf toen de vandalisme of sabotage incidenten plaatsvonden?
(*meer dan één antwoord mogelijk*)

- medewerker
- opdrachtnemer, verkoper, uitzendkracht
- vroegere medewerker, opdrachtnemer, verkoper, uitzendkracht
- buitenstaander, iemand die nooit voor het bedrijf heeft gewerkt
- binnenlandse concurrent
- buitenlandse concurrent
- binnenlandse hacker
- buitenlandse hacker
- andere hacker (land onbekend)
- anders, namelijk …
- weet niet

ev10. **[VS]** Wat was de totale downtime (in uren) als gevolg van vandalisme of sabotage incidenten; wilt u de tijd nodig voor reparatie meetellen? (als u het niet precies weet, geeft u dan een schatting)

- voor de websites, webservers …. uur
- voor de servers, routers en switches …. uur
- voor de individuele PC's/werkstations …. uur

ev11. **[VS]** Hoeveel is de afgelopen 12 maanden uitgegeven aan het herstel van de schade als gevolg van vandalisme en sabotage incidenten (als u het niet precies weet, geeft u dan een schatting); tel mee: de interne en externe kosten van diagnose, reparatie en vervanging: arbeidskosten, hardware en software; tel niet mee: preventie van nieuwe incidenten.
…. Euro

ev12. **[VS]** Tot welke verliezen en kosten hebben de vandalisme en sabotage incidenten de afgelopen 12 maanden geleid? (als u het niet precies weet, geeft u dan een schatting). Tel daarbij mee de waarde van de verloren informatie,verloren productiviteit, gemiste verkopen, juridische kosten etc.
…. Euro

Verduistering

Verduistering is de onwettige toe-eigening van geld of andere waardevolle zaken door degene aan wie deze waren toevertrouwd (meestal een werknemer).

Tel daarbij mee de gevallen waarin een computer is gebruikt om geld ten onrechte over te maken, te vervalsen, ten onrechte toegang te krijgen tot geld, bezittingen, financiële documenten, verzekeringspolissen, gebruik van huurauto's en andere diensten door de persoon aan wie dit was toevertrouwd.

vd1 **[VS]** Heeft dit bedrijf de afgelopen 12 maanden incidenten ontdekt waarin de computer was gebruikt voor verduistering tegen het bedrijf?

- ja
- nee

Indien vd1<>ja: naar fr1

Indien vd1=ja

vd2. **[VS]** Om hoe veel verduisteringsincidenten gaat het?

…. incidenten

vd3. **[VS]** Welke van de volgende vormen van veiligheidstechnologie of –procedures faalden bij het voorkomen van deze incidenten?

(*meer dan één antwoord mogelijk*)

- interne computer bescherming
- externe computer bescherming
- anti-virus software
- anti-spyware/adware software
- biometrie
- unieke wachtwoord generator
- wachtwoorden die periodiek veranderd moeten worden
- digitale certificaten
- firewall
- DMZ-Host
- indringers ontdekkingssyteem (Intrusion Detection System)
- indringers beveiligingssysteem (Intrusion Protection System)
- versleutelen, encryptie
- kwetsbaarheid software/buffer overload
- e-mail logs of filters
- computer/netwerk bewakingssysteem
- configuratie management
- fysieke/omgevings beveiliging
- personeelsbeleid
- misbruik van geautoriseerde toegang
- anders, namelijk …

- weet niet

vd4. **[VS]** Welke van de volgende onderdelen is gebruikt voor deze verduisteringsincidenten? (*meer dan één antwoord mogelijk*)
- local area network (LAN)
- wide area network (WAN)
- process control network (PCN)
- virtual private network (VPN)
- draadloos netwerk
- electronic data interchange (EDI)
- intranet
- extranet
- stand-alone PC's (niet op een LAN)
- laptop die eigendom zijn van het bedrijf
- laptops die geen eigendom zijn van het bedrijf
- anders, namelijk …
- weet niet

vd5. **[VS]** Aan welke van de volgende organisaties zijn deze incidenten gerapporteerd? (*meer dan één antwoord mogelijk*)
- de politie
- GOVCERT.nl
- computerleverancier
- gespecialiseerd computerbeveiligingsbedrijf
- anders, namelijk …

vd6. **[VS]** Hoeveel van de … verduisteringsincidenten zijn gerapporteerd bij de politie? …
Indien alle incidenten gerapporteerd zijn bij de politie: naar vd8

Indien incidenten niet gerapporteerd zijn bij de politie

vd7. **[VS]** Wat zijn de redenen dat incidenten niet gerapporteerd zijn bij de politie? (*meer dan één antwoord mogelijk*)
- intern afgehandeld
- aan een andere organisatie gerapporteerd, namelijk …
- negatieve publiciteit
- verlaagt vertrouwen van klanten of investeerders
- concurrentie overwegingen
- wilde niet dat de hardware als bewijsmateriaal in beslag werd genomen
- hier gaat de politie niet over
- niet aan gedacht
- viel niets mee te winnen
- anders, namelijk …

Indien incidenten wel gerapporteerd zijn bij de politie

vd8. Is de politie erin geslaagd de daders op te sporen?

- ja, in alle gevallen
- ja, in sommige gevallen
- de daders zijn wel bekend, maar nooit dankzij de politie
- de daders zijn in geen van de incidenten bekend

Indien geen dader bekend: naar vd10

Indien daders bekend

vd9. **[VS]** Wat was de relatie tussen de dader(s) en het bedrijf toen de incidenten plaatsvonden?
(*meer dan één antwoord mogelijk*)

- medewerker
- opdrachtnemer, verkoper, uitzendkracht
- vroegere medewerker, opdrachtnemer, verkoper, uitzendkracht
- buitenstaander, iemand die nooit voor het bedrijf heeft gewerkt
- binnenlandse concurrent
- buitenlandse concurrent
- binnenlandse hacker
- buitenlandse hacker
- andere hacker (land onbekend)
- anders, namelijk …
- weet niet

vd10. **[VS]** Wat was de waarde in Euro's van het geld en andere zaken die de afgelopen 12 maanden zijn verduisterd?
…. Euro

vd11. **[VS]** Tot welke andere verliezen en kosten hebben de verduisteringsincidenten de afgelopen 12 maanden geleid? (als u het niet precies weet, geeft u dan een schatting). Tel daarbij mee de kosten van diagnose, reparatie en vervanging zoals arbeid, hardware en software. Indien mogelijk ook de waarde van downtime, van de verloren informatie,verloren productiviteit, gemiste verkopen, juridische kosten etc. Tel niet mee de maatregelen ter voorkoming van dit soort incidenten in de toekomst.
…. Euro

Fraude

Fraude is:

- het geven van een moedwillig verkeerde voorstelling van informatie om anderen te misleiden
- het aannemen van een valse identiteit om anderen te misleiden
- het ongeoorloofd gebruik van een credit kaart of een bankpas
- het gebruiken van elektronische middelen om geld of andere waardevolle dingen te krijgen

Fraude kan worden gepleegd door iemand binnen of buiten het bedrijf.

Tel daarbij mee de gevallen waarin een computer is gebruikt om tegen het bedrijf te frauderen met geld, bezittingen, financiële documenten, verzekeringspolissen, aktes, gebruik van huurauto's en andere diensten door middel van vervalsing, valse identiteit, credit card etc.
Tel **niet** mee: verduisteringsincidenten.

fr1. **[VS]** Heeft dit bedrijf de afgelopen 12 maanden incidenten ontdekt waarin iemand binnen of buiten het bedrijf de computer heeft gebruikt voor fraude tegen het bedrijf.

- ja
- nee

Indien fr1<>ja: naar de1

Indien fr1=ja

fr2. **[VS]** Om hoe veel fraude-incidenten gaat het?

…. incidenten

fr3. **[VS]** Welke van de volgende vormen van veiligheidstechnologie of –procedures faalden bij het voorkomen van deze incidenten?
(*meer dan één antwoord mogelijk*)

- interne computer bescherming
- externe computer bescherming
- anti-virus software
- anti-spyware/adware software
- biometrie
- unieke wachtwoord generator
- wachtwoorden die periodiek veranderd moeten worden
- digitale certificaten
- firewall
- DMZ-Host
- indringers ontdekkingssyteem (Intrusion Detection System)
- indringers beveiligingssysteem (Intrusion Protection System)
- versleutelen, encryptie
- kwetsbaarheid software/buffer overload
- e-mail logs of filters
- computer/netwerk bewakingssysteem

- configuratie management
- fysieke/omgevingsbeveiliging
- personeelsbeleid
- misbruik van geautoriseerde toegang
- anders, namelijk …
- weet niet

fr4. **[VS]** Welke van de volgende onderdelen is gebruikt voor deze fraude-incidenten? (*meer dan één antwoord mogelijk*)

- local area network (LAN)
- wide area network (WAN)
- process control network (PCN)
- virtual private network (VPN)
- draadloos netwerk
- electronic data interchange (EDI)
- intranet
- extranet
- stand-alone PC's (niet op een LAN)
- laptop die eigendom zijn van het bedrijf
- laptops die geen eigendom zijn van het bedrijf
- anders, namelijk …
- weet niet

fr5. **[VS]** Aan welke van de volgende organisaties zijn deze incidenten gerapporteerd? (*meer dan één antwoord mogelijk*)

- de politie
- GOVCERT.nl
- computerleverancier
- gespecialiseerd computerbeveiligingsbedrijf
- anders, namelijk …

fr6. **[VS]** Hoeveel van de … fraude-incidenten zijn gerapporteerd bij de politie? …
Indien alle incidenten gerapporteerd zijn bij de politie: naar fr8

Indien incidenten niet gerapporteerd zijn bij de politie

fr7. **[VS]** Wat zijn de redenen dat incidenten niet gerapporteerd zijn bij de politie? (*meer dan één antwoord mogelijk*)

- intern afgehandeld
- aan een andere organisatie gerapporteerd, namelijk …
- negatieve publiciteit
- verlaagt vertrouwen van klanten of investeerders
- concurrentie overwegingen
- wilde niet dat de hardware als bewijsmateriaal in beslag werd genomen
- hier gaat de politie niet over
- niet aan gedacht

- viel niets mee te winnen
- anders, namelijk …

Indien incidenten wel gerapporteerd zijn bij de politie

fr8. Is de politie erin geslaagd de daders op te sporen?

- ja, in alle gevallen
- ja, in sommige gevallen
- de daders zijn wel bekend, maar nooit dankzij de politie
- de daders zijn in geen van de incidenten bekend

Indien geen dader bekend: naar fr10

Indien daders bekend

fr9. **[VS]** Wat was de relatie tussen de dader(s) en het bedrijf toen de fraude-incidenten plaatsvonden?
(*meer dan één antwoord mogelijk*)

- medewerker
- opdrachtnemer, verkoper, uitzendkracht
- vroegere medewerker, opdrachtnemer, verkoper, uitzendkracht
- buitenstaander, iemand die nooit voor het bedrijf heeft gewerkt
- binnenlandse concurrent
- buitenlandse concurrent
- binnenlandse hacker
- buitenlandse hacker
- andere hacker (land onbekend)
- anders, namelijk …
- weet niet

fr10. **[VS]** Wat was de waarde in Euro's van het geld en andere zaken die de afgelopen 12 maanden door fraude zijn kwijtgeraakt?
…. Euro

fr11. **[VS]** Tot welke andere verliezen en kosten hebben de fraude-incidenten de afgelopen 12 maanden geleid? (als u het niet precies weet, geeft u dan een schatting). Tel daarbij mee de kosten van diagnose, reparatie en vervanging zoals arbeid, hardware en software. Indien mogelijk ook de waarde van downtime, van de verloren informatie,verloren productiviteit, gemiste verkopen, juridische kosten etc. Tel niet mee de maatregelen ter voorkoming van dit soort incidenten in de toekomst.
…. Euro

Diefstal van intellectueel eigendom

Diefstal van intellectueel eigendom is het illegaal verkrijgen van materiaal waarop copy rights of patenten rusten, bedrijfsgeheimen of handelsmerken, waaronder ontwerpen, plannen, blauwdrukken, codes, computer programma's formules, recepten, grafieken etc.

Tel daarbij **niet** mee de diefstal van persoonlijke of financiële informatie zoals credit card of sofi-nummers namen en geboortedata, rekeningnummers etc. Tel ook de diefstal van andere informatie niet mee.

de1. **[VS]** Heeft dit bedrijf de afgelopen 12 maanden incidenten ontdekt waarin iemand binnen of buiten het bedrijf een computer gebruikt heeft voor de diefstal van intellectueel eigendom?

- ja
- nee

Indien de1<>ja: naar di1

Indien de1=ja

de2. **[VS]** Om hoe veel incidenten van diefstal van intellectueel eigendom gaat het?

…. incidenten

de3. **[VS]** Wat voor soort intellectueel eigendom was gestolen?

(*meer dan één antwoord mogelijk*)

- materiaal waarop copy rights rusten
- materiaal waarop een patent rust
- bedrijfsgeheimen
- handelsmerken

de4. **[VS]** Welke van de volgende vormen van veiligheidstechnologie of –procedures faalden bij het voorkomen van deze incidenten?

(*meer dan één antwoord mogelijk*)

- interne computer bescherming
- externe computer bescherming
- anti-virus software
- anti-spyware/adware software
- biometrie
- unieke wachtwoord generator
- wachtwoorden die periodiek veranderd moeten worden
- digitale certificaten
- firewall
- DMZ-Host
- indringers ontdekkingssyteem (Intrusion Detection System)
- indringers beveiligingssysteem (Intrusion Protection System)
- versleutelen, encryptie
- kwetsbaarheid software/buffer overload

- e-mail logs of filters
- computer/netwerk bewakingssysteem
- configuratie management
- fysieke/omgevings beveiliging
- personeelsbeleid
- misbruik van geautoriseerde toegang
- anders, namelijk …
- weet niet

de5. **[VS]** Welke van de volgende onderdelen is gebruikt voor deze diefstallen van intellectueel eigendom?
(*meer dan één antwoord mogelijk*)

- local area network (LAN)
- wide area network (WAN)
- process control network (PCN)
- virtual private network (VPN)
- draadloos netwerk
- electronic data interchange (EDI)
- intranet
- extranet
- stand-alone PC's (niet op een LAN)
- laptop die eigendom zijn van het bedrijf
- laptops die geen eigendom zijn van het bedrijf
- anders, namelijk …
- weet niet

de6. **[VS]** Aan welke van de volgende organisaties zijn deze diefstallen van intellectueel eigendom gerapporteerd?
(*meer dan één antwoord mogelijk*)

- de politie
- GOVCERT.nl
- computerleverancier
- gespecialiseerd computerbeveiligingsbedrijf
- anders, namelijk …

Indien niet gerapporteerd aan de politie: naar de8

de7. **[VS]** Hoeveel van de … diefstallen zijn gerapporteerd bij de politie? …
Indien alle incidenten gerapporteerd zijn bij de politie: naar de9

Indien incidenten niet gerapporteerd zijn bij de politie

de8. **[VS]** Wat zijn de redenen dat diefstallen niet gerapporteerd zijn bij de politie?
(*meer dan één antwoord mogelijk*)

- intern afgehandeld
- aan een andere organisatie gerapporteerd, namelijk …
- negatieve publiciteit

- verlaagt vertrouwen van klanten of investeerders
- concurrentie overwegingen
- wilde niet dat de hardware als bewijsmateriaal in beslag werd genomen
- hier gaat de politie niet over
- niet aan gedacht
- viel niets mee te winnen
- anders, namelijk …

Indien incidenten wel gerapporteerd zijn bij de politie

de9. Is de politie erin geslaagd de daders, de dieven van het intellectueel eigendom op te sporen?

- ja, in alle gevallen
- ja, in sommige gevallen
- de daders zijn wel bekend, maar nooit dankzij de politie
- de daders zijn in geen van de incidenten bekend

Indien geen dader bekend: naar de11

Indien daders bekend

de10. **[VS]** Wat was de relatie tussen de dader(s) en het bedrijf toen de diefstallen van intellectueel eigendom plaatsvonden?

(*meer dan één antwoord mogelijk*)

- medewerker
- opdrachtnemer, verkoper, uitzendkracht
- vroegere medewerker, opdrachtnemer, verkoper, uitzendkracht
- buitenstaander, iemand die nooit voor het bedrijf heeft gewerkt
- binnenlandse concurrent
- buitenlandse concurrent
- binnenlandse hacker
- buitenlandse hacker
- andere hacker (land onbekend)
- anders, namelijk …
- weet niet

de11. **[VS]** Wat was de waarde in Euro's van het intellectueel eigendom dat de afgelopen 12 maanden is gestolen?

…. Euro

de12. **[VS]** Tot welke andere verliezen en kosten hebben de diefstallen de afgelopen 12 maanden geleid? (als u het niet precies weet, geeft u dan een schatting). Tel daarbij mee de kosten van diagnose, reparatie en vervanging zoals arbeid, hardware en software. Indien mogelijk ook de waarde van downtime, van de verloren informatie,verloren productiviteit, gemiste verkopen, juridische kosten etc. Tel niet mee de maatregelen ter voorkoming van dit soort incidenten in de toekomst.

…. Euro

de13. **[VS]** Hoe veel van de diefstallen van intellectueel eigendom hadden betrekking op illegaal kopiëren of illegaal gebruik (piraterij) van producten die het bedrijf had ontwikkeld voor verkoop.

....

Diefstal van persoonlijke en financiële informatie

Diefstal van persoonlijke of financiële informatie is het illegaal verkrijgen van informatie die iemand in staat stelt om rekeningen te openen of te gebruiken onder een valse naam (persoonlijk of zakelijk). Persoonlijke informatie heeft betrekking op namen, geboortedata, sofi-nummers etc. Financiële informatie heeft betrekking op credit cards, bankpassen, rekeningnummers en PIN-codes.

Tel daarbij **niet** mee de diefstal van intellectueel eigendom, zoals copy rights, patenten, bedrijfsgeheimen en handelsmerken. Tel ook de diefstal van andere informatie niet mee.

di1. **[VS]** Heeft dit bedrijf de afgelopen 12 maanden incidenten ontdekt die betrekking hadden op de diefstal van persoonlijke of financiële informatie?

- ja
- nee

Indien di1<>ja: naar ov1

Indien di1=ja

di2. **[VS]** Om hoeveel diefstallen gaat het?

…. incidenten

di3. **[VS]** Om wat voor diefstallen van persoonlijke of financiële informatie gaat het?
(*meer dan één antwoord mogelijk*)

- Namen of geboortedata
- Sofi-nummers
- Credit card nummers
- Bankpassen
- Rekeningnummers of PIN-codes
- anders, namelijk ...

di4. **[VS]** Welke van de volgende vormen van veiligheidstechnologie of –procedures faalden bij het voorkomen van deze diefstallen?
(*meer dan één antwoord mogelijk*)

- interne computer bescherming
- externe computer bescherming
- anti-virus software
- anti-spyware/adware software
- biometrie
- unieke wachtwoord generator
- wachtwoorden die periodiek veranderd moeten worden
- digitale certificaten
- firewall
- DMZ-Host
- indringers Ontdekkingssyteem (Intrusion Detection System)
- indringers Beveiligingssysteem (Intrusion Protection System)
- versleutelen, encryptie

- kwetsbaarheid software/buffer overload
- e-mail logs of filters
- computer/netwerk bewakingssysteem
- configuratie management
- fysieke/omgevings beveiliging
- personeelsbeleid
- misbruik van geautoriseerde toegang
- anders, namelijk …
- weet niet

di5. **[VS]** Welke van de volgende onderdelen is gebruikt bij de diefstallen van persoonlijke of financiële informatie?
(*meer dan één antwoord mogelijk*)

- local area network (LAN)
- wide area network (WAN)
- process control network (PCN)
- virtual private network (VPN)
- draadloos netwerk
- electronic data interchange (EDI)
- intranet
- extranet
- stand-alone PC's (niet op een LAN)
- laptop die eigendom zijn van het bedrijf
- laptops die geen eigendom zijn van het bedrijf
- anders, namelijk …
- weet niet

di6. **[VS]** Aan welke van de volgende organisaties zijn deze diefstallen van persoonlijke of financiële informatie gerapporteerd?
(*meer dan één antwoord mogelijk*)

- de politie
- GOVCERT.nl
- computerleverancier
- gespecialiseerd computerbeveiligingsbedrijf
- anders, namelijk …

Indien niet gerapporteerd aan de politie: naar di8

di7. **[VS]** Hoeveel van de … diefstallen zijn gerapporteerd bij de politie? …
Indien alle incidenten gerapporteerd zijn bij de politie: naar di9

Indien incidenten niet gerapporteerd zijn bij de politie

di8. **[VS]** Wat zijn de redenen dat diefstallen van persoonlijke of financiële informatie niet gerapporteerd zijn bij de politie?
(*meer dan één antwoord mogelijk*)

- intern afgehandeld

- aan een andere organisatie gerapporteerd, namelijk …
- negatieve publiciteit
- verlaagt vertrouwen van klanten of investeerders
- concurrentie overwegingen
- wilde niet dat de hardware als bewijsmateriaal in beslag werd genomen
- hier gaat de politie niet over
- niet aan gedacht
- viel niets mee te winnen
- anders, namelijk …

Indien incidenten wel gerapporteerd zijn bij de politie

di9. Is de politie erin geslaagd de daders op te sporen?

- ja, in alle gevallen
- ja, in sommige gevallen
- de daders zijn wel bekend, maar nooit dankzij de politie
- de daders zijn in geen van de incidenten bekend

Indien geen dader bekend: naar di11

Indien daders bekend

di10. **[VS]** Wat was de relatie tussen de dader(s) en het bedrijf toen de diefstallen van persoonlijke of financiële informatie plaatsvonden?
(*meer dan één antwoord mogelijk*)

- medewerker
- opdrachtnemer, verkoper, uitzendkracht
- vroegere medewerker, opdrachtnemer, verkoper, uitzendkracht
- buitenstaander, iemand die nooit voor het bedrijf heeft gewerkt
- binnenlandse concurrent
- buitenlandse concurrent
- binnenlandse hacker
- buitenlandse hacker
- andere hacker (land onbekend)
- anders, namelijk …
- weet niet

di11. **[VS]** Wat was de waarde in Euro's van de persoonlijke of financiële informatie die de afgelopen 12 maanden is gestolen? (als u het niet precies weet, geeft u dan een schatting)
…. Euro

di12. **[VS]** Tot welke andere verliezen en kosten hebben de diefstallen de afgelopen 12 maanden geleid? (als u het niet precies weet, geeft u dan een schatting). Tel daarbij mee de kosten van diagnose, reparatie en vervanging zoals arbeid, hardware en software. Indien mogelijk ook de waarde van downtime, van de verloren informatie,verloren productiviteit, gemiste verkopen, juridische kosten etc. Tel niet mee de maatregelen ter voorkoming van dit soort incidenten in de toekomst.
…. Euro

Overige veiligheidsincidenten met computers

Hier gaat het om alle andere veiligheidsincidenten die zijn gebeurd op de computers of netwerken van het bedrijf, zoals hacken, sniffen, spyware, diefstal en andere incidenten, ongeacht of dit tot schade of financiële verliezen heeft geleid.

Tel daarbij **niet** mee alle incidenten die al eerder in deze vragenlijst aan de orde zijn geweest.

ov1. **[VS]** Heeft dit bedrijf de afgelopen 12 maanden andere incidenten ontdekt die betrekking hadden op computerveiligheid?

- ja
- nee

Indien ov1<>ja: naar ov14

Indien ov1=ja

ov2. **[VS]** Om hoe veel veiligheidsincidenten gaat het?

…. incidenten

ov3. **[VS]** Wat voor veiligheidsincidenten waren het?
(*meer dan één antwoord mogelijk*)

- hacken (inbreken)
- spoofen (identiteitsvervalsing, waarbij de bron zich voordoet als iets of iemand anders)
- phishing (het op een misleidende manier vragen van persoonlijke gegevens)
- sniffing (bekijken van netwerkverkeer en onderscheppen van wachtwoorden)
- pinging (het continu contact maken met een poort)
- scanning (het identificeren welke poorten actief zijn)
- spyware, keystroke logging (het vastleggen van toetsaanslagen)
- adware
- andere malware
- diefstal van informatie die niet eerder beschreven is, namelijk ...
- anders, namelijk ...

ov4. **[VS]** Welke van de volgende vormen van veiligheidstechnologie of –procedures faalden bij het voorkomen van deze incidenten?
(*meer dan één antwoord mogelijk*)

- interne computer bescherming
- externe computer bescherming
- anti-virus software
- anti-spyware/adware software
- biometrie
- unieke wachtwoord generator
- wachtwoorden die periodiek veranderd moeten worden
- digitale certificaten
- firewall
- DMZ-Host

- indringers Ontdekkingssyteem (Intrusion Detection System)
- indringers Beveiligingssysteem (Intrusion Protection System)
- versleutelen, encryptie
- kwetsbaarheid software/buffer overload
- e-mail logs of filters
- computer/netwerk bewakingssysteem
- configuratie management
- fysieke/omgevings beveiliging
- personeelsbeleid
- misbruik van geautoriseerde toegang
- anders, namelijk …
- weet niet

ov5. **[VS]** Welke van de volgende onderdelen is gebruikt, benaderd of aangetast bij deze veiligheidsincidenten?
(*meer dan één antwoord mogelijk*)

- local area network (LAN)
- wide area network (WAN)
- process control network (PCN)
- virtual private network (VPN)
- draadloos netwerk
- electronic data interchange (EDI)
- intranet
- extranet
- stand-alone PC's (niet op een LAN)
- laptop die eigendom zijn van het bedrijf
- laptops die geen eigendom zijn van het bedrijf
- anders, namelijk …
- weet niet

ov6. **[VS]** Aan welke van de volgende organisaties zijn deze veiligheidsincidenten gerapporteerd?
(*meer dan één antwoord mogelijk*)

- de politie
- GOVCERT.nl
- computerleverancier
- gespecialiseerd computerbeveiligingsbedrijf
- anders, namelijk …

Indien niet gerapporteerd aan de politie: naar ov8

ov7. **[VS]** Hoeveel van de … veiligheidsincidenten zijn gerapporteerd bij de politie? …
Indien alle incidenten gerapporteerd zijn bij de politie: naar ov9

Indien incidenten niet gerapporteerd zijn bij de politie

ov8. **[VS]** Wat zijn de redenen dat incidenten niet gerapporteerd zijn bij de politie?

(*meer dan één antwoord mogelijk*)
- intern afgehandeld
- aan een andere organisatie gerapporteerd, namelijk …
- negatieve publiciteit
- verlaagt vertrouwen van klanten of investeerders
- concurrentie overwegingen
- wilde niet dat de hardware als bewijsmateriaal in beslag werd genomen
- hier gaat de politie niet over
- niet aan gedacht
- viel niets mee te winnen
- anders, namelijk …

Indien incidenten wel gerapporteerd zijn bij de politie

ov9. Is de politie erin geslaagd de daders op te sporen?
- ja, in alle gevallen
- ja, in sommige gevallen
- de daders zijn wel bekend, maar nooit dankzij de politie
- de daders zijn in geen van de incidenten bekend

Indien geen dader bekend: naar ov11

Indien daders bekend

ov10. **[VS]** Wat was de relatie tussen de dader(s) en het bedrijf toen de veiligheidsincidenten plaatsvonden?
(*meer dan één antwoord mogelijk*)
- medewerker
- opdrachtnemer, verkoper, uitzendkracht
- vroegere medewerker, opdrachtnemer, verkoper, uitzendkracht
- buitenstaander, iemand die nooit voor het bedrijf heeft gewerkt
- binnenlandse concurrent
- buitenlandse concurrent
- binnenlandse hacker
- buitenlandse hacker
- andere hacker (land onbekend)
- anders, namelijk …
- weet niet

ov11. **[VS]** Wat was de gemiddelde downtime (in uren) per veiligheidsincident; wilt u de tijd nodig voor reparatie meetellen? (als u het niet precies weet, geeft u dan een schatting)
- voor de webservers en webpagina's van het bedrijf .... uur
- voor de servers, routers en switches …. uur
- voor de individuele PC's/werkstations …. uur

ov12. **[VS]** Hoeveel is de afgelopen 12 maanden uitgegeven om te herstellen van deze veiligheidsincidenten? (als u het niet precies weet, geeft u dan een schatting). Tel daarbij mee de kosten van diagnose, reparatie en vervanging: arbeid, hardware en software.

…. Euro

ov13. **[VS]** Tot welke andere verliezen en kosten hebben de veiligheidsincidenten de afgelopen 12 maanden geleid? (als u het niet precies weet, geeft u dan een schatting). Tel daarbij mee de waarde van downtime, van de verloren informatie,verloren productiviteit, gemiste verkopen, juridische kosten etc. Tel niet mee de maatregelen ter voorkoming van dit soort incidenten in de toekomst.
…. Euro

Overige aspecten van computerveiligheid

ov14 **[VS]** Zijn er de afgelopen 12 maanden veiligheidsincidenten geweest die het gevolg zijn van misbruik van informatie op een gestolen laptop computer?

- ja
- nee

ov15. **[VS]** Zijn er de afgelopen 12 maanden veiligheidsincidenten geweest die het gevolg zijn van misbruik van informatie op een gestolen of kwijtgeraakte USB-stick?

- ja
- nee

ov16. **[VS]** Is het aantal veiligheidsincidenten de afgelopen 12 maanden af- of toegenomen ten opzichte van het jaar ervoor?

- afgenomen
- toegenomen
- gelijk gebleven
- weet niet

ov17. Had het bedrijf de afgelopen 12 maanden een verzekering die de schade van dit soort incidenten dekt?

- nee, niets is gedekt
- een gedeelte is gedekt
- alle schade is gedekt
- weet niet

Voor alle incidenten (zie voorafgaande rubrieken) die zich hebben voorgedaan:
ov18. Heeft het bedrijf naar aanleiding van deze incidenten preventieve maatregelen genomen ter preventie die

- extra uitgaven met zich meebrengen
- het personeel beperkingen opleggen die er daarvoor niet waren

ov19. **[VS]** Welk percentage van het aantal financiële transacties van het bedrijf loopt via het internet?
... %

Overige fraude en financieel-economische criminaliteit

De rest van de enquête gaat over fraude en financieel-economische criminaliteit die niet onder het voorafgaande viel, en waarin niet (noodzakelijk) de computer een rol speelt.

Het eigen personeel

fe1. Is het in de afgelopen 12 maanden voorgekomen dat kandidaat-werknemers hebben gesolliciteerd en daarbij valse diploma's, getuigschriften of cv's hebben overlegd?

- ja
- nee

Indien fe1<>ja: naar fe5

Indien fe1=ja:

fe2. Hoe vaak gebeurde dit?

… keer

fe3. Zijn deze sollicitanten (aanvankelijk) ook aangenomen?

- nee
- deels
- ja
- weet niet

fe4. Aan welke van de volgende organisaties zijn deze incidenten gerapporteerd? (*meer dan één antwoord mogelijk*)

- de politie
- de instituten waarvan de vervalste documenten afkomstig waren
- een koepelorganisatie van uw bedrijfstak
- anders, namelijk …
- geen

fe5. Zijn er in de afgelopen 12 maanden gevallen ontdekt waarin personeel is aangenomen die infiltranten van een concurrent of andere kwaadwillende partij bleken te zijn? (NB. Omkoping valt hier niet onder)

- ja
- nee

Indien fe5<>ja: naar fe11

Indien fe5= ja:

fe6. Om hoeveel gevallen ging het?

… keer

fe7. Wat was de bedoeling van de infiltratie?

- spionage, bedrijfsinformatie doorspelen

- sabotage
- het bedrijf gebruiken voor illegale doeleinden (zoals smokkel, illegaal verspreiden producten)
- diefstal
- anders, namelijk …
- weet niet

fe8. Aan welke van de volgende organisaties zijn deze incidenten gerapporteerd?
(*meer dan één antwoord mogelijk*)

- de politie
- de instituten waarvan de vervalste documenten afkomstig waren
- een koepelorganisatie van uw bedrijfstakf
- anders, namelijk …
- geen

fe9. Heeft (hebben) de infiltrant(en) het bedrijf de afgelopen 12 maanden daadwerkelijk schade kunnen berokkenen?

- ja
- nee

Indien fe9<>ja: naar fe11

Indien fe9=ja:
fe10. Hoe groot was deze schade de afgelopen 12 maanden? (als u het niet precies weet, geeft u dan een schatting) Tel mee eventuele juridische kosten en arbeidskosten.
… Euro

fe11. Zijn er de afgelopen 12 maanden gevallen ontdekt waarin het eigen personeel is omgekocht door een concurrent of andere kwaadwillende partij?

- ja
- nee

Indien fe11<>ja: naar fe17

Indien fe11= ja:
fe12. Om hoeveel gevallen ging het?
… keer

fe13. Wat was de bedoeling van de omkoping?

- spionage, bedrijfsinformatie doorspelen
- sabotage
- het bedrijf gebruiken voor illegale doeleinden (zoals smokkel, illegaal verspreiden producten)
- diefstal
- anders, namelijk …
- weet niet

fe14. Aan welke van de volgende organisaties zijn deze incidenten gerapporteerd?
(*meer dan één antwoord mogelijk*)

- de politie
- een koepelorganisatie van uw bedrijfstak
- anders, namelijk …
- geen

fe15. Heeft het omgekochte personeelslid/hebben de omgekochte personeelsleden het bedrijf daadwerkelijk schade kunnen berokkenen?
- ja
- nee

Indien fe15<>ja: naar fe17

Indien fe15=ja:
fe16. Hoe groot was de afgelopen 12 maanden deze schade door omkoping (als u het niet precies weet, geeft u dan een schatting)? Tel mee eventuele juridische kosten en arbeidskosten.
… Euro

fe17. Is uw bedrijf de afgelopen 12 maanden op een andere manier slachtoffer geweest van spionage op een manier die nog niet genoemd is (dus niet door infiltratie in of omkoping van het eigen personeel, of door inbreken in het computersysteem)?
- ja
- nee

Indien fe17<>ja: naar fe19

Indien fe17= ja:
fe18. Kunt u kort omschrijven hoe dit in zijn werk ging? open

Leveranciers

fe19. Heeft het bedrijf de afgelopen 12 maanden goederen geheel of gedeeltelijk betaald die vervolgens niet geleverd zijn?
- ja
- nee

Indien fe19<>ja: ga naar fe23

Indien fe19= ja:
fe20. Om hoeveel gevallen ging het?
… keer

fe21. Aan welke van de volgende organisaties zijn deze incidenten gerapporteerd?
(*meer dan één antwoord mogelijk*)
- de politie
- een koepelorganisatie van uw bedrijfstak
- anders, namelijk …

- geen

fe22. Hoe groot was deze schade de afgelopen 12 maanden (als u het niet precies weet, geeft u dan een schatting)? Tel mee eventuele juridische kosten en arbeidskosten.
… Euro

fe23. Heeft het bedrijf de afgelopen 12 maanden voor advertenties betaald die vervolgens niet gemaakt of gepubliceerd zijn?
- ja
- nee

Indien fe23<>ja ga naar fe26

Indien fe23=ja:
fe24. Om hoeveel gevallen ging het?
… keer

fe25. Hoe groot was deze schade (als u het niet precies weet, geeft u dan een schatting)? Tel mee eventuele juridische kosten en arbeidskosten.
… Euro

fe26. Heeft het bedrijf de afgelopen 12 maanden goederen aangeboden gekregen, waarvan de afkomst verdacht was (uitnodiging tot heling)?
- ja
- nee

Indien fe26<>ja: ga naar fe29

Indien fe26= ja:
fe27. Hoeveel keren gebeurde dit?
… keer

fe28. Hoe hoog was de waarde van deze goederen de afgelopen 12 maanden (als u het niet precies weet, geeft u dan een schatting)?
… Euro

fe29. Heeft het bedrijf de afgelopen 12 maanden facturen/rekeningen gekregen voor goederen of diensten die helemaal nooit geleverd zijn (spooknota's)?
- ja
- nee

Indien fe29<>ja: ga naar fe34

Indien fe29=ja:
fe30. Om hoeveel spooknota's ging het?
… nota's

fe31. Hoeveel daarvan zijn de afgelopen 12 maanden daadwerkelijk betaald?

… nota's

fe32. Aan welke van de volgende organisaties zijn deze incidenten gerapporteerd?
(*meer dan één antwoord mogelijk*)
- de politie
- een koepelorganisatie van uw bedrijfstak
- anders, namelijk …
- geen

fe33. Hoe groot was deze schade de afgelopen 12 maanden (als u het niet precies weet, geeft u dan een schatting)?
… Euro

Klanten

fe34. Heeft het bedrijf de afgelopen 12 maanden goederen of diensten geleverd aan klanten die daarvoor vervolgens niet betaald hebben? Reken hieronder ook het betalen met valse middelen zoals een gestolen credit card, bankpas of PIN-code waarbij de schade niet door de bank is vergoed.
- ja
- nee

Indien fe34<>ja: ga naar fe40

Indien fe34= ja:
fe35. Om hoeveel gevallen ging het?
… gevallen

fe36. Wat was de reden (waren de redenen) dat er niet is betaald?
(meer dan één antwoord mogelijk)
- onwil
- faillissement
- klant had valse identiteit aangenomen
- klant betaalde met valse middelen/credit card/bankpas
- anders, namelijk …

Indien faillissement
fe37. Heeft de klant het faillissement te gebruikt om te frauderen, geld waar uw bedrijf recht op had weg te sluizen?
- ja
- nee

fe38. Aan welke van de volgende organisaties zijn deze incidenten gerapporteerd?
(*meer dan één antwoord mogelijk*)
- de politie
- een koepelorganisatie van uw bedrijfstak
- anders, namelijk …

- geen

fe39. Hoe groot was de afgelopen 12 maanden de schade als gevolg van niet betalende klanten (als u het niet precies weet, geeft u dan een schatting)? Tel mee eventuele juridische kosten en arbeidskosten.
… Euro

Overig

fe40. Is het bedrijf de afgelopen 12 maanden gedwongen geweest om mensen om te kopen, geld aan mensen te betalen die daar geen recht op hadden, om voor het bedrijf essentiële zaken voor elkaar te krijgen (vergunningen, contracten etc.)? Beperkt u zich daarbij tot omkopingsgevallen in Nederland.

- ja
- nee

Indien fe40<>ja: ga naar fe44

Indien fe40= ja:
fe41. Om hoeveel gevallen ging het?
… gevallen

fe42. Wat voor soort mensen heeft het bedrijf moeten omkopen?
(meer dan één antwoord mogelijk)

- ambtenaren
- politie, douane
- mensen die een sleutelpositie in een ander bedrijf bekleedden
- particulieren
- anders, namelijk …
- weet niet

fe43. Wat is het totale bedrag dat uw bedrijf de afgelopen 12 maanden heeft besteed aan omkoping in Nederland (als u het niet precies weet, geeft u dan een schatting)?
… Euro

fe44. Is het bedrijf de afgelopen 12 maanden gedwongen geweest om geld aan mensen te betalen die anders dreigden het bedrijf schade toe te brengen (afpersing).

- ja
- nee

Indien fe44<>ja: ga naar fe51

Indien fe44=ja:
fe45. Om hoeveel gevallen van afpersing ging het de afgelopen 12 maanden? …

fe46. Wat was de aard van de bedreiging van de afpersers?
(meer dan één antwoord mogelijk)

- beschadiging van het interne computersysteem
- beschadiging van het contact met de klant via het internet (e-mail, bestellingen, betalingen)
- fysieke beschadiging van het bedrijf (brandstichting, vernieling; ook van auto's)
- fysieke bedreiging van personen
- anders, namelijk …

fe47. Zijn deze gevallen van afpersing aan de politie gerapporteerd?
- nee
- deels [*alleen opnemen indien meerdere incidenten*]
- ja

Indien fe47=ja: ga naar fe49

Indien fe47<>ja

fe48. **[VS]** Wat zijn de redenen dat incidenten niet gerapporteerd zijn bij de politie? (*meer dan één antwoord mogelijk*)
- intern afgehandeld
- aan een andere organisatie gerapporteerd, namelijk …
- negatieve publiciteit
- verlaagt vertrouwen van klanten of investeerders
- concurrentie overwegingen
- wilde niet dat de hardware als bewijsmateriaal in beslag werd genomen
- hier gaat de politie niet over
- niet aan gedacht
- viel niets mee te winnen
- anders, namelijk …

Indien fe47=nee: ga naar fe50

Indien fe47=deels of ja

fe49. Is de politie erin geslaagd de daders uit te schakelen?
- ja
- ten dele
- nee
- weet niet

fe50. Wat is het totale bedrag dat uw bedrijf de afgelopen 12 maanden heeft besteed aan afpersing (als u het niet precies weet, geeft u dan een schatting)?
… Euro

fe51. Is het bedrijf de afgelopen 12 maanden slachtoffer geweest van marktmanipulatie, het opzettelijk verspreiden van geruchten die de goede naam en de positie van het bedrijf aantasten?
- ja
- nee

Indien fe51=ja:

fe52. Kunt u het incident in uw eigen woorden kort omschrijven? (open)

Hartelijk dank voor uw medewerking aan deze enquête.