MASTER'S THESIS

Centrale aansturing van informatiebeveiliging bij een nationale departementale organisatie

Brehen, M.

Award date:
2020

Centrale aansturing van informatiebeveiliging bij een nationale departementale organisatie

Central control of information security at a national departmental organization

Opleiding:	Open Universiteit, faculteit Management, Science & Technology Masteropleiding Business Process Management & IT
Programme:	Open University of the Netherlands, faculty of Management, Science & Technology Master Business Process Management & IT
Cursus:	IM0602 Voorbereiden Afstuderen BPMIT IM9806 Afstudeertraject Business Process Management and IT
Student:	M. Brehen
Identiteitsnummer:	
Datum:	31-03-2020
Afstudeerbegeleider	Prof. dr. L. Bijlsma
Meelezer	Dr. L.W. Rutledge
Versienummer:	v31032020
Status:	definitief

Abstract

Het doel van dit onderzoek is theoretische inzichten op het gebied van centrale aansturing van informatiebeveiliging te toetsen aan de toepassing van deze inzichten bij een nationale departementale organisatie in de praktijk.

De doelstelling van het empirisch onderzoek is in kaart te brengen hoe in de praktijk invulling wordt gegeven aan de centrale aansturing van de informatiebeveiliging bij een nationale departementale organisatie. Om de doelstelling te kunnen bereiken is informatie nodig waaruit herleid kon worden hoe nu binnen een nationale departementale organisatie wordt omgegaan met de centrale aansturing van informatiebeveiliging.

De conclusie is dat het de vraag is in hoeverre de departementale top inzicht en grip heeft op de informatiebeveiliging binnen hun departement als het beschreven beleid niet tot uitvoer wordt gebracht in de praktijk. Alleen als het topmanagement zich houdt aan zijn taakomschrijving in de beleidsdocumenten en dit daadwerkelijk toepast dan kan het inzicht in en grip hebben op de informatiebeveiliging in de praktijk.

Hoofdaanbeveling van dit onderzoek is dat het topmanagement invulling dient te geven in de praktijk aan de beschreven rol op het gebied van informatiebeveiliging. Alleen op deze manier kan het topmanagement waarborgen dat ze inzicht en grip hebben op de informatiebeveiliging in hun organisatie.

Sleutelbegrippen

Informatiebeveiliging, informatiebeveiligingsbeheer, departementale organisatie

Samenvatting

De Nederlandse rijksoverheid onderkent het toenemende belang van informatiebeveiliging. De Algemene Rekenkamer doet hier intern ook onderzoek naar. Een van de speerpunten in dit onderzoek is de versteviging van de centrale sturing. Centrale sturing is belangrijk omdat de Nederlandse rijksoverheid van mening is dat informatiebeveiliging een zaak is van de departementale top. Deze zou inzicht in en zo nodig grip moeten hebben op de maatregelen, risico's en incidenten die decentraal spelen. Dit blijkt onder meer uit de kamerbrief die de Minister van Binnenlandse Zaken en Koninkrijksrelaties heeft opgesteld en waarin het rijksbrede beleid op het gebied van informatiebeveiliging wordt uitgezet. Dit is tevens verwoord in het Besluit voorschrift informatiebeveiliging rijksdienst 2007: "Informatiebeveiliging vormt een integraal onderdeel van de bedrijfsvoering en is daarmee een managementverantwoordelijkheid." Het doel van dit onderzoek is theoretische inzichten op het gebied van centrale aansturing van informatiebeveiliging te toetsen aan de toepassing van deze inzichten bij een nationale departementale organisatie in de praktijk.

De Nederlandse rijksoverheid heeft een verplichting richting haar burgers, die steeds hogere verwachtingen hebben van wat de overheid voor ze kan betekenen. De uitdaging op dit gebied is dat de Nederlandse rijksoverheid moet anticiperen op de snelle technologische ontwikkelingen maar ook de informatiebeveiliging moet waarborgen. Zoals eerder beschreven is informatiebeveiliging een zaak van de departementale top. Daarom is het maatschappelijk relevant om te toetsen of de theoretische inzichten op het gebied van de centrale aansturing van de informatiebeveiliging ook toegepast worden binnen de Nederlandse rijksoverheid. Daarnaast is vanuit de wetenschappelijke literatuur bekend dat ondersteuning van het topmanagement een belangrijke invloed heeft op informatiebeveiliging, maar ook dat de effecten hiervan zelden empirisch worden onderzocht. Slechts een paar studies beschrijven de empirisch relatie tussen ondersteuning door het topmanagement en de effecten op informatiebeveiliging.

Informatiebeveiliging is het proces van vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit, alsmede het treffen, onderhouden en controleren van bijbehorende maatregelen. Informatiebeveiliging vormt een belangrijk kwaliteitsaspect van de informatievoorziening van de Nederlandse rijksoverheid. Het beveiligen van informatie is echter geen eenmalige zaak, maar een proces waarbij steeds de Plan-Do-Check-Act cyclus wordt doorlopen. Binnen de Nederlandse rijksoverheid is het doorlopen van dit proces een verantwoordelijkheid van de departementale top. De vraag is: in hoeverre heeft de departementale top inzicht in en grip op de informatiebeveiliging binnen het departement?

De doelstelling van het empirisch onderzoek was het onderzoeken hoe in de praktijk invulling wordt gegeven aan de centrale aansturing van de informatiebeveiliging bij een nationale departementale organisatie. Om de doelstelling te kunnen bereiken was informatie nodig waaruit herleid kan worden hoe nu binnen een nationale departementale organisatie wordt omgegaan met de centrale aansturing van informatiebeveiliging.

De belangrijkste resultaten van dit onderzoek worden hieronder weergegeven.

Op het gebied van betrokkenheid van het topmanagement zijn dit de voornaamste resultaten De departementale secretaris-generaal van een ministerie is eindverantwoordelijk voor de integrale beveiliging. Daarom dient deze het beleid voor informatiebeveiliging vast te stellen en uit te dragen in de departementale organisatie. De directie van de departementale organisatie dient een duidelijke beleidsrichting aan te geven door een informatiebeveiligingsbeleid uit te geven en dit te handhaven voor de gehele departementale organisatie. Een kritische succesfactor voor een geslaagde

implementatie van informatiebeveiliging in een organisatie is zichtbare steun en betrokkenheid van alle managementniveaus.

Op het gebied van organisatiestructuren voor het afdwingen van informatiebeveiliging zijn dit de voornaamste resultaten. De departementale secretaris wijst een departementale beveiligings-ambtenaar aan die zorg draagt voor het toezicht op de integrale beveiliging van het departement. Daarnaast is door de leiding van de organisatie vastgelegd wat de verantwoordelijkheden en de rollen zijn op het gebied van informatiebeveiliging binnen de organisatie. Als laatste dient het beveiligingsbeleid een eigenaar te hebben die door de directie goedgekeurde verantwoordelijkheden heeft.

Op het gebied van gebruikersbewustzijn en betrokkenheid bij informatiebeveiliging zijn dit de voornaamste resultaten. Het informatiebeveiligingsbeleid dient aan alle medewerkers te worden gecommuniceerd. Hierbij moeten eisen gesteld worden met betrekking tot beveiligingsscholing, -training en bewustwording. De ervaring leert dat de volgende twee factoren van belang zijn voor een geslaagde implementatie van informatiebeveiliging: ten eerste een effectieve marketing van informatiebeveiliging naar alle medewerkers van de organisatie en ten tweede het verzorgen van training en opleiding om beveiligingsbewustzijn te creëren. Belangrijk om te beseffen is dat verandering in de mentaliteit op het gebied van informatiebeveiliging van medewerkers slechts geleidelijk gerealiseerd kan worden.

Op het gebied van compliance zijn dit de voornaamste resultaten. Binnen de departementale organisatie is een rijksbeveiligingsambtenaar verantwoordelijk voor het toezicht van de naleving van de rijksbrede kaders. Daarnaast dient het management van alle medewerkers te eisen dat ze informatiebeveiliging toepassen conform het beveiligingsbeleid. Het management dient tevens te communiceren wat de gevolgen zijn van het niet naleven van het informatiebeveiligingsbeleid. Informatiebeveiliging moet op een natuurlijke wijze zijn ingebed in de normale gang van zaken en niet als iets aparts wordt ervaren. Het management heeft een voorbeeldfunctie op het gebied van compliance; goed voorbeeld doet goed volgen.

In de diverse beleidsdocumenten binnen de departementale organisatie is beschreven hoe de departementale top betrokken dient te zijn bij de verschillende facetten van het informatiebeveiligingsbeheer. De conclusie is dat het de vraag is in hoeverre de departementale top inzicht en grip heeft op de informatiebeveiliging binnen hun departement als het beschreven beleid niet tot uitvoer wordt gebracht in de praktijk. Alleen als het topmanagement zich houdt aan zijn taakomschrijving in de beleidsdocumenten en dit daadwerkelijk toepast dan kan het inzicht in en grip hebben op de informatiebeveiliging in de praktijk.

De hoofdaanbeveling van dit onderzoek is dat de rol van het topmanagement op het gebied van Informatiebeveilingsbeheer duidelijk beschreven dient te zijn in diverse beleidsdocumenten. Dit is bij deze departementale organisatie ook het geval maar alleen het beschrijven van deze rol is niet afdoende. Het topmanagement dient ook invulling te geven in de praktijk aan de beschreven rol op het gebied van informatiebeveiliging. Alleen op deze manier kan het topmanagement in de praktijk waarborgen dat ze inzicht en grip hebben op de informatiebeveiliging in hun organisatie.

Summary

The Dutch central government recognizes the increasing importance of good information security, and the Court of Audit also investigates this internally. One of the focus areas in this study is the strengthening of central control. Central control is important because the Dutch central government believes that information security is a departmental top's responsibility. At the departmental top, there should be insight and, if necessary, a grip on the measures, risks, and incidents that may occur within an organization. This recommendation appears in a letter to the parliament drawn up by the Minister of the Interior and Kingdom Relations in which the government-wide policy on information security is set out. Moreover, it is also expressed in the Decree on information security for government service 2007: "Information security forms an integral part of business operations and is therefore a management responsibility." The aim of this research is to test theoretical insights in the field of central control of information security against their use in a national departmental organization in practice.

The Dutch government has an obligation towards citizens, who have increasingly higher expectations of what the government can do for them. The challenge in this area is that the Dutch central government must anticipate the fast developments that take place while ensuring information security. As mentioned earlier, information security is a departmental top's responsibility. It is thus socially relevant to test whether the theoretical insights into the central control of information security are also applied within the Dutch government. Furthermore, the scientific literature indicates that supporting top management has an important influence on information security the effect of which are rarely investigated empirically. Only a few studies investigate the empirical relationship between support from top management and the effects on information security.

Information security is the process of determining the required reliability of information systems in terms of confidentiality, availability, and integrity as well as taking, maintaining, and checking associated measures. Information security is an important quality aspect of the information management of the Dutch central government. However, securing information is not a one-off thing but a process in which the Plan-Do-Check-Act cycle is always followed. Within the Dutch government, completing this process is the responsibility of the departmental top. The question is: to what extent is there insight and control within the departmental top on information security within their department?

The present study offers an overview of the way the central management of information security is implemented in a national departmental organization. Information was gathered that could be reduced back into the way in which a national departmental organization deals with the central management of information security.

The most important results of this research are shown below.

The following are the most important results in terms of the involvement of top management: the departmental secretary-general of a ministry has the overall responsibility for integral security. For this reason, the secretary-general must put a huge amount of information security policy in place and carry it within the departmental organization. Furthermore, the management of a departmental organization must indicate a clear policy direction and does this by issuing an information security policy and enforcing it for the entire departmental organization. A critical success factor for a successful implementation of information security in an organization is visible support from and involvement of all management levels.

The following are the most important results in the area of organizational structures for enforcing information security: the departmental secretary nominates a departmental security officer who is responsible for supervising the integral security of the department; in addition, the management of the organization establishes what the responsibilities and roles are in the field of information security within the organization; finally, the security policy must have an owner who has responsibilities recognized by the management.

The following are the most important results in terms of user awareness and involvement in information security: the information security policy must be communicated to all employees, and requirements must be set with regard to security training, training, and awareness. Experience shows that the following two factors are important for the successful implementation of information security: the first is the effective marketing of information security to all employees of the organization, and the second is the provision of training and education to create security awareness. It is important to realize that changing the mentality in the field of information security of employees can only be achieved gradually.

The following are the most important results in terms of compliance: within the departmental organization, a government security officer is responsible for supervising compliance with government-wide frameworks; furthermore, management must require all employees to apply information security following security policy. Management also serves to communicate the consequences of failure to comply with the information security policy. Information security should be naturally embedded in the ordinary course of business and should not be experienced as something special. Management has an important exemplary function in terms of compliance, and good examples tend to be followed.

The various policy documents within the departmental organization describe how the departmental top should be involved in the various facets of information security management. The conclusion is that the question is to what extent the departmental top has insight and control over information security within their department if the described policy is not implemented in practice. Only if top management adheres to its job description in the policy documents and applies this factually can it gain insight into and control over information security in practice.

The most important recommendation of this study is that the role of top management in the field of information security management should be clearly described in various policy documents. This is also the case with this departmental organization, but only describing this role is not sufficient. Top management should also give practical substance to the described role in the field of information security. Only in this way can top management guarantee in practice that they have insight and control over the information security in their organization.

Inhoudsopgave

1. Introductie

1.1. Achtergrond

Anno 2018 verkeren we nog midden in de digitale transformatie en de daarmee onlosmakelijk verbonden security-thema's. Deze digitale transformatie zien we terug in het toenemende gebruik van clouddiensten, de ontwikkelingen op het gebied van artifical intelligence (AI) en de inbedding van internet of things (IoT) in onze samenleving (Leest, 2018). Deze digitale transformatie levert ook steeds meer potentiële kwetsbaarheden op. In het buitenland zijn de voorbeelden hiervan de hacks van Cozy Bear op de Democratische partij in de Verenigde Staten en de WannaCry-ransomware die wereldwijd spoorwegen, bedrijven en ziekenhuizen trof. Dichterbij zijn het onder andere de DDoS-aanvallen die plaatsvonden op de belastingdienst en op DigiD (Algemene Rekenkamer, 2017) met als effect dat deze overheidsdiensten verminderd bereikbaar waren. Een ander voorbeeld is het besluit van de Minister van Justitie en Veiligheid over de voorzorgsmaatregel die door het kabinet is genomen ten aanzien van het gebruik van de antivirussoftware van Kaspersky Lab. In een brief geeft de minister van Veiligheid en Justitie aan dat de zorgen over de digitale dreigingen hebben geleid tot een aangescherpte afweging ten aanzien van het gebruik van digitale producten en diensten (Grapperhaus, 2018). In dat kader heeft het kabinet bepaald dat, als voorzorgsmaatregel, Kaspersky's antivirussoftware bij de Nederlandse rijksoverheid[1] wordt uitgefaseerd.

De digitale transformatie en de kwetsbaarheden die hieruit voortvloeien onderstrepen het toenemend belang van informatiebeveiliging. Bij de genoemde voorbeelden werden democratische processen beïnvloed, burgers en instellingen gechanteerd en de dienstverlening werd ontregeld. Ook de Nederlandse rijksoverheid ondergaat deze digitale transformatie en ook zij wordt getroffen door deze kwetsbaarheden. De Nederlandse rijksoverheid heeft hierin wel een uitzonderlijke positie. De samenleving is in hoge mate afhankelijk van de diensten die de Nederlandse rijksoverheid levert en daarnaast heeft de zij een kaderstellende functie (Algemene Rekenkamer, 2017). Dit vereist dat de Nederlandse rijksoverheid zelf haar informatiebeveiliging op orde heeft en daarmee het goede voorbeeld geeft.

De Nederlandse rijksoverheid onderkent het toenemende belang van goede informatiebeveiliging en de Algemene Rekenkamer doet hier intern ook onderzoek naar. Een van de speerpunten in dit onderzoek is de versteviging van de centrale sturing (Algemene Rekenkamer, 2017). Centrale sturing is belangrijk, omdat de Nederlandse rijksoverheid van mening is dat informatiebeveiliging een zaak is van de departementale top. Deze zou inzicht in en zo nodig grip moeten hebben op de maatregelen, risico's en incidenten die decentraal spelen. Dit blijkt onder andere uit de kamerbrief die de Minister van Binnenlandse Zaken en Koninkrijksrelaties heeft opgesteld en waarin het rijksbrede beleid op het gebied van informatiebeveiliging wordt uitgezet (Ollongren, 2017). Daarnaast is dit verwoord in het Besluit voorschrift informatiebeveiliging rijksdienst 2007 (Balkenende, 2007, p. 11): "Informatiebeveiliging vormt een integraal onderdeel van de bedrijfsvoering en is daarmee een managementverantwoordelijkheid." Het doel van dit onderzoek is theoretische inzichten op het gebied van centrale aansturing van informatiebeveiliging te toetsen aan de toepassing van deze inzichten bij een nationale departementale organisatie in de praktijk.

Dit hoofdstuk vormt de introductie voor de afstudeeropdracht en heeft de volgende opbouw. Paragraaf 1.2. is de gebiedsverkenning en definieert de basisbegrippen van het onderzoeksgebied. In paragraaf 1.3. volgt de probleemstelling waaraan een bijdrage wordt geleverd en in paragraaf 1.4. wordt de onderzoeksvraag gepresenteerd, met de onderliggende deelvragen. Paragraaf 1.5. beschrijft

[1] De rijksoverheid is het landelijk bestuur van Nederland en bestaat uit ministeries, uitvoeringsorganisaties en organisaties zoals de Tweede Kamer en de Algemene Rekenkamer (Ensie, 2016).

zowel de maatschappelijke als de wetenschappelijke relevantie van het onderzoek en de laatste paragraaf (1.6.) beschrijft in hoofdlijnen hoe het onderzoek is uitgevoerd.

1.2. Gebiedsverkenning

Dit onderzoek vond plaats binnen een wetenschappelijk gebied, waarin basisdefinities worden gebruikt. Deze paragraaf geeft informatie over het gebied informatiebeveiliging, het daarbij horende taalgebruik[2] en de gehanteerde definities. De focus binnen het informatiebeveiligingsgebied ligt op centrale aansturing van de informatiebeveiliging. De volgende begrippen worden hier behandeld:

- Informatiebeveiliging (information security);
- Informatiebeveiligingsbeheer (information security governance).

Informatiebeveiliging (information security):
De meest voorkomende definitie van informatiebeveiliging uit de literatuur is gebaseerd op de volgende triade[3] van eigenschappen (Lundgren & Moller, 2017):

- Vertrouwelijkheid: de eigenschap dat de informatie niet beschikbaar wordt gemaakt voor onbevoegde personen, entiteiten of processen;
- Integriteit: de mate waarin informatie accuraat en compleet is;
- Beschikbaarheid: eigenschap dat de informatie beschikbaar en bruikbaar is als een bevoegd persoon de informatie nodig heeft.

Informatiebeveiligingsbeheer (information security governance):
Informatiebeveiligingsbeheer accentueert de hoofdrol van het topmanagement in de manier waarop wordt omgegaan met informatiebeveiliging. Informatiebeveiligingsbeheer bestaat uit de volgende elementen (von Solms, 2006):

- De betrokkenheid van het topmanagement op het gebied van management en leiderschap bij goede informatiebeveiliging;
- Juiste organisatiestructuren voor het afdwingen van een goede informatiebeveiliging;
- Gebruikersbewustzijn en betrokkenheid, voor goede informatiebeveiliging;
- Het nodige beleid, procedures, processen, technologieën en compliance-mechanismen voor naleving.

Alle bovenstaande elementen werken samen met het doel dat de vertrouwelijkheid, de integriteit en de beschikbaarheid van de elektronische middelen van de organisatie te allen tijde worden gehandhaafd.

1.3. Probleemstelling

Informatiebeveiliging is het proces van vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit, alsmede het treffen, onderhouden en controleren van bijbehorende maatregelen. Informatiebeveiliging vormt een belangrijk kwaliteitsaspect van de informatievoorziening van de Nederlandse rijksoverheid. Het beveiligen van informatie is echter geen eenmalige zaak, maar een proces waarbij steeds de Plan-Do-Check-Act cyclus wordt doorlopen (Ministerie van Binnenlandse Zaken en Koninkrijkrelaties, 2017; von Solms, 2006). Binnen de Nederlandse rijksoverheid is het doorlopen van dit proces een verantwoordelijkheid van de departementale top (Balkenende, 2007; Ollongren, 2017). De vraag is: in

[2] In het taalgebruik wordt tevens de Engelse vertaling van de begrippen gegeven. Dit is noodzakelijk omdat in de literatuurstudie gezocht is aan de hand van de Engelstalige begrippen.
[3] Deze triade staat in het Engels bekend als CIA (Confidentiality, Integrity, Availability) (Lundgren & Moller, 2017)

hoeverre heeft de departementale top inzicht in en grip op de informatiebeveiliging binnen het departement?

1.4. Opdrachtformulering

Het doel van dit onderzoek is het toetsen van theoretische inzichten op het gebied van centrale aansturing van informatiebeveiliging aan de toepassing van deze inzichten bij een nationale departementale organisatie in de praktijk. De centrale onderzoeksvraag luidt:

> "Hoe worden theoretische inzichten op het gebied van centrale aansturing van informatiebeveiliging toegepast bij een nationale departementale organisatie in de praktijk?"

Om de onderzoeksvraag te beantwoorden zijn de volgende twee deelvragen opgesteld:

1. Wat zijn de theoretische inzichten op het gebied van de centrale aansturing van de informatiebeveiliging?
2. Hoe wordt omgegaan met de centrale aansturing van de informatiebeveiliging bij een nationale departementale organisatie in de praktijk?

De eerste deelvraag maakt deel uit van het literatuuronderzoek en vormt de basis voor hoofdstuk 2: Theoretisch kader. De tweede vraag vormt de basis voor het empirisch onderzoek en is onderdeel van hoofdstuk 3: Methodologie.

1.5. Relevantie

1.5.1. Maatschappelijke relevantie

De Nederlandse rijksoverheid heeft een verplichting richting haar burgers, die steeds hogere verwachtingen hebben van wat de overheid voor ze kan betekenen. Nederlandse burgers verwachten tegenwoordig dat ze de rijksoverheid niet alleen kunnen bezoeken of bellen, maar ook dat informatie online beschikbaar wordt gesteld en dat ambtenaren via e-mail of webchat bereikbaar zijn (Leest, 2018). Huidige ontwikkelingen zoals IoT en AI doen deze verwachtingen alleen maar toenemen. Van de Nederlandse rijksoverheid wordt verwacht dat ze door deze nieuwe technieken de overheid efficiënter laat werken en een betere dienstverlening biedt. Daarnaast wordt verwacht dat door een juiste toepassing van informatiebeveiliging de gegevens van burgers veilig zijn. De uitdaging hier is dat de Nederlandse rijksoverheid moet anticiperen op de snelle technologische ontwikkelingen maar tegelijkertijd de informatiebeveiliging moet waarborgen. Zoals eerder beschreven is informatiebeveiliging een zaak van de departementale top (Balkenende, 2007; Ollongren, 2017). Daarom is het maatschappelijk relevant om te toetsen of de theoretische inzichten op het gebied van de centrale aansturing van de informatiebeveiliging ook toegepast worden binnen de Nederlandse rijksoverheid, zeker gezien de verplichtingen die de Nederlandse rijksoverheid heeft ten aanzien van de Nederlandse burgers.

1.5.2. Wetenschappelijke relevantie

Cuganesan, Steele, en Hart (2017) stellen dat ondersteuning van het topmanagement een belangrijke invloed heeft op informatiebeveiliging, maar ook dat de effecten hiervan zelden empirisch worden onderzocht. Slechts een paar studies beschrijven de empirisch relatie tussen ondersteuning door het topmanagement en de effecten op informatiebeveiliging. Daarnaast stellen Soomro, Shah, en Ahmed (2016) vast dat de hoeveelheid artikelen gepubliceerd in de afgelopen jaren op het gebied van de managementrol in informatiebeveiliging groeit; er is een onderzoekstrend ontstaan op dit wetenschappelijk vakgebied.

1.6. Aanpak in hoofdlijnen

In hoofdstuk 2 wordt de relevante literatuur besproken, om het theoretisch kader dat betrekking heeft op de centrale aansturing van informatiebeveiliging helder te krijgen. Vanuit de literatuur ontstaat een overzicht van de belangrijkste facetten op het gebied van de centrale aansturing van informatiebeveiliging. Hoofdstuk 3 beschrijft op welke manier het theoretisch kader getoetst werd aan de empirie. In hoofdstuk 4 worden de resultaten van het empirisch onderzoek gepresenteerd en het laatste hoofdstuk (5) sluit af met de discussie, conclusies en aanbevelingen.

2. Theoretisch kader

In het vorige hoofdstuk is aan de hand van de onderzoeksvraag een aantal deelvragen geformuleerd. Dit hoofdstuk beantwoordt de eerste deelvraag aan de hand van een literatuurstudie[4].

Deelvraag 1: Wat zijn de theoretische inzichten op het gebied van de centrale aansturing van de informatiebeveiliging?

2.1. Resultaten en conclusies

2.1.1. Ontwikkelingen op het gebied van informatiebeveiliging

De ontwikkelingen op het gebied van informatiebeveiliging kunnen op verschillende manieren beschreven worden. von Solms (2000) beschrijft de ontwikkelingen aan de hand van verschillende golven. In eerste instantie spreekt von Solms (2000) over drie golven, waarbij de eerste golf gekenmerkt wordt door een puur technische benadering van informatiebeveiliging. De tweede golf beschrijft von Solms (2000) als de managementgolf. Deze wordt gekenmerkt door een groeiende realisatie bij het management van het belang van informatiebeveiliging, waarbij het topmanagement betrokken raakte bij de uitvoering ervan. De derde golf kenmerkt zich vooral door standaardisatie van informatiebeveiliging. Een aantal jaren later onderkent von Solms (2006) een vierde golf op het gebied van informatiebeveiliging. Deze golf heeft betrekking op de ontwikkeling en de cruciale rol van informatiebeveiligingsbeheer.

In informatiebeveiligingsbeheer is duidelijk de verantwoordelijkheid van het management voor de informatiebeveiliging terug te vinden. Die bestaat uit het geheel van verantwoordelijkheden uitgeoefend door het management met als doel de strategische richting van informatiebeveiliging te bieden, ervoor te zorgen dat doelstellingen voor informatiebeveiliging worden behaald, vast te stellen dat informatiebeveiligingsrisico's op de juiste manier worden afgehandeld en dat informatie-beveiligingsmiddelen op een verantwoorde wijze gebruikt worden (Abu-Musa, 2010). Kenmerk van deze vierde golf is dat het topmanagement de druk voelde toen het persoonlijk verantwoordelijk werd gehouden voor de informatiebeveiliging (von Solms, 2006). Informatiebeveiligingsbeheer onderstreept de essentiële rol van het topmanagement in de manier waarop wordt omgegaan met informatiebeveiliging. Barton, Tejay, Lane, en Terrell (2016) concluderen in hun studie dat informatiebeveiligingsbeheer een primaire rol is van het topmanagement. Informatiebeveiligings-beheer bestaat uit de volgende elementen (von Solms, 2006):

- De betrokkenheid van het topmanagement op het gebied van management en leiderschap bij goede informatiebeveiliging;
- Juiste organisatiestructuren voor het afdwingen van een goede informatiebeveiliging;
- Gebruikersbewustzijn en betrokkenheid voor een goede informatiebeveiliging;
- Het nodige beleid, procedures, processen, technologieën en compliance-mechanismen voor naleving.

Alle bovenstaande elementen werken samen om te zorgen dat de vertrouwelijkheid, de integriteit en de beschikbaarheid (CIA) van de elektronische middelen van de organisatie te allen tijde worden gehandhaafd.

[4] In bijlage 1 wordt uitvoerig beschreven welke zoekstategie gehanteerd is voor het literatuuronderzoek en hoe de uitvoering van de zoekstategie is verlopen.

2.1.2. Betrokkenheid topmanagement bij informatiebeveiliging

von Solms (2006) beschrijft dat informatiebeveiliging start met de toewijding van het management aan informatiebeveiliging. Hierbij wordt informatiebeveiliging beschouwd als een strategisch aspect dat cruciaal is voor het bestaan van de organisatie en voor de beheersing van de risico's die de organisatie loopt op het gebied van informatiebeveiliging. Uit organisatorisch onderzoek blijkt dat leiderschap in het algemeen een belangrijke rol speelt bij het vormgeven van overtuigingen over het werk en de vereiste taken (Wang, Tsui, & Xin, 2011). Ernest Chang en Ho (2006) geven aan dat vanuit een breder kader het management in de basis verantwoordelijk is voor zakelijke aangelegenheden en dus ook voor de informatiebeveiliging. Informatiebeveiliging is primair een managementkwestie, dus het topmanagement moet zich bewust zijn van het belang van de ontwikkeling en implementatie van informatiebeveiliging binnen de organisatie. Ook Atkins (2013) benadrukt dit: als het management informatiebeveiliging juist prioriteert en behandelt als alle andere beveiligingsissues dan is er geen twijfel dat de informatie beter beschermd is. De bescherming van data en informatie dient onderdeel van de bedrijfsstrategie te zijn omdat het concurrentievoordeel kan bieden. Falen of gebrek aan focus op het gebied van informatiebeveiliging is een managementfout, omdat informatiebeveiliging niet hoog genoeg geprioriteerd is. Het belang van de betrokkenheid van het topmanagement wordt door meerdere onderzoekers beschreven. Hier volgt een opsomming van wetenschappers die dit onderbouwen:

- Ondersteuning door het topmanagement signaleert het belang van informatiebeveiliging voor de rest van de organisatie (Kayworth & Whitten, 2010; Rocha Flores & Ekstedt, 2016);
- Betrokkenheid van het topmanagement is belangrijk voor het bereiken van effectieve informatiebeveiliging in organisaties (Boss, Kirsch, Angermeier, Shingler, & Boss, 2009; Bulgurcu, Cavusoglu, & Benbasat, 2010; Hu, Hart, & Cooke, 2007; McFadzean, Ezingeard, & Birchall, 2006; Veiga & Eloff, 2007);
- Ernst en Young (2012) als geciteerd in (Soomro et al., 2016) vinden dat informatiebeveiliging moet worden beschouwd als een prioriteit op bestuursniveau en dat de verantwoordelijkheid niet beperkt mag worden tot de chief information officer (CIO);
- Barton et al. (2016) tonen in hun studie aan dat vertrouwen van het topmanagement in informatiebeveiliging leidt tot grotere informatiebeveiligingsassimilatie in organisaties waarbij de deelname van het topmanagement aan informatiebeveiligingsbeheer wordt vergroot. Dit ondersteunt het argument dat sponsoring door het topmanagement cruciaal is voor een succesvolle informatiebeveiliging.

Ondanks dat het onderzoek het belang van betrokkenheid van het topmanagement bij informatie-beveiliging aantoont, is er niet altijd voldoende toewijding en betrokkenheid van dit topmanagement bij de informatiebeveiliging (Ernest Chang & Ho, 2006; Hu et al., 2007).

Onderzoek toont aan dat effectieve informatiebeveiliging organisatorische risico's vermindert en dat betrokkenheid van topmanagement cruciaal is voor effectieve informatiebeveiliging. Deze betrokkenheid wordt aangetoond door middelen aan te wenden voor informatiebeveiliging waarbij rollen en verantwoordelijkheden worden toegekend (paragraaf 2.3.3.), het communiceren van de visie op informatiebeveiliging richting de gebruikers (paragraaf 2.3.4.) en het monitoren van compliance (paragraaf 2.3.5.) (Barton et al., 2016).

2.1.3. Organisatiestructuren voor het afdwingen van informatiebeveiliging

von Solms (2006) beschrijft dat informatiebeveiliging ondersteund dient te worden door een geschikte organisatiestructuur met vermelding van het eigenaarschap en de verantwoordelijkheden die gelden

op de verschillende niveaus. Daarnaast moet deze organisatiestructuur rekening houden met de compliance en het beheer van informatiebeveiliging (von Solms, 2005). Deze organisatiestructuur is enorm belangrijk bij het beheer van informatiebeveiliging (Kayworth & Whitten, 2010). Soomro et al. (2016) geven aan dat informatiebeveiligingsbeheer een organisatiestructuur vereist die rapportage, effectieve communicatie, duidelijke autoriteit en snelle werkstromen mogelijk maakt. De bestaande literatuur ondersteunt een formele organisatiestructuur voor beter beheer van informatiebeveiliging (Kayworth & Whitten, 2010). Daarnaast wordt ook gepleit voor een gedecentraliseerd beslissingssysteem voor effectief beheer van informatiebeveiliging (Soomro et al., 2016). Tenslotte concluderen da Veiga en Martins (2015) dat een organisatie afhankelijk is van een sterke organisatorisch veiligheidscultuur die gecontroleerd wordt door het topmanagement. Soomro et al. (2016); von Solms (2006) lijken elkaar tegen te spreken door aan de ene kant een gedecentraliseerd beslissingssysteem te propageren en aan de andere kant te pleiten voor nadruk op eigenaarschap en verantwoordelijkheid. (Pulkkinen, Naumenko, & Luostarinen, 2007) weten dit te weerleggen door te stellen dat een kader nodig is om overwegingen en beslissingen van het strategisch management op het gebied van informatiebeveiliging te duiden. De uitvoering van dit kader dient plaats te vinden in de praktische organisatie en vanuit dit niveau dient dan weer terugkoppeling gegeven te worden aan het strategische management.

2.1.4. Gebruikersbewustzijn en betrokkenheid bij informatiebeveiliging

In de vorige paragraaf is de organisatiestructuur behandeld die benodigd is voor het afdwingen van informatiebeveiliging. Eigenaarschap en verantwoordelijkheden spelen hierin een belangrijke rol en worden versterkt door bewustmakingsprogramma's voor de gebruikers binnen een organisatie (von Solms, 2006). Ondersteuning door het topmanagement signaleert het belang van informatie-beveiliging voor de rest van de organisatie en kan medewerkers beïnvloeden in hun benadering van informatiebeveiliging (Kayworth & Whitten, 2010; Rocha Flores & Ekstedt, 2016). Daarnaast concludeert Albrechtsen (2007) dat effectieve communicatie van het beveiligingsbeleid en bewustmakingscampagnes noodzakelijk zijn voor goede informatiebeveiliging in de praktijk. In het onderzoek naar de rol van topmanagement en het gedrag van medewerkers wordt niet altijd een significantie relatie gevonden (Hu, Dinev, Hart, & Cooke, 2012; Rocha Flores & Ekstedt, 2016). Cuganesan et al. (2017) vonden in hun onderzoek wel empirische ondersteuning voor de opvatting dat topmanagement de houding van werknemers ten aanzien van de informatiebeveiliging, ook bij grote organisaties, rechtstreeks kan beïnvloeden. De betrokkenheid van het topmanagement is nodig om optimaal profijt te trekken uit informatiebeveiligingstraining en informatiebeveiligings-bewustzijnstraining, en daarnaast voor het ontwikkelen van de informatiebeveiligingscultuur (Boss et al., 2009; Bulgurcu et al., 2010; Hu et al., 2007; McFadzean et al., 2006) Tenslotte zijn programma's en training voor het creëren van bewustwording op het gebied van informatiebeveiliging een verantwoordelijkheid voor het management, om het te integreren in de organisatie (Soomro et al., 2016). Rocha Flores en Ekstedt (2016) onderkennen dat leiderschapsstijl belangrijk is voor het beïnvloeden van de medewerkers. Een hiervoor geschikte leiderschapsstijl is het transformationeel leiderschap. Transformationele leiders richten zich op het welzijn van de organisatie, genereren bewustwording en acceptatie van het organisatiedoel en motiveren werknemers verder te kijken dan hun eigenbelang: naar het organisatiebelang. In het kader van informatiebeveiliging betekent dit dat de leider een veiligheidsvisie moet formuleren, zodat alle medewerkers de doelstelling van het informatiebeveiligingsbeleid gemakkelijk en goed kunnen begrijpen.

2.1.5. Compliance informatiebeveiliging

da Veiga en Martins (2015) vonden aan dat ondersteuning van het topmanagement op het gebied van informatiebeveiliging een positieve invloed heeft op de naleving door medewerkers van het informatiebeveiligingsbeleid van een organisatie. Betrokkenheid van het topmanagement is een

voorwaarde om effectieve naleving van het informatiebeveiligingsbeleid te bewerkstelligen (Boss et al., 2009; Bulgurcu et al., 2010; Hu et al., 2007; McFadzean et al., 2006). Ifinedo (2014) concludeert dat onderzoek op het gebied van naleving van informatiebeveiliging zich richt op attitude en gedrag van werknemers, maar dat het onderliggende thema in dit onderzoek de rol van het management is bij het vormgeven van de gewenste overtuigingen, attitudes en gedrag. Tenslotte merkten Puhakainen en Siponen (2010) op dat zichtbare topmanagementondersteuning (zoals actief beveiligings-aangelegenheden promoten en het goede voorbeeld geven) impact had op de houding van medewerkers op het gebied van informatiebeveiliging en belangrijk was voor het naleven van beleidsregels door medewerkers op het gebied van informatiebeveiliging.

2.1.6. Conclusies theoretisch kader

Uit het literatuuronderzoek blijkt dat de ontwikkelingen op het gebied van informatiebeveiliging niet hebben stilgestaan. Waar in het begin vooral voor een technische benadering werd gekozen, ligt de nadruk nu op de managementbenadering. Een benadering waarbij informatiebeveiligingsbeheer en het topmanagement onlosmakelijk met elkaar verbonden zijn (von Solms, 2000, 2006). Informatiebeveiligingsbeheer impliceert betrokkenheid van het topmanagement, juiste organisatie-structuren voor het afdwingen, gebruikersbewustzijn, betrokkenheid en compliance ten aanzien van alle facetten van informatiebeveiliging (von Solms, 2006).

Het belang van de betrokkenheid van topmanagement wordt door meerdere onderzoekers beschreven. De ondersteuning door het topmanagement duidt op het belang van informatie-beveiliging voor de rest van de organisatie (Kayworth & Whitten, 2010; Rocha Flores & Ekstedt, 2016). Voor de betrokkenheid van het topmanagement bij informatiebeveiliging is de conclusie dat betrokkenheid van het topmanagement essentieel is voor het bereiken van effectieve informatie-beveiliging in organisaties (Boss et al., 2009; Bulgurcu et al., 2010; Hu et al., 2007; McFadzean et al., 2006; Veiga & Eloff, 2007). Daarnaast is sponsoring door het topmanagement van cruciaal belang is voor een succesvolle informatiebeveiliging (Barton et al., 2016). De conclusie die hieruit getrokken kan worden is dat zonder betrokkenheid van het topmanagement het belang van informatiebeveiliging niet duidelijk wordt voor de rest van de organisatie, zodat effectieve en succesvolle informatie-beveiliging niet mogelijk is. Ondanks deze conclusie is er niet altijd voldoende toewijding en betrokkenheid van ditzelfde topmanagement bij de informatiebeveiliging (Ernest Chang & Ho, 2006; Hu et al., 2007). Het gevolg van de afwezigheid van de betrokkenheid bij de informatiebeveiliging is dat informatie niet op een correcte manier beschermd wordt (Atkins, 2013) en het bestaan van organisaties in gevaar kan brengen (von Solms, 2006). De betrokkenheid van topmanagement wordt aangetoond door middelen aan te wenden voor informatiebeveiliging waarbij rollen en verantwoordelijkheden worden toegekend, het communiceren van de visie op informatiebeveiliging richting de gebruikers en het monitoren van de compliance op het gebied van informatiebeveiliging (Barton et al., 2016).

De organisatiestructuur voor het afdwingen van informatiebeveiliging is zeer belangrijk bij het beheer van informatiebeveiliging (Kayworth & Whitten, 2010). Zonder vermelding van het eigenaarschap en de verantwoordelijkheden die gelden op verschillende niveaus is geen ondersteuning op het gebied van informatiebeveiliging mogelijk (von Solms, 2006). Daarnaast is een sterke organisatorische veiligheidscultuur niet mogelijk zonder deze organisatiestructuur (da Veiga & Martins, 2015). Het is van belang om een formele organisatiestructuur te hebben (Kayworth & Whitten, 2010) waarbij de nadruk aan de ene kant wordt gelegd op eigenaarschap en verantwoordelijkheden (von Solms, 2006) en aan de andere kant op een gedecentraliseerd beslissingssysteem (Soomro et al., 2016). Dit hoeft niet tegenstrijdig te zijn, want er is een kader nodig om overwegingen en beslissingen van het strategisch management op het gebied van informatiebeveiliging te duiden, en de uitvoering daarvan dient plaats te vinden in de organisatie (Pulkkinen et al., 2007). Het topmanagement moet een

organisatiestructuur creëren die rapportage, effectieve communicatie, duidelijke autoriteit en snelle werkstromen mogelijk maakt (Soomro et al., 2016).

Voor het gebruikersbewustzijn en de betrokkenheid bij informatiebeveiliging is de conclusie dat het topmanagement de houding van medewerkers rechtstreeks kan beïnvloeden (Cuganesan et al., 2017; Kayworth & Whitten, 2010; Rocha Flores & Ekstedt, 2016). Zonder de betrokkenheid van het topmanagement is de informatiebeveiliging en de informatiebeveiligingscultuur veel minder effectief (Boss et al., 2009; Bulgurcu et al., 2010; Hu et al., 2007; McFadzean et al., 2006). De hoofdconclusie is dat effectieve communicatie van het beveiligingsbeleid noodzakelijk is voor goede informatiebeveiliging in de praktijk (Albrechtsen, 2007). Het topmanagement is integraal verantwoordelijk voor het creëren van bewustwording op het gebied van informatiebeveiliging (Soomro et al., 2016). De eindconclusie is dat de leiderschapsstijl belangrijk is voor het beïnvloeden van de medewerkers. Rocha Flores en Ekstedt (2016) geven aan dat transformationeel leiderschap hier geschikt voor is. Daarbij richten leiders zich op het welzijn van de organisatie, bewustwording en acceptatie van het organisatiedoel en het motiveren van medewerkers om te denken in het organisatiebelang. Een veiligheidsvisie op het gebied van informatiebeveiliging kan hiervoor als basis dienen.

Op het gebied van compliance van informatiebeveiliging is de conclusie dat de ondersteuning van het topmanagement op het gebied van informatiebeveiliging een positieve invloed heeft op de naleving van de medewerkers (da Veiga & Martins, 2015). Zonder deze betrokkenheid van het topmanagement is effectieve naleving van het informatiebeveiligingsbeleid niet mogelijk (Boss et al., 2009; Bulgurcu et al., 2010; Hu et al., 2007; McFadzean et al., 2006). Een belangrijke rol voor het management op het gebied van compliance van informatiebeveiliging is het vormgeven van gewenste overtuigingen, attitudes en gedrag van werknemers (Ifinedo, 2014). Daarnaast dient het topmanagement zichtbaar ondersteuning te geven door middel van het promoten van informatiebeveiliging en het goede voorbeeld geven in het eigen nalevingsgedrag.

2.2. Doel van het vervolgonderzoek

Doelstelling van het vervolgonderzoek was het in kaart brengen van de invulling die in de praktijk wordt gegeven aan de centrale aansturing van de informatiebeveiliging bij een nationale departementale organisatie. Deze doelstelling is relevant omdat dit uiteindelijk tot antwoorden moest leiden op deelvraag 2, die luidde:

Hoe wordt omgegaan met de centrale aansturing van de informatiebeveiliging bij een nationale departementale organisatie in de praktijk?

Door de gevonden theoretische inzichten te toetsen aan de empirie volgt uiteindelijk een antwoord op de geformuleerde onderzoeksvraag:

> “Hoe worden theoretische inzichten op het gebied van centrale aansturing van informatiebeveiliging toegepast bij een nationale departementale organisatie in de praktijk?”

Het empirisch onderzoek richtte zich op de vraag welke theoretische inzichten op het gebied van centrale aansturing in de praktijk worden toegepast. Om deze vraag te kunnen beantwoorden is informatie nodig waaruit afgeleid kon worden hoe deze inzichten beschreven worden in de beleids-documenten van de departementale organisatie en hoe het topmanagement deze inzichten toepast in de praktijk.

3. Methodologie

Essentieel in dit onderzoek is het beantwoorden van de praktijkgerichte deelvraag. De manieren waarop data wordt gegenereerd, zijn een belangrijk aspect in een onderzoeksontwerp. Dit hoofdstuk is de methodologische verantwoording, waarbij de keuzes in de aanpak van het onderzoek nauwkeurig beschreven worden (Saunders et al., 2015).

3.1. Conceptueel ontwerp: keuze van onderzoeksmethode

Doelstelling van het vervolgonderzoek was het in kaart te brengen hoe in de praktijk invulling wordt gegeven aan de centrale aansturing van de informatiebeveiliging bij een nationale departementale organisatie. Om de doelstelling te kunnen bereiken is informatie nodig waaruit herleid kon worden hoe nu wordt omgegaan binnen een nationale departementale organisatie met de centrale aansturing van informatiebeveiliging. Deze informatie kon op verschillende manieren gevonden worden. Er zijn diverse beleidsdocumenten die richting geven aan informatiebeveiliging binnen de organisatie, en daarnaast vormden leden van het topmanagement een gegevensbron aangezien zij uitvoering dienen te geven aan de theoretische inzichten op het gebied van centrale aansturing van informatiebeveiliging.

De casestudy werd geselecteerd als methode, omdat deze gebruikmaakt van een empirisch onderzoek van een bepaald hedendaags verschijnsel binnen de actuele context en verschillende soorten bewijsmateriaal oplevert (Verschuren & Doorewaard, 2015). Daarnaast bood de casestudy de gelegenheid om een diepgaander onderzoek uit te voeren, het is een waardevolle manier om een bestaande theorie te onderzoeken (Saunders et al., 2015). De uitgevoerde casestudy is gebaseerd op de enkelvoudige en ingebedde case dimensie, waarbij sprake was van een dwarsdoorsnedeonderzoek[5] (Saunders et al., 2015). Deze casestudy heeft de volgende kenmerken (Verschuren & Doorewaard, 2015):

1. Een smal domein;
2. Een arbeidsintensieve benadering;
3. Meer diepte dan breedte;
4. Een selecte steekproef;
5. Kwalitatieve data en dito onderzoeksmethoden.

De casestudy vereiste ook het gebruik van meerdere databronnen en het toepassen van triangulatie[6] op deze databronnen.

3.2. Technisch ontwerp: uitwerking van de methode

Deze paragraaf geeft het technisch ontwerp weer van deze casestudy. De casestudy werd gebaseerd op een kwalitatief onderzoek met de multimethode. Dit houdt in dat gebruik gemaakt werd van meer dan één kwalitatieve methode voor gegevensverzameling en corresponderende kwalitatieve analyse-procedure(s) (Saunders et al., 2015). De methode voor gegevensverzameling komt in deze paragraaf aan bod, de volgende paragraaf behandelt de analyseprocedure(s). Belangrijk voor het technisch ontwerp is dat de onderzoeker gekenmerkt kon worden als intern of participerend onderzoeker, waardoor bepaalde bronnen toegankelijker zijn (Saunders et al., 2015).

[5] "Het bestuderen van een bepaald verschijnsel (of verschillende verschijnselen) op een bepaald tijdstip. Op een tijdstip data verzamelen bij vaak eenzelfde groep." (Saunders et al., 2015, p. 93)

[6] "Het gebruik van twee of meer onafhankelijke gegevensbronnen of methoden om gegevens te verzamelen binnen één onderzoek, om te controleren of de gegevens je werkelijk dat vertellen wat je denkt dat ze je vertellen," (Saunders et al., 2015, p. 84)

3.2.1. Documentaire secundaire data

De documentaire secundaire gegevens die benodigd waren voor dit onderzoek zijn schriftelijke documenten; brief, persoonlijke brief, kamerbrief, nota, intern memorandum, notitie, rapport, fax of e-mail. Deze documenten konden gevonden worden via het internet, het intranet van de departementale organisatie en aangeleverd worden door de respondenten die onderdeel uitmaakte van dit onderzoek. Het is belangrijk om de geschiktheid van de gevonden secundaire gegevens te beoordelen (Saunders et al., 2015), om uiteindelijk antwoord te kunnen geven op deelvraag.

3.2.2. Semigestructureerde interviews

Voor het verzamelen van primaire kwalitatieve data werden semigestructureerde interviews gehouden. Daarbij kan gekozen worden uit een reeks interviewthema's, maar het biedt ook kansen om de volgorde waarin de vragen worden gesteld te variëren. Tevens bestaat de mogelijkheid om nieuwe vragen te stellen in de context van de onderzoekssituatie (Saunders et al., 2015). De semigestructureerde interviews moesten bijdragen aan het beantwoorden van deelvraag 2. Daarom werd gekozen voor een doelgerichte steekproef. Dit is een selecte steekproefmethode waarbij het oordeel van de onderzoeker bepaalt welke respondenten deel uitmaken van de steekproef (Saunders et al., 2015). Saunders et al. (2015) geven aan dat bij het verzamelen van kwalitatieve data door middel van interviews geïnterviewd moet worden tot er dataverzadiging[7] optreedt. De respondenten werden specifiek geselecteerd op hun specifieke managementrol binnen de departementale organisatie.

3.3. Gegevensanalyse

Voordat gestart kon worden met de gegevensanalyse is de eerste stap het creëren van transcripten van de verzamelde data (Saunders et al., 2015). Dit betekende dat de semigestructureerde interviews met toestemming van de respondent werden opgenomen en daarna getranscribeerd. Daarnaast werd de documentaire secundaire data geanonimiseerd, per document opgeslagen en opgeschoond. De eerste stap in het analyseproces was het samenvatten van alle transcripten, waarbij de belangrijke zaken vermeld werden in de samenvatting. De tweede stap het indelen van de data in categorieën (Saunders et al., 2015). De categorieën werden ontwikkeld aan de hand van het theoretisch kader en vormden de eenheden van de data. De gegevensanalyse werd ondersteund door Computer Assisted Qualitative Data Analyses Software[8] (CAQDAS). Systematisch gebruik van CAQDAS kan bijdragen aan de continuïteit van de gegevensanalyse en het onderzoek op methodisch vlak transparanter en strakker maken (Saunders et al., 2015).

3.4. Reflectie t.a.v. validiteit, betrouwbaarheid en ethische aspecten

3.4.1. Validiteit

3.4.1.1. Interne validiteit

De interne validiteit van dit onderzoek betreft de kwaliteit van de conclusies uit dit onderzoeksontwerp (Saunders et al., 2015). De secundaire data moesten de informatie leveren om de onderzoeksvraag te beantwoorden, anders was er sprake van niet-valide antwoorden. Daarnaast moet de autoriteit van de secundaire data beoordeeld worden (Saunders et al., 2015). Voor de semigestructureerde

[7] "De fase waarin nieuwe data die worden verzameld weinig tot geen nieuwe inzichten meer bieden." (Saunders et al., 2015, p. 162).

[8] "Analysesoftware die gebruikt kan worden in een of meer van de volgende processen bij het analyseren van kwalitatieve data: projectmanagement, databeheer, en het opstellen van hypothesen en theorieën." (Saunders et al., 2015, p. 304)

interviews was de validiteit van het onderzoek gewaarborgd. De hoge mate van validiteit van semigestructureerde interviews werd bereikt doordat vragen nader konden worden toegelicht, er dieper op antwoorden kon worden ingegaan en onderwerpen vanuit verschillende invalshoeken konden worden besproken (Saunders et al., 2015). Als laatste werd de validiteit gewaarborgd door het onderzoeksdesign waarbij triangulatie van de data plaatsvond om zeker te stellen dat het juiste gemeten werd in dit onderzoek.

3.4.1.2. Externe validiteit

De externe validiteit[9] (generaliseerbaarheid) van de casestudy is zeer beperkt. Dit komt onder andere omdat het een enkelvoudige casus betreft. Dit betekent dat de resultaten en conclusies van dit onderzoek niet per definitie gegeneraliseerd mogen worden. Volgens Saunders et al. (2015) is dit geen probleem als het doel van het onderzoek niet het generaliseren is van de theorie naar alle populaties. Dit onderzoek richtte zich op een specifieke situatie bij een departementale organisatie.

3.4.2. Betrouwbaarheid

Betrouwbaarheid heeft te maken met de mate waarin de dataverzamelingstechnieken en analyse-procedures tot consistente bevindingen leiden (Saunders et al., 2015). Saunders et al. (2015) geven aan dat er vier verschillende factoren zijn die de betrouwbaarheid kunnen aantasten. De eerste factor is de deelnemersfout[10]. Dit werd in dit onderzoek voorkomen doordat de geïnterviewde zelf met een voorstel mag komen over de tijd en plaats waar het interview gaat plaatsvinden. De tweede factor is de deelnemersvertekening[11]. Deze werd voorkomen omdat de geïnterviewden geen werkrelatie hebben met de onderzoeker, hun anonimiteit in het onderzoek was gewaarborgd. De derde factor is de waarnemersfout[12], deze werd voorkomen doordat de interviews semigestructureerd zijn en door één onderzoeker werden afgenomen. De laatste factor is de waarnemersbias, waarbij antwoorden verschillend geïnterpreteerd worden. Deze werd voorkomen doordat duidelijk gekozen werd voor een methode voor het analyseren van de antwoorden.

3.4.3. Ethische aspecten

Saunders et al. (2015) schrijven voor dat een onderzoek behalve methodologisch gezond ook moreel verdedigbaar moet zijn tegenover alle betrokkenen bij het onderzoek. In dit onderzoek werd rekening gehouden met de volgende ethische aspecten:

- Deelnemers werden niet gedwongen om mee te doen aan dit onderzoek;
- Alle deelnemers waren vrij om zich elk moment terug te trekken uit dit onderzoek en werden hierover vooraf geïnformeerd;
- Alle verzamelde informatie van de deelnemers van dit onderzoek werd vertrouwelijk behandeld en anoniem verwerkt in dit onderzoeksverslag;
- De onderzoeker trachtte op een zo objectief mogelijke manier alle data te analyseren en te rapporteren.

[9] “Algemeen: de mate waarin onderzoeksresultaten uit een steekproef gegeneraliseerd kunnen worden naar eenheden buiten de steekproef” (Saunders et al., 2015, p. 96).
[10] “Fout die kan ontstaan als deelnemers aan het onderzoek in situaties bestudeerd worden die niet in overeenstemming zijn met hun normale gedragspatronen, waardoor afwijkende antwoorden gegeven kunnen worden” (Saunders et al., 2015, p. 94).
[11] “Vertekening die kan ontstaan als deelnemers aan een onderzoek onnauwkeurige antwoorden geven om de resultaten van het onderzoek te vervormen” (Saunders et al., 2015, p. 94)
[12] “Systematische fout die door waarnemers wordt gemaakt, bijvoorbeeld ten gevolge van vermoeidheid” (Saunders et al., 2015, p. 95)

4. Resultaten

Dit hoofdstuk geeft weer hoe de uitvoering van het onderzoek verlopen is en met name de afwijkingen ten opzichte van het oorspronkelijke plan worden belicht. De afsluiting van dit is hoofdstuk is de presentatie van de resultaten.

4.1. Uitvoering onderzoek

4.1.1. Onderzoeksmethode casestudy

Doelstelling van het vervolgonderzoek was het in kaart te brengen hoe in de praktijk invulling wordt gegeven aan de centrale aansturing van de informatiebeveiliging bij een nationale departementale organisatie. De uitgevoerde casestudy is gebaseerd op de enkelvoudige en ingebedde case dimensie. De case die de onderzoeker heeft gekozen is een departementale organisatie waar de onderzoeker zelf een medewerker is. De reden hiervoor is dat de onderzoeker dan gekenmerkt kan worden als intern onderzoeker waardoor bepaalde bronnen toegankelijker waren (Saunders et al., 2015). Bij deze nationale departementale organisatie is specifiek gekeken naar de rol van de departementale top op het gebied van informatiebeveiliging.

4.1.2. Semigestructureerde interviews

Voor het verzamelen van primaire data werden semigestructureerde interviews gehouden. Hierbij is gekozen voor een selecte-steekproefmethode. Hiervoor zijn door de onderzoeker binnen de departementale top een aantal functionarissen geselecteerd die in aanmerking kwamen om geïnterviewd te worden. Het initiële plan was om vier a vijf functionarissen te benaderen die binnen departementale top een managementfunctie bekleden of direct betrokken waren bij de informatiebeveiliging vanuit de departementale top. Deze functionarissen zijn eerst door de onderzoeker telefonisch benaderd met de vraag of ze wilden meewerken aan dit onderzoek. Daarna hebben ze een e-mail ontvangen met meer informatie over de inhoud van het onderzoek. In de e-mail is specifiek toegevoegd een informatieblad voor de deelnemer van het interview (zie bijlage 2 Informatieblad deelnemer interview). Dit informatieblad was bedoeld om de respondenten een duidelijk beeld te schetsen van de inhoud van het onderzoek en wat de interview opzet was. Helaas waren niet alle respondenten die geselecteerd waren bereid mee te werken aan dit onderzoek. In totaal zijn er twee personen formeel geïnterviewd. Gevolg hiervan is dat er geen sprake is van dataverzadiging aan de hand van de interviews. Voor de interviews is een interview protocol samengesteld (zie bijlage 3 Interviewprotocol). Voor de interviews is gekozen voor een reeks interviewthema's die vanuit het literatuuronderzoek gekozen zijn. De volgende thema's zijn opgenomen in het interviewprotocol met de bijbehorende deelvragen:

- Betrokkenheid topmanagement bij informatiebeveiliging;
- Organisatiestructuren voor het afdwingen van informatiebeveiliging;
- Gebruikersbewustzijn en betrokkenheid bij informatiebeveiliging;
- Compliance informatiebeveiliging.

4.1.3. Documentaire secundaire data

De documentaire secundaire gegevens die benodigd waren voor dit onderzoek waren schriftelijke documenten. Deze documenten zijn door de onderzoeker gezocht op het internet, het intranet van de departementale organisatie en zijn aangedragen door de respondenten die deel uitmaken van dit onderzoek. Voordat de documenten als documentaire secundaire data zijn opgenomen is eerst de geschiktheid beoordeeld om deelvraag 2 te kunnen beantwoorden. In totaal zijn 21 documenten

geselecteerd voor de gegevensanalyse. De inhoud van de 21 secundaire is hieronder weergegeven in tabel 1

Documentaire secundaire data
Basis richtlijnen informatiebeveiligingsdocumenten vanuit de Nederlandse overheid
Beveiligingsvoorschriften vanuit de Nederlandse overheid
Nederlandse normeringsdocumenten op het gebied van informatiebeveiliging
Departementale aanwijzingen op het gebied van informatiebeveiliging die specifiek voor gemaakt zijn voor een Nederlandse departementale organisatie
Instructies op het gebied van informatiebeveiliging die specifiek gemaakt zijn voor een Nederlandse departementale organisatie

Tabel 1: Inhoud documentaire secundaire data

4.1.4. Gegevensanalyse

In deze paragraaf wordt weergegeven hoe de gegevensanalyse van de ruwe onderzoeksdata heeft plaatsgevonden in dit onderzoek. De eerste stap is dat de semigestructureerde interviews die zijn opgenomen compleet zijn getranscribeerd. Daarna zijn de transcripten van de interviews en de documentaire secundaire data ingevoerd in CAQDAS-programma ATLAS.ti. In de documentaire secundaire data zijn alle documenten uitgebreid bestudeerd en doormiddel van ATLAS.ti zijn er binnen de documenten quotaties aangemaakt. De quotaties zijn uiteindelijk opgedeeld in vier categorieën die ontwikkeld zijn aan de hand van het theoretische kader:

- Betrokkenheid topmanagement bij informatiebeveiliging;
- Compliance informatiebeveiliging;
- Gebruikersbewustzijn en betrokkenheid informatiebeveiliging;
- Organisatiestructuren voor het afdwingen van informatiebeveiliging.

De quotaties zijn per categorie gebundeld vanuit ATLAS.ti. Daarnaar zijn de quotaties doormiddel van het theoretisch kader voorzien van labels die het aandachtgebied weergeven van de quotaties. Voor de vier verschillende categorieën zijn de labels gecreëerd die worden weergeven in tabel 2. Een overzicht van de uitkomsten van de categorieën en labels zijn opgenomen in bijlage 4 Categorieën en labels documentaire secundaire data.

Categorie	Betrokkenheid topmanagement	Organisatiestructuren	Gebruikersbewustzijn	Compliance
Label	Betrokkenheid management	Beslissingssysteem	Betrokkenheid management	Betrokkenheid management
	Strategisch aspect	Eigenaarschap	Bewustmakingprogramma's	Gedrag beïnvloeden
	Ondersteuning beleid	(Formele) organisatiestructuur	Effectieve communicatie	
	Verantwoording management	Rapportagestructuur	Effectieve communicatiebeveiligingsbeleid	
	Toewijding management		Gebruikersbewustzijn	

Tabel 2: Labels categorieën

Voor de semigestructureerde interviews zijn er binnen de transcripten tevens quotaties gemaakt en in dezelfde vier categorieën opgedeeld als voor de documentaire secundaire data is gebeurd. Zowel de gecategoriseerde quotaties van de documentaire secundaire data en de semigestructureerde interviews zijn samengevoegd en geordend per categorie. Binnen alle categorieën is nu per categorie gezocht naar de verbanden die te leggen waren tussen de documentaire secundaire data en de semigestructureerde interviews dit om triangulatie te laten plaatvinden op de beide databronnen. De

resultaten hiervan worden in de vorm van een relaas in paragraaf 4.2 weergegeven. Hierin wordt antwoord gegeven op deelvraag 2: Hoe wordt omgegaan met de centrale aansturing van de informatiebeveiliging bij een nationale departementale organisatie in de praktijk?

4.2. Resultaten

4.2.1. De interne organisatie van een ministerie

Een ministerie valt uiteen in een ministeriële secretarie of het kerndepartement, diensten, instellingen en adviesorganen. Onder de ministeriële secretarie vallen die onderdelen, die de politieke leiding rechtstreeks terzijde staan. Binnen een 'traditionele' ministeriële secretarie kan allereerst de algemene leiding worden onderscheiden. Deze bestaat uit de secretaris-generaal en zijn of haar plaatsvervangers. Tevens heeft de secretaris-generaal de ambtelijke leiding over het ministerie. De positie van de secretaris-generaal als eerste ambtenaar is geformaliseerd in het Koninklijk Besluit van 18 oktober 1988. De feitelijke macht van de secretaris-generaal kan van ministerie tot ministerie verschillen. Hij wordt veelal terzijde gestaan door een plaatsvervanger. De plaatsvervangend secretaris-generaal heeft meestal het interne management van de ministeriële secretarie in zijn of haar portefeuille. De politieke en ambtelijke leiding wordt ondersteund door het bureau secretaris-generaal. Dit verleent assistentie bij de intra- en interdepartementale coördinatie van de beleidsontwikkeling. De term 'algemene leiding' is misleidend: de algemene leiding is niet altijd feitelijk hiërarchisch bovengeschikt aan de beleidsonderdelen. Naast de algemene leiding vormen de beleidsonderdelen de kern van de ministeriële secretarie. De hoofdonderdelen van een ministerie die zich bezighouden met de beleidsontwikkeling worden gewoonlijk directoraten-generaal genoemd. Elk directoraat-generaal valt op zijn beurt uiteen in directies en de directies weer in afdelingen (De Nederlandse grondwet, 2019).

4.2.2. Betrokkenheid topmanagement bij informatiebeveiliging

Op het gebied van betrokkenheid van het topmanagement zijn de volgende resultaten gevonden. De departementale secretaris-generaal van een ministerie is eindverantwoordelijk voor de integrale beveiliging en de inrichting van de ministeriele beveiligingsorganisatie. In die hoedanigheid is hij eindverantwoordelijk voor de implementatie van alle beveiligingskaders in zijn organisatie. Daarbij is bepaald dat het beleid voor informatiebeveiliging wordt vastgesteld en uitgedragen door deze departementale secretaris-generaal. Vanuit de interviews wordt aangegeven dat er ook een beveiligingsbeleid is op het gebied van informatiebeveiliging en dat die wordt opgelegd door de secretaris-generaal.

> Als eindverantwoordelijke voor het beveiligingsbeleid in de organisatie is de departementale secretaris-generaal verantwoordelijk voor de uitvoering van organisatiebrede vraagstukken ten aanzien van informatiebeveiliging.[13]

De directie behoort een duidelijke beleidsrichting aan te geven in overeenstemming met de bedrijfsdoelstellingen, en te demonstreren dat zij informatiebeveiliging ondersteunt en zich hiertoe verplicht. Hiervoor dient de directie een informatiebeveiligingsbeleid uit te brengen en te handhaven voor de gehele organisatie. Dit beleidsdocument voor informatiebeveiliging behoort de betrokkenheid van de directie te verwoorden, evenals de benadering van de organisatie ten aanzien van het beheer van informatiebeveiliging. Daarnaast dient de directie van alle medewerkers te eisen dat ze

[13] De grijze teksten weergegeven bij de resultaten zijn citaten uit documenten van de documentanalyse of uit de interviews die gehouden zijn met de respondenten. De teksten met een * aan het einde komen direct uit de transcripten uit de interviews.

informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures in de organisatie. De directie dient ook actief de beveiliging binnen de organisatie te ondersteunen door duidelijk richting te geven, betrokkenheid te tonen en expliciet verantwoordelijkheden voor informatiebeveiliging toe te kennen en te erkennen. Het eerder vermelde beveiligingsbeleid behoort met geplande tussenpozen, of als zich significantie veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffen is. Vanuit de interviews is te concluderen dat de betrokkenheid vanuit de directie vaak reactief is. Eerst moet er wat gebeuren voordat er gereageerd wordt vanuit de directie.

> Ja, we hebben natuurlijk een beveiligingsbeleid en we hebben ons daaraan te houden.*

Vanuit het perspectief van de bedrijfsvoering is het management verantwoordelijk voor de kwaliteit van de bedrijfsvoering. Die verantwoordelijkheid wordt verticaal gedeeld, van organisatietop tot het afdelingshoofd. Informatiebeveiliging geldt als een integraal onderdeel van de bedrijfsvoering, daarom is het management ook eindverantwoordelijk voor informatiebeveiliging. Een kritische succesfactor die van wezenlijk belang is voor een geslaagde implementatie van informatiebeveiliging in een organisatie is zichtbare steun en betrokkenheid van alle managementniveaus. Vanuit de interviews blijkt dat het management steeds meer betrokken raakt en ook meer geïnteresseerd is wat er allemaal speelt op het gebied van informatiebeveiliging.

> Je merkt wel dat het management steeds meer betrokken raakt en ook meer geïnteresseerd is in wat er allemaal gebeurt en wat er speelt op het gebied van informatiebeveiliging.*

4.2.3. Organisatiestructuren voor het afdwingen van informatiebeveiliging

Op het gebied van organisatiestructuren voor het afdwingen van informatiebeveiliging zijn de volgende resultaten gevonden. De departementale secretaris wijst een departementale beveiligings-ambtenaar aan die zorg draagt voor het toezicht op de integrale beveiliging van het departement, hierover adviseert en ter zake hiervan incidenten laat onderzoeken alsmede zorg draagt voor het toezicht op de organisatie van de beveiliging van het departement. Vanuit de interviews blijkt ook dat de secretaris-generaal een aanwijzing uitgeeft waarbij in beschreven staat dat de departementale organisatie een beveiligingsbeleid dient te verwoorden en dat binnen de departementale organisatie daarvoor een autoriteit is aangewezen.

> De beveiligingsambtenaar rapporteert periodiek over de stand van de departementale integrale beveiliging aan zijn secretaris-generaal.

De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging binnen de organisatie. Hierbij dient de directie het toekennen van deze verantwoordelijkheden en rollen voor informatiebeveiliging in alle lagen van de organisatie goed te keuren. Daarnaast dienen directieverantwoordelijkheden en -procedures te worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen. Het informatiebeveiligingsbeleid behoort een eigenaar te hebben die door de directie goedgekeurde verantwoordelijkheid heeft voor het ontwikkelen, beoordelen en evalueren van het beveiligingsbeleid. Vanuit de interviews blijkt dat de organisatie verantwoordelijkheden en rollen op het gebied van organisatiebeveiliging door de hele organisatie heeft ingeregeld doormiddel van een autoriteit. Deze heeft door de hele organisatie beveiligingcoördinatoren die toezien op de naleving van het beveiligingsbeleid.

> Je hebt natuurlijk de secretaris-generaal, die heeft natuurlijk een aanwijzing waarin hij zegt: “Er moet een beveiligingsbeleid komen”.*

Op het gebied van rapportagestructuren dienen informatiebeveiligingsgebeurtenissen zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd. Vanuit de interviews blijkt dat er een specifieke rapportage structuur is binnen de organisatie om incidenten op het gebied van informatiebeveiliging snel door de organisatie heen te krijgen tot op het juiste niveau.

> Ik denk dat iedereen wel weet bij een incident hoe je dat moet rapporteren als het gaat om informatiebeveiliging.*

4.2.4. Gebruikersbewustzijn en betrokkenheid bij informatiebeveiliging

Op het gebied van gebruikersbewustzijn en betrokkenheid bij informatiebeveiliging zijn de volgende resultaten gevonden. Een document met het informatiebeveiligingsbeleid behoort door de directie te worden goedgekeurd, gepubliceerd en gecommuniceerd aan alle medewerkers. Dit document dient op het gebied van gebruikersbewustzijn en betrokkenheid eisen te stellen met betrekking tot beveiligingsscholing, -training en bewustwording. Daarnaast dient de directie plannen en programma’s te initiëren om het informatiebeveiligingsbewustzijn levend te houden.
De directie is verantwoordelijk dat de werknemers:

- goed zijn ingelicht over hun informatiebeveiligingsrollen en verantwoordelijkheden voor toegang wordt verleend tot informatiesystemen;
- zijn voorzien van richtlijnen die de beveiligingsverwachtingen van hun rol in de organisatie aangeven;
- gemotiveerd zijn om het beveiligingsbeleid van de organisatie uit te voeren;
- een zodanig niveau van veiligheidsbewustzijn verwerven als nodig is voor hun rollen en verantwoordelijkheden binnen de organisatie;
- een passende bewustzijnsopleiding en -training krijgen en regelmatig bijscholing van beleidsregels en procedures van de organisatie.

Vanuit de interviews blijkt dat de organisatie wel bezig is om de bewustwording te verbeteren. Hiervoor is een programma opgezet om de dit weer beter onder de aandacht te brengen. Dit is onder andere zichtbaar door verschillende flyers en posters die in de organisatie gedeeld worden.
De ervaring leert dat de volgende twee factoren van wezenlijk belang zijn voor een geslaagde implementatie van informatiebeveiliging in de organisatie. De eerste is effectieve marketing van informatiebeveiliging naar alle managers, werknemers en andere partijen, met het doel beveiligingsbewustzijn te creëren. Een tweede is het verzorgen van geschikte training en opleidingen om beveiligingsbewustzijn te creëren. Deze trainingen en opleidingen dienen met regelmaat terug te komen in allerlei opleidingstrajecten van de medewerkers. vanuit de interviews blijkt ook dat binnen de organisatie in trainingen en opleidingen steeds meer aandacht wordt besteed aan beveiligingsbewustzijn en dat dit een integraal onderdeel aan het worden is binnen de trainingen en opleidingen.

> We zijn natuurlijk nu bezig met een stuk bewustwording, dus ze hebben nu een programma opgezet om organisatiebreed middels een programma te zorgen dat in ieder geval die bewustwording weer beter wordt.*

De naleving van de beveiligingsvoorschriften blijft mensenwerk en vereist de voortdurende aandacht. Deugdelijke procedures en technische maatregelen zijn niet voldoende. Beveiliging is vooral een kwestie van mentaliteit waarbij lering trekken uit fouten essentieel is. Het is belangrijk dat beveiliging op natuurlijke wijze is ingebed in de normale gang van zaken en niet als iets aparts wordt ervaren. Het

veranderen van de mentaliteit van medewerkers kan slechts geleidelijk gerealiseerd worden, bijvoorbeeld door middel van periodieke voorlichting. Vanuit de interviews blijkt dat binnen de organisatie beveiligingsvoorlichtingen worden gegeven waarbij informatiebeveiliging een deel van uitmaakt.

> Waar wij nu mee bezig zijn is dat op het moment dat een medewerker bij de organisatie binnenkomt informatiebeveiliging al onderdeel van zijn initiële opleiding deel uitmaakt. *

4.2.5. Compliance informatiebeveiliging

Op het gebied van compliance van informatiebeveiliging zijn de volgende resultaten gevonden. Binnen de departementale organisatie is een rijksbeveiligingsambtenaar verantwoordelijk voor de realisatie van rijksbreed toezicht op de naleving van rijksbrede kaders. Hij bevordert tevens een gezamenlijke aanpak van beveiligingsissues en -belangen wanneer deze bij meerdere departementen spelen. Het management behoort regelmatig de naleving van beveiligingsbeleid en -normen binnen haar verantwoordelijkheidsgebied te beoordelen aan de hand van de betreffende beleidsregels, normen en andere eisen betreffende beveiliging. Daarnaast dient het management van alle medewerkers te eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie. Een factor van wezenlijk belang hier is het verstrekken van richtlijnen over informatiebeveiligingsbeleid en normen aan alle managers, werknemers en andere partijen.

> Hoe maakt het management die compliance dan zichtbaar binnen de organisatie?: Ik denk hoofdzakelijk door er veel nadrukkelijker aandacht aan te schenken. Het is een onderwerp dat tegenwoordig regelmatig naar voren komt.*

Het is tevens belangrijk dat het management communiceert over de gevolgen van het niet naleven van het informatiebeveiligingsbeleid. Dit behoort een formele en gecommuniceerde disciplinaire procedure te zijn, om actie te kunnen ondernemen tegen medewerkers die inbreuk hebben gepleegd op de informatiebeveiliging. Zoals al beschreven in de vorige paragraaf blijft de naleving van het informatiebeveiligingsbeleid mensenwerk en vereist voortdurende aandacht. Deugdelijke procedures en technische maatregelen zijn niet voldoende. Beveiliging is vooral een kwestie van mentaliteit, waarbij lering trekken uit fouten essentieel is. Het is belangrijk dat beveiliging op natuurlijke wijze is ingebed in de normale gang van zaken en niet als iets aparts wordt ervaren. Het veranderen van de mentaliteit van medewerkers kan slechts geleidelijk gerealiseerd worden. Vanuit de interviews blijkt dat deze mentaliteit aan het verbeteren is. In het verleden is de mentaliteit op het gebied van informatiebeveiliging niet erg goed geweest. De afgelopen jaren is deze mentaliteit binnen de organisatie wel veranderd omdat iedereen steeds meer het belang hiervan in ziet.

Daarnaast heeft het management een voorbeeldfunctie op het gebied van compliance. Wanneer het management zich niet conformeert aan het opgelegde informatiebeveiligingsbeleid werkt dit door naar alle medewerkers. Het gezegde ‘goed voorbeeld doet goed volgen’ gaat zeker op voor het conformeren aan compliance op het gebied van informatiebeveiliging. Vanuit de interviews blijkt dat dit voorbeeldgedrag veel meer aanwezig is dan enkele jaren geleden. Het management is momenteel veel meer bewust van zijn voorbeeldrol op het gebied van informatiebeveiliging. Toch gaat dit nog niet altijd goed binnen de organisatie hier en daar wordt door het management nog steeds niet altijd het goede voorbeeld gegeven.

> Als hij vervolgens iemand van het topmanagement ziet die het juist niet doet, dan kun je nog zoveel campagnes voeren maar dan is het draagvlak nul.*

5. Discussie en reflectie, conclusies en aanbevelingen

5.1. Discussie en reflectie

De resultaten van dit onderzoek zijn gepresenteerd aan vier elementen van informatiebeveiligings-beheer, Daarbij is weergeven hoe het management van de departementale organisatie zijn rol dient te vervullen op de volgende deelgebieden van informatiebeveiligingsbeheer:

- Betrokkenheid topmanagement bij informatiebeveiliging;
- Organisatiestructuren voor het afdwingen van informatiebeveiliging;
- Gebruikersbewustzijn en betrokkenheid bij informatiebeveiliging;
- Compliance informatiebeveiliging.

De conclusie is dan ook dat von Solms (2000, 2006) gelijk heeft gehad en dat topmanagement en informatiebeveiliging onlosmakelijk met elkaar verbonden zijn.

Op het gebied van betrokkenheid van het topmanagement zijn dit de voornaamste resultaten. De secretaris-generaal en de directie van de departementale organisatie hebben een prominente rol in de informatiebeveiliging en het bijbehorende informatiebeveiligingsbeleid. Dit is essentieel om tot effectieve informatiebeveiliging te komen, zoals beschreven door diverse reeds genoemde auteurs. Uit de resultaten blijkt dat dit op zichzelf niet voldoende is ook zichtbare steun en betrokkenheid van alle managementniveaus is een kritische succesfactor voor een geslaagde implementatie van informatiebeveiliging in een organisatie. Dit zien we niet terug in het theoretisch kader, waarbij vooral gekeken wordt naar de rol van het topmanagement. Het kan derhalve een aanvulling zijn op de bestaande theoretische kaders.

Op het gebied van organisatiestructuren voor het afdwingen van informatiebeveiliging zijn dit de voornaamste resultaten. De leiding van de organisatie heeft de verantwoordelijkheden en de rollen op het gebied van informatiebeveiliging binnen de organisatie vastgelegd. Het beveiligingsbeleid dient een eigenaar te hebben die door de directie goedgekeurde verantwoordelijkheden heeft. Dit is in lijn met wat gevonden is in de theorie: Kayworth en Whitten (2010) stellen dat het van belang is om een formele organisatiestructuur te hebben waarbij nadruk gelegd wordt op eigenaarschap en verantwoordelijkheden.

Op het gebied van gebruikersbewustzijn en betrokkenheid bij informatiebeveiliging zijn dit de voornaamste resultaten. De ervaring leert dat de volgende twee factoren van belang zijn voor een geslaagde implementatie van informatiebeveiliging. De eerste is effectieve ‘marketing’ van informatiebeveiliging richting alle medewerkers van de organisatie, en de tweede is het verzorgen van training en opleiding om beveiligingsbewustzijn te creëren. De eerste factor komt overeen met de conclusie van Albrechtsen (2007) dat effectieve communicatie van het beveiligingsbeleid noodzakelijk is voor goede informatiebeveiliging in de praktijk. De resultaten geven ook weer dat het belangrijk is om te beseffen dat het veranderen van de mentaliteit op het gebied van informatiebeveiliging van medewerkers slechts geleidelijk gerealiseerd kan worden. Dit zien we niet direct terug in de theoretische kaders en kan daarom een aanvulling zijn op de bestaande theoretische kaders.

Op het gebied van compliance zijn dit de voornaamste resultaten. Het management dient van alle medewerkers te eisen dat ze informatiebeveiliging toepassen conform het beveiligingsbeleid, en te communiceren wat de gevolgen zijn van het niet naleven van het informatiebeveiligingsbeleid. Zonder deze betrokkenheid is effectieve naleving van het informatiebeleid niet mogelijk (Boss et al., 2009; Bulgurcu et al., 2010; Hu et al., 2007; McFadzean et al., 2006). Het is tevens belangrijk dat informatiebeveiliging op een natuurlijke wijze is ingebed in de normale gang van zaken en niet als iets

aparts wordt ervaren. In de theorie zijn we dit niet direct terug en het kan dus dienen als aanvulling op de bestaande theoretische kaders.

De hierboven beschreven resultaten zijn vooral gebaseerd op de beschrijving van de rol van de departementale top in de departementale organisatie in de diverse beleidsdocumenten. Een beperking van dit onderzoek is dus dat er beperkt wordt ingegaan op hoe dit beleid daadwerkelijk wordt uitgevoerd door de departementale top, en op de vraag wat de effecten hiervan zijn op de departementale organisatie. Deze beperking heeft vooral als gevolg dat momenteel de discussie voor een deel gebaseerd is op de papieren werkelijkheid binnen de departementale organisatie.

Een onderdeel van deze paragraaf is de reflectie op het proces en product van dit onderzoek. In tabel 3 worden de zwaktes en sterktes van het onderzoek beschreven vanuit twee perspectieven: het product en het proces. Een aantal sterktes en zwaktes worden hieronder verder verdiept uitgewerkt.

Een van de zwaktes van het product is dat het onderzoek niet compleet is uitgevoerd zoals beschreven is in het methodologisch kader. Vooral ontbreekt het aan dataverzadiging in de semigestructureerde interviews. Als er wel dataverzadiging had plaatsgevonden in de semigestructureerde interviews was het misschien mogelijk om betere triangulatie toe te passen op de documentaire secundaire data. Een aanvulling op het methodologisch kader kan eventueel ook het toevoegen van een survey zijn waarbij door de gehele departementale organisatie gemeten kan worden hoe het staat met de informatiebeveiliging in de praktijk. Een andere zwakte van dit onderzoek is de beperkte generaliseerbaarheid in verband met de casestudy. Volgens Saunders et al. (2015) is dit geen probleem als het doel van het onderzoek niet het generaliseren is van de theorie naar alle populaties. In de opzet van de casestudy was het misschien beter om te kiezen voor een meervoudige case waardoor de externe validiteit van dit onderzoek verhoogd kan worden. De conclusies zouden dan beter generaliseerd kunnen worden voor meerdere departementale organisaties. Door bovenstaande zwaktes op deze manier anders aan te pakken in het onderzoek kan ook de interne validiteit van dit onderzoek beter gewaarborgd worden. De sterkte van dit onderzoek is het theoretisch kader en hoe dit vorm gegeven is. Juist door dat de onderzoeksaanpak en uitvoering uitvoerig beschreven staan biedt dit de mogelijkheid om de resultaten en conclusies in de toekomst verder te verfijnen als er meer wetenschappelijke literatuur op dit gebied ter beschikking komt. Daarnaast is het door de duidelijke weergave van het methodologisch kader mogelijk om dit onderzoek in een andere departementale organisatie te herhalen. Wel dient dan extra aandacht gegeven worden aan het verbeteren van de zwaktes die nu zijn opgetreden in het huidige onderzoek.

Voor het proces van dit onderzoek is veel gebruik gemaakt van de handleiding methoden en technieken van onderzoek van Saunders et al. (2015). Dit helpt vooral het gestructureerd aanlopen van het onderzoek. Wat zeker noodzakelijk is als een onderzoek een verschillende etappes verloopt en biedt de onderzoeker het houvast dat nodig was. Voor het verwerken van de data is gebruik gemaakt van een CAQDAS wat bijdraagt aan het systematisch kunnen analyseren en vergelijken van de verschillende gegevens bronnen.

Reflectie	Sterktes	Zwaktes
Product	+ Het gebruik van de elementen van informatiebeveiligingsbeheer met von Solms (2006) als kapstok. + Duidelijke weergave onderzoeksaanpak en uitvoering voor theoretisch kader. + Resultaten en conclusies theoretisch kader. + Duidelijke weergave methodologisch kader.	- Onderzoek niet compleet kunnen uitvoeren aan de hand van het methodologisch kader. - Beperkte generaliseerbaarheid in verband met de casestudy. - Interne validiteit door beperkte mogelijkheid triangulatie. - Niet alle theoretische inzichten kunnen toetsen aan de empirie.

Proces	+ Structureel gebruik van de handleiding Methoden en technieken van onderzoek. + Gebruik van CAQDAS voor de gegevensanalyse. + Respecteren van de ethische aspecten.	- Afstuderen heeft in verschillende etappes plaatsgevonden. - Vertraging door de medewerking van respondenten.

Tabel 3: Reflectie op basis van product en proces

5.2. Conclusies

In de introductie van dit onderzoek is beschreven dat informatiebeveiliging een verantwoordelijkheid is van de departementale top, en dat vanuit de wetenschappelijk literatuur bekend is dat ondersteuning van het topmanagement een belangrijke invloed heeft op de informatiebeveiliging. Het beveiligen van informatie is echter geen eenmalige zaak, maar een proces waarbij steeds de Plan-Do-Check-Act cyclus wordt doorlopen (Ministerie van Binnenlandse Zaken en Koninkrijkrelaties, 2017; von Solms, 2006). Binnen de Nederlandse rijksoverheid is het doorlopen van dit proces een verantwoordelijkheid van de departementale top (Balkenende, 2007; Ollongren, 2017). De daarom gestelde vraag is: in hoeverre heeft de departementale top inzicht in en grip op de informatie-beveiliging binnen het betreffende departement? Deze paragraaf geeft de voornaamste conclusies weer die getrokken kunnen worden naar aanleiding van dit onderzoek.

Op het gebied van betrokkenheid topmanagement bij informatiebeveiliging zijn de volgende conclusies te trekken. De departementale secretaris-generaal stelt het beveiligingsbeleid vast voor de departementale organisatie en legt deze ook op binnen de departementale organisatie. De directie dient een informatiebeveiligingsbeleid uit te brengen en te handhaven voor de gehele organisatie vanuit de interviews is te concluderen dat de betrokkenheid vooral reactief is. Als laatste geldt dat informatiebeveiliging een integraal onderdeel van de bedrijfsvoering dient te zijn en het management eindverantwoordelijk is. De conclusies is dat het management wel meer steeds betrokken raakt en geïnteresseerd is wat er speelt op het gebied van informatiebeveiliging.

Op het gebied van organisatiestructuren voor het afdwingen van informatiebeveiliging zijn de volgende conclusie te trekken. De departementale organisatie heeft een departementale beveiligingsautoriteit die toezicht houdt op de informatiebeveiliging binnen het departement. Daarnaast heeft de departementale organisatie verantwoordelijkheden en rollen vastgelegd op het gebied van informatiebeveiliging binnen de organisatie. Hiervoor zijn er door de gehele organisatie beveiligingscoördinatoren die toezien op de naleving. Tevens is er een specifieke rapportage structuur om informatiebeveilingsincidenten snel op het juiste niveau te krijgen.

Op het gebied van gebruikersbewustzijn en betrokken bij informatiebeveiliging zijn de volgende conclusies te trekken. De directie dient plannen en programma's te initiëren om informatiebeveiligingsbewustzijn levend te houden. De departementale organisatie is bezig om deze bewustwording te verbeteren en hier is een dan ook een programma voor opgezet. Daarnaast dienen trainingen en opleidingen gegeven te worden om veiligheidsbewustzijn te creëren. Binnen de departementale organisatie wordt getracht beveiligingsbewustzijn een integraal onderdeel te laten vormen binnen alle trainingen en opleidingen. Als laatste dient de mentaliteit op het gebied van informatiebeveiliging veranderd binnen de departementale organisatie. Dit wordt geprobeerd door periodieke voorlichtingen te geven waarbij informatiebeveiliging een deel van uitmaakt.

Op het gebied van compliance van informatiebeveiliging zijn de volgende conclusies te trekken. Het management dient van alle medewerkers te eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures. In de departementale organisatie wordt hier nadrukkelijk meer aandacht aan besteed. Het is daarnaast belangrijk dat informatiebeveiliging op een natuurlijke wijze is ingebed in de normale gang van zaken en onderdeel is van de mentaliteit van de medewerkers. Binnen de departementale organisatie is deze mentaliteit

afgelopen jaren positief aan het wijzigen mede doordat iedereen steeds meer het belang in ziet van informatiebeveiliging. Als laatste heeft het management een voorbeeldfunctie op het gebied van compliance. We zien dat het management zich steeds meer bewust is van deze rol. Desondanks gebeurt het nog wel eens dat het management dit voorbeeldgedrag niet uitdraagt.

In de diverse beleidsdocumenten binnen de departementale organisatie is beschreven hoe de departementale top betrokken dient te zijn bij de verschillende facetten van het informatie-beveiligingsbeheer. Het beschrijven alleen is niet voldoende want in de praktijk blijken niet alle beschreven beleidsdocumenten een op een uitgevoerd te worden in de praktijk. De conclusie is dat het de vraag is in hoeverre de departementale top inzicht en grip heeft op de informatiebeveiliging binnen hun departement als het beschreven beleid niet tot uitvoer wordt gebracht in de praktijk. Alleen als het topmanagement zich houdt aan zijn taakomschrijving in de beleidsdocumenten en dit daadwerkelijk toepast dan kan het inzicht in en grip hebben op de informatiebeveiliging in de praktijk.

5.3. Aanbevelingen voor de praktijk

Deze paragraaf geeft relevante praktische implementaties van dit onderzoek weer. Daarbij wordt aandacht besteed aan de vraag hoe dit onderzoek kan bijdragen aan het werk in de praktijk. De voornaamste aanbeveling voor de praktijk is als volgt. Ten eerste dient de rol van het topmanagement op het gebied van Informatiebeveilingsbeheer duidelijk beschreven te zijn in diverse beleidsdocumenten. Dit is bij deze departementale organisatie ook het geval maar alleen het beschrijven van deze rol is niet afdoende. Het topmanagement dient ook invulling te geven in de praktijk aan de beschreven rol op het gebied van informatiebeveiliging. Alleen op deze manier kan het topmanagement in de praktijk waarborgen dat ze inzicht en grip hebben op de informatiebeveiliging in hun organisatie.

5.4. Aanbevelingen voor verder onderzoek

Deze paragraaf presenteert aanbevelingen voor verder onderzoek, voortkomend uit twee aspecten. De eerste zijn de beperkingen van dit onderzoek en de tweede zijn de resultaten van dit onderzoek, met het oog op de vraag welke resultaten eventueel verder onderzoek behoeven.

De belangrijkste beperking van dit onderzoek is dat een van de twee methodes van gegevens-verzameling - het houden van semigestructureerde interviews - niet tot de gewenste dataverzadiging heeft geleid. Het risico daarvan is dat de onderzochte werkelijkheid veelal gebaseerd is op de beschrijving van de werkelijkheid in verschillende documentaire secundaire data.
Daarom is een van de aanbevelingen een dergelijk onderzoek uit te voeren bij een andere nationale departementale organisatie, om de resultaten te kunnen valideren of eventueel weerleggen.

Daarnaast zijn de resultaten vooral gebaseerd op de vraag hoe in de departementale organisatie de rol van de departementale top is beschreven in de diverse beleidsdocumenten. Deze beperking heeft vooral als gevolg dat de discussie momenteel slechts gebaseerd is op de papieren werkelijkheid binnen de departementale organisatie. Een aanbeveling is dan ook verder te onderzoeken hoe het beleid daadwerkelijk wordt uitgevoerd door de departementale top, en wat de effecten hiervan zijn op de departementale organisatie.

De resultaten geven vooral weer hoe de departementale top de centrale aansturing van informatie-beveiliging toepast bij een nationale departementale organisatie. Een ander onderzoeksperspectief is te onderzoeken hoe de medewerkers de centrale aansturing ervaren van diezelfde departementale top. Hierbij zou dan kunnen worden onderzocht of de theoretische inzichten ook ervaren worden door de medewerkers binnen de organisatie.

Referenties

Abu-Musa, A. (2010). Information security governance in Saudi organizations: an empirical study. *Information Management & Computer Security, 18*(4), 226-276. doi:https://doi.org/10.1108/09685221011079180

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security, 26*(4), 276-289. doi:https://doi.org/10.1016/j.cose.2006.11.004

Algemene Rekenkamer. (2017). *Resultaten verantwoordingsonderzoek 2017 Ministerie van Defensie (X)*. Den Haag Retrieved 15-11-2018 from https://www.rekenkamer.nl/publicaties/rapporten/2018/05/16/resultaten-verantwoordingsonderzoek-2017-bij-het-ministerie-van-defensie.

Atkins, B. (2013). Board focus on cyber security: a director's perspective. *Corporate Governance Advisor, 21*(4), 24.

Balkenende, J. P. (2007). Besluit voorschrift informatiebeveiliging rijksdienst 2007. *Staatscourant*. Retrieved 11-10-2018 from https://zoek.officielebekendmakingen.nl/stcrt-2007-122-p11-SC81084.pdf

Barton, K. A., Tejay, G., Lane, M., & Terrell, S. (2016). Information system security commitment: A study of external influences on senior management. *Computers & Security, 59*, 9-25. doi:https://doi.org/10.1016/j.cose.2016.02.007

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems, 18*(2), 151-164. doi:https://doi.org/10.1057/ejis.2009.8

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly, 34*(3), 523-548. doi:https://doi.org/10.2307/25750690

Cuganesan, S., Steele, C., & Hart, A. (2017). How senior management and workplace norms influence information security attitudes and self-efficacy. *Behaviour & Information Technology, 37*(1), 50-65. doi:https://doi.org/10.1080/0144929x.2017.1397193

da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security, 49*, 162-176. doi:https://doi.org/10.1016/j.cose.2014.12.006

De Nederlandse grondwet. (2019). De interne organisatie van de ministeries. Retrieved 25-09-2019 from https://www.denederlandsegrondwet.nl/id/vh4vamhbp7zp/de_interne_organisatie_van_de

Ensie. (2016). Betekenis & definitie Rijksoverheid. Retrieved 13-11-2018 from https://www.ensie.nl/algemene-rekenkamer/rijksoverheidRijksoverheid

Ernest Chang, S., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems, 106*(3), 345-361. doi:https://doi.org/doi:10.1108/02635570610653498

Grapperhaus, F. (2018). *Voorzorgsmaatregel ten aanzien van gebruik Kaspersky antivirussoftware*. Den Haag Retrieved 11-10-2018 from https://www.rijksoverheid.nl/documenten/kamerstukken/2018/05/14/voorzorgsmaatregel-ten-aanzien-van-gebruik-kaspersky-antivirussoftware.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture*. *Decision Sciences, 43*(4), 615-660. doi:https://doi.org/doi:10.1111/j.1540-5915.2012.00361.x

Hu, Q., Hart, P., & Cooke, D. (2007). The role of external and internal influences on information systems security – a neo-institutional perspective. *Journal of Strategic Information Systems, 16*(2), 153-172. doi:https://doi.org/10.1016/j.jsis.2007.05.004

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, 51*(1), 69-79. doi:https://doi.org/10.1016/j.im.2013.10.001

Kayworth, T., & Whitten, D. (2010). Effective information security requires a balance of social and technology factors. *MIS QUARTERLY EXECUTIVE, 9*(3), 163-175.

Leest, P. (2018). Vijf uitdagingen voor CIO's bij de overheid. Retrieved 05-11-2018 from https://cio.nl/management/106365-vijf-uitdagingen-voor-cio-s-bij-de-overheid

Lundgren, B., & Moller, N. (2017). Defining Information Security. *Sci Eng Ethics*. doi:https://doi.org/10.1007/s11948-017-9992-1

McFadzean, E., Ezingeard, J.-N., & Birchall, D. (2006). Anchoring information security governance research: sociological groundings and future directions. *Journal of Information System Security, 2*(3), 3-48.

Ministerie van Binnenlandse Zaken en Koninkrijkrelaties. (2017). *Baseline informatiebeveiliging Rijksdienst*. Den Haag Retrieved 03-10-2018 from https://informatiebeveiliging-gemeenten.nl/download/bir-2017/.

Ollongren, K. H. (2017). *Toezegging verantwoordingsdebat 2016 over informatiebeveiliging en bijbehorende motie de Vries*. Den Haag Retrieved 03-10-2018 from https://www.rijksoverheid.nl/documenten/kamerstukken/2017/12/22/kamerbrief-over-informatiebeveiliging-bij-de-overheid.

Puhakainen, P., & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly, 34*(4), 757-778. doi:https://doi.org/10.2307/25750704

Pulkkinen, M., Naumenko, A., & Luostarinen, K. (2007). Managing information security in a business network of machinery maintenance services business – Enterprise architecture as a coordination tool. *The Journal of Systems & Software, 80*(10), 1607-1620. doi:https://10.1016/j.jss.2007.01.044

Rocha Flores, W., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security, 59*, 26-44. doi:https://doi.org/10.1016/j.cose.2016.01.004

Saunders, M., Lewis, P., Thornhill, A., Booij, M. C., Beltman, S., Booy, A., & Borggreve, A. (2015). *Methoden en technieken van onderzoek* (7e editie ed.). Amsterdam: Pearson Benelux.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management, 36*(2), 215-225. doi:https://doi.org/10.1016/j.ijinfomgt.2015.11.009

University of Groningen. (2018). Informatievaardigheden: Zoekmethoden. Retrieved 05-11-2018 from https://libguides.rug.nl/c.php?g=531668&p=3637472

Veiga, A. D., & Eloff, J. H. P. (2007). An Information Security Governance Framework. *Information Systems Management, 24*(4), 361-372. doi:https://doi.org/10.1080/10580530701586136

Verschuren, P., & Doorewaard, H. (2015). *Het ontwerpen van een onderzoek* (Vijfde druk ed.). Amsterdam: Boom Lemma uitgevers.

von Solms, B. (2000). Information Security — The Third Wave? *Computers & Security, 19*(7), 615-620. doi:https://doi.org/10.1016/s0167-4048(00)07021-8

von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both? *Computers & Security, 24*(2), 99-104. doi:https://doi.org/10.1016/j.cose.2005.02.002

von Solms, B. (2006). Information Security – The Fourth Wave. *Computers & Security, 25*(3), 165-168. doi:https://doi.org/10.1016/j.cose.2006.03.004

Wang, H., Tsui, A. S., & Xin, K. R. (2011). CEO leadership behaviors, organizational performance, and employees' attitudes. *The Leadership Quarterly, 22*(1), 92-105. doi:https://doi.org/10.1016/j.leaqua.2010.12.009

Bijlagen

Bijlage 1 Zoekstrategie en uitvoering literatuurstudie

Onderzoeksaanpak

In deze bijlage wordt de zoekstrategie weergegeven die vorm geeft aan het theoretisch kader. De gebruikte parameters, gegevensbronnen en zoektermen worden beschreven.

Saunders et al. (2015) beschrijven een aantal parameters waarover in ieder geval duidelijkheid dient te zijn. Deze parameters in tabel 1 vormende de basis voor de zoekstrategie.

Parameter	
Taal	Engels
Onderzoeksgebied	Computertechnologie
Bedrijfssector	Overheid
Geografische gebied	Europa
Publicatieperiode	2013 tot en met 2018
Soort literatuur	Wetenschappelijke tijdschriften met peer review

Tabel 1: Parameters zoekstrategie

De zoekstrategie maakte gebruik van twee gegevensbronnen: de digitale bibliotheek van de Open Universiteit (OU) en Google Scholar. De eerste is de hoofdgegevensbron. Hierbij werd de 'advanced search'-optie van de 'quick search' gebruikt. Voor Google Scholar werd gebruikgemaakt van de links afkomstig uit de digitale bibliotheek van de OU. Ook Google Scholar heeft een 'geavanceerd zoeken'-functie.

Op basis van de parameters en de gegevensbronnen van de zoekstrategie werd de zoekopdracht gedefinieerd. Voor de eerste deelvraag is de zoekopdracht in tabel 2 gedefinieerd:.

Antwoord op	Zoekopdrachten in digitale bibliotheek OU en Google Scholar
Deelvraag 1: Wat zijn de theoretische inzichten op het gebied van de centrale aansturing van de informatiebeveiliging?	"information security" AND ("governance" OR "management")

Tabel 2: Zoekopdrachten voor het literatuuronderzoek

In tabel 2 is de zoekstrategie beschreven die gebruikt is om relevante wetenschappelijke artikelen te vinden die antwoord kunnen geven op deelvraag 1. Onderdeel van deze zoekstrategie is ook de zoekmethode die gehanteerd word. Op basis van de gevonden literatuur werd ook gebruikgemaakt van de sneeuwbalmethode[14] en het citatiezoeken[15]. Op deze manier werd ook relevante oudere en recentere literatuur over het onderwerp gevonden (University of Groningen, 2018).

Volgens Saunders et al. (2015) moet ook de relevantie beoordeeld worden van de literatuur die gevonden is door middel van de zoekstrategie. Voor deze zoekstrategie werden de volgende criteria gehanteerd:

1. De publicatie past goed bij de gestelde onderzoeksvraag;

[14] De sneeuwbalmethode is een manier om literatuur te vinden op basis van een artikel over het onderwerp. De literatuurlijst van het artikel wordt geraadpleegd om meer titels over het onderwerp te vinden. Met de sneeuwbalmethode kan snel en relatief gemakkelijk veel literatuur over een onderwerp verzameld worden (University of Groningen, 2018).

[15] Citatiezoeken draait hierom: wie heeft de gevonden publicatie geciteerd? Zo wordt recentere literatuur gevonden (University of Groningen, 2018).

2. De publicatie is gedaan in een wetenschappelijk tijdschrift met peer review;
3. De publicatie belicht het onderwerp centrale aansturing van informatiebeveiliging op verschillende deelgebieden.

Uitvoering

In de vorige paragraaf is uitvoerig stilgestaan bij de gehanteerde zoekstrategie. De vraag was nu: hoe is de uitvoering van de strategie verlopen en welke keuzes zijn gemaakt om literatuur te vinden die antwoord kan geven op de deelvraag? In beide gegevensbronnen is gezocht door middel van de opgestelde zoekopdracht. De resultaten hiervan zijn weergegeven in tabel 3. Hierbij is onderscheid gemaakt tussen het zoeken in alle velden en het zoeken in alleen de titel.

Antwoord op	Zoekopdrachten in digitale bibliotheek OU en Google Scholar	Zoeken in alle velden digitale bibliotheek OU	Zoeken in de titel digitale bibliotheek OU	Zoeken in alle velden Google Scholar	Zoeken in de titel Google Scholar
Deelvraag 1: Wat zijn de theoretische inzichten op het gebied van de centrale aansturing van de informatiebeveiliging?	“information security” AND (“governance” OR “management”)	15890	28	832000	821

Tabel 3: Uitkomsten zoekopdrachten voor het literatuuronderzoek

Het zoeken in alle velden in zowel de digitale bibliotheek van de OU als Google Scholar leverde voor de eerste deelvraag veel te veel resultaten op. Daarom is gekozen om alleen artikelen te selecteren die gevonden zijn met het zoeken in de titel. Voor zoekresultaten in de digitale bibliotheek van de OU zijn alle samenvattingen gelezen en op basis daarvan zijn in totaal negen artikelen geselecteerd. Deze negen artikelen zijn verder gescand op relevantie en op basis daarvan bleven uiteindelijk drie artikelen over. Voor Google Scholar zijn in totaal 821 artikelen gevonden. Te veel om alle samenvattingen te kunnen lezen. Daarom is besloten om te zoeken in een recentere publicatieperiode, hetgeen het aantal artikelen terugbracht tot in totaal 99. Bij de selectie van de artikelen is ervoor gekozen om te kijken naar relevantie in de titel in combinatie met het aantal malen dat een artikel geciteerd is. Dit leverde nog twee relevante artikelen op. Na het bestuderen van de gevonden artikelen zijn met de sneeuwbalmethode en het citatiezoeken nog vijf relevante artikelen gevonden. Voor het beantwoorden van deelvraag 1 zijn in totaal tien artikelen gebruikt.

Bijlage 2 Informatieblad deelnemer interview

Informatieblad deelnemer interview

1. Titel van het onderzoeksproject

Centrale aansturing van informatiebeveiliging bij een nationale departementale organisatie.

2. Naam, functie, bereikbaarheid van de onderzoeker en afstudeerbegeleiders

Michel Brehen
Student Masteropleiding Business Process Management & IT Open Universiteit
Tel: 06-57104513
E-mail: m.brehen@mindef.nl
Afstudeerbegeleiders: Prof. dr. L. Bijlsma (Lex.Bijlsma@ou.nl) & Dr. L.W. Rutledge (lloyd.rutledge@ou.nl)

3. Introductie afstudeeronderzoek

De Nederlandse rijksoverheid onderkent het toenemende belang van goede informatiebeveiliging en de Algemene Rekenkamer doet hier intern ook onderzoek naar. Een van de speerpunten in dit onderzoek is met name de versteviging van de centrale sturing (Algemene Rekenkamer, 2017). De centrale sturing is belangrijk omdat de Nederlandse rijksoverheid van mening is dat informatiebeveiliging een zaak is van de departementale top. In de departementale top zou inzicht en zo nodig grip moeten zijn op de maatregelen, risico's en incidenten die decentraal spelen. Dit blijkt o.a. uit de kamerbrief die de Minister Binnenlandse Zaken en Koninkrijksrelaties heeft opgesteld waarin het rijksbrede beleid op het gebied van informatiebeveiliging wordt uitgezet (Ollongren, 2017). Daarnaast staat dit tevens verwoord in het Besluit voorschrift informatiebeveiliging rijksdienst 2007 (Balkenende, 2007): "Informatiebeveiliging vormt een integraal onderdeel van de bedrijfsvoering en is daarmee een managementverantwoordelijkheid." Het doel van dit onderzoek is theoretische inzichten op het gebied van centrale aansturing van informatiebeveiliging te toetsen aan de toepassing van deze theoretische inzichten bij een nationale departementale organisatie in de praktijk.
Deze theoretische inzichten komen voort uit informatiebeveilingsbeheer en bestaan uit de volgende elementen (von Solms, 2006):

- De betrokkenheid van het topmanagement op het gebied van management en leiderschap bij goede informatiebeveiliging;
- Juiste organisatiestructuren voor het afdwingen van een goede informatiebeveiliging;
- Gebruikersbewustzijn en betrokkenheid voor een goede informatiebeveiliging;
- Het nodige beleid, procedures, processen, technologieën en compliance mechanismen voor naleving.

Bovenstaande elementen werken allemaal samen om ervoor te zorgen dat de vertrouwelijkheid, integriteit en beschikbaarheid van de elektronische middelen van de organisatie te allen tijde worden gehandhaafd.

4. Interviewopzet

- Het interview wordt door de onderzoeker in persoon uitgevoerd bij een lid van het management van een nationale departementale organisatie. Deze deelnemer hoeft geen specifieke voorbereidingen te treffen.
- Het betreft een semigestructureerd interview waarbij gekozen is voor een reeks interview thema's waarbij de mogelijkheid bestaat om nieuwe vragen te stellen in de context van de onderzoekssituatie.
- Het interview heeft een maximale duur van anderhalf uur.
- Het interview wordt in vertrouwen en onder volledige anonimiteit uitgevoerd. Dit betekend dat namen van organisaties of personen niet worden gepubliceerd.
- Het interview wordt opgenomen door middel van een dictafoon, zodat de onderzoeksdata kwalitatief geanalyseerd kan worden.
- De geïnterviewde werkt vrijwillig mee aan dit onderzoek en is vrij om zich elk moment terug te trekken uit dit onderzoek

Bijlage 3 Interviewprotocol

Interviewprotocol (totale duur 90[16] minuten)

1. Fase I: Voorbereiding (5 minuten)

- Bedanken van de deelnemer voor deelname aan dit interview.
- Gelegenheid geven tot vragen n.a.v. het verstrekte informatieblad.
- Interviewopzet doornemen met de deelnemer.
- Toestemming vragen om de audio opname te starten.

2. Fase II: Inleiding (5 minuten)

- Deelnemer eigen functie binnen de organisatie laten beschrijven.
- Deelnemer vragen wat zijn/haar rol is op het gebied van informatiebeveiliging binnen de organisatie.

3. Fase IIIa: Betrokkenheid topmanagement bij informatiebeveiliging (15 minuten)

- Hoe is het management betrokken bij de informatiebeveiliging van de organisatie?
- Hoe geeft het management ondersteuning aan de informatiebeveiliging van de organisatie? (*Ontwikkeling en implementatie zijn hier belangrijk in, signaleert het belang voor de rest van de organisatie)*
- Hoe maakt de informatiebeveiliging onderdeel uit van de strategie van de organisatie?
- *Verdiepende vragen: Als het management geen invulling geeft aan de betrokkenheid van het topmanagement bij informatiebeveiliging waarom wordt hier dan geen invulling aan gegeven?*

4. Fase IIIb: Organisatiestructuren voor het afdwingen van informatiebeveiliging (15 minuten)

- Wat is de organisatiestructuur die gehanteerd wordt binnen de organisatie voor het ondersteunen van de informatiebeveiliging? (*nodig voor rapportage, effectieve communicatie en duidelijke autoriteit)*
- Hoe is het eigenaarschap en de verantwoordelijkheden belegd binnen de organisatie op het gebied van informatiebeveiliging? (*Moeten gelden op verschillende niveau's)*
- Hoe is het beslissingssysteem op het gebied van informatiebeveiliging binnen de organisatie te beschrijven? (*Gedecentraliseerd heeft hier de voorkeur omdat uitvoering intern de gehele organisatie dient plaats te vinden).*
- *Verdiepende vragen: Als er geen invulling gegeven wordt aan de inzichten op het gebied van organisatiestructuren voor het afdwingen van informatiebeveiliging waarom wordt hier dan geen invulling aan gegeven?*

[16] Geplande interview duur is 90 minuten hierbij zijn in totaal 75 minuten gepland en is 15 minuten ingecalculeerd op uit te kunnen lopen gedurende het interview.

5. Fase IIIc: Gebruikersbewustzijn en betrokkenheid bij informatiebeveiliging (15 minuten)

- Hoe creëert het management gebruikersbewustzijn en betrokkenheid op het gebied van informatiebeveiliging binnen de organisatie? *(management kan de houding van medewerkers rechtstreeks beïnvloeden)*
- Hoe wordt het informatiebeveiligingsbeleid binnen de organisatie gedeeld?
- Hoe creëert het management integraal bewustwording op het gebied van informatiebeveiliging binnen de organisatie? *(moet onderdeel zijn van de gehele strategie van de organisatie)*
- Welke leiderschapsstijl wordt vanuit de organisatie verwacht om compliance te bewerkstellingen van de medewerkers? *(leiders richten zich op welzijn van de organisatie, bewustwording genereren en motiveren van medewerkers)*
- *Verdiepende vragen: Als er geen invulling gegeven wordt aan de inzichten op het gebied van gebruikersbewustzijn en betrokkenheidorganisatiestructuren bij informatiebeveiliging waarom wordt hier dan geen invulling aan gegeven?*

6. Fase IIId: Compliance informatiebeveiliging (15 minuten)

- Hoe is het management betrokken bij het creëren van compliance binnen de organisatie?
- Hoe wordt binnen de organisatie gestreefd naar compliance van de medewerkers op het gebied van informatiebeveiliging? *(vormgeven van overtuigingen, attitudes en gedrag)*
- Hoe ondersteunt het management zichtbaar de compliance op het gebied van informatiebeveiliging binnen de organisatie? *(bijvoorbeeld door actief beveiligingsaangelegenheden te promoten en het goede voorbeeld geven door middel van hun eigen nalevingsgedrag.)*
- *Verdiepende vragen: Als er geen invulling gegeven wordt aan de inzichten op het gebied van compliance van informatiebeveiliging waarom wordt hier dan geen invulling aan gegeven?*

7. Fase IV: Afronding (5 minuten)

- Deelnemer bedanken.
- Deelnemer om feedback vragen ten aanzien van het interview.
- Deelnemer informeren over het verdere verloop van het onderzoek.

Bijlage 4 Categorieën en labels documentaire secundaire data

Betrokkenheid topmanagement bij informatiebeveiliging

Aandachtsgebied	Resultaat
Verantwoordelijkheid management	Het lijnmanagement verantwoordelijk is voor de beveiliging van informatie(systemen).
Betrokkenheid management	De departementale secretaris-generaal van een ministerie is eindverantwoordelijk voor de integrale beveiliging en de inrichting en werking van de ministeriële beveiligingsorganisatie. In die hoedanigheid is hij eindverantwoordelijk voor de implementatie van alle beveiligingskaders in zijn organisatie.
Strategisch aspect	Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.
Betrokkenheid management	Als eindverantwoordelijke voor het beveiligingsbeleid in de organisatie is de departementale secretaris-generaal verantwoordelijk voor de uitvoering van organisatiebrede vraagstukken ten aanzien van informatiebeveiliging
Betrokkenheid management	De directie behoort van alle medewerkers en contractanten te eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie.
Strategisch aspect; ondersteuning beleid	De directie behoort een duidelijke beleidsrichting aan te geven in overeenstemming met de bedrijfsdoelstellingen en te demonstreren dat het informatiebeveiliging ondersteunt en zich hiertoe verplicht, door het uitbrengen en handhaven van een informatiebeveiligingsbeleid voor de hele organisatie.
Betrokkenheid management; strategisch aspect	Het beleidsdocument voor informatiebeveiliging behoort de betrokkenheid van de directie te verwoorden, evenals de benadering van de organisatie ten aanzien van het beheer van informatiebeveiliging.
Toewijding management; betrokkenheid management	De ervaring leert dat de volgende factor vaak van wezenlijk belang is voor een geslaagde implementatie van informatiebeveiliging in een organisatie: zichtbare steun en betrokkenheid van alle managementniveaus.
Toewijding management; betrokkenheid management	De directie behoort actief beveiliging binnen de organisatie te ondersteunen door duidelijk richting te geven, betrokkenheid te tonen en expliciet verantwoordelijkheden voor informatiebeveiliging toe te kennen en te erkennen.
Ontbreken van management	Door zwak management kan het personeel zich ondergewaardeerd gaan voelen, wat kan leiden tot een negatieve invloed op de beveiliging van de organisatie. Zwak management kan er bijvoorbeeld toe leiden dat de beveiliging wordt verwaarloosd of dat bedrijfsmiddelen van de organisatie mogelijk worden misbruikt.

Verantwoording management	Het lijnmanagement is verantwoordelijk voor de kwaliteit van bedrijfsvoering. Die verantwoordelijkheid wordt verticaal in de lijn verdeeld, van organisatietop tot afdelingshoofd. Informatiebeveiliging geldt als een integraal onderdeel van de bedrijfsvoering. Zo is het lijnmanagement ook eindverantwoordelijk voor informatiebeveiliging.
Strategisch aspect; verantwoording management	Informatiebeveiliging vormt een integraal onderdeel van de bedrijfsvoering en is daarmee een managementverantwoordelijkheid. Daarom wordt de aandacht en verantwoordelijkheid van lijnmanagement en organisatie voor de informatiebeveiliging nog meer benadrukt
Verantwoording management	Dit artikel bepaalt dat voor een Ministerie het beleid voor informatiebeveiliging wordt vastgesteld en uitgedragen door de hoogst verantwoordelijke ambtenaar.

Organisatiestructuren voor het afdwingen van informatiebeveiliging

Aandachtsgebied	Resultaat
Eigenaarschap & verantwoordelijkheden	De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging binnen haar organisatie.
Beslissingssysteem	Het lijnmanagement stelt vast dat de getroffen maatregelen aantoonbaar overeenstemmen met de betrouwbaarheidseisen en dat deze maatregelen worden nageleefd. De proportionaliteit die eerder beschreven is, is ook van toepassing bij het toekennen van het niveau waar de verantwoordelijkheid voor risicomanagement wordt belegd.
Organisatiestructuur	Directieverantwoordelijkheden en -procedures behoren te worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.
Rapportage structuur	Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.
Eigenaarschap	De secretaris-generaal van zijn ministerie wijst een rijksbeveiligingsambtenaar aan die belast is met het bewaken van het integrale karakter en de consistentie van de Rijksbrede kaders voor beveiliging alsmede het toezicht op de werking van de integrale beveiliging van de Rijksdienst.
Eigenaarschap	De departementale secretaris-generaal wijst een departementale beveiligingsambtenaar aan die zorg draagt voor het toezicht op de integrale beveiliging van het departement, hierover adviseert en ter zake hiervan incidenten laat onderzoeken alsmede zorg draagt voor het toezicht op de organisatie van de beveiliging van het departement.
Rapportage structuur	De beveiligingsambtenaar rapporteert periodiek over de stand van de departementale integrale beveiliging aan zijn secretaris-generaal en informeert hierover periodiek de rijksbeveiligingsambtenaar.

Eigenaarschap	Het informatiebeveiligingsbeleid behoort een eigenaar te hebben die een door de directie goedgekeurde verantwoordelijkheid heeft voor het ontwikkelen, beoordelen en evalueren van het beveiligingsbeleid.
Formele organisatiestructuur	De directie behoort het toekennen van rollen en verantwoordelijkheden voor de informatiebeveiliging in alle lagen van de organisatie goed te keuren.
Rapportage structuur	Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.

Gebruikersbewustzijn en betrokkenheid bij informatiebeveiliging

Aandachtsgebied	Resultaat
Effectieve communicatie beveiligingsbeleid	Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.
Bewustmakingprogramma's	Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.
Effectieve communicatie beveiligingsbeleid; betrokkenheid management	Tot de verantwoordelijkheden van de directie zou moeten behoren dat werknemers, ingehuurd personeel en externe gebruikers: - goed zijn ingelicht over hun informatiebeveiligingsrollen en verantwoordelijkheden voordat de toegang wordt verleend tot gevoelige informatie of informatiesystemen; - zijn voorzien van richtlijnen die de beveiligingsverwachtingen van hun rol in de organisatie aangeven; -gemotiveerd zijn om het beveiligingsbeleid van de organisatie uit te voeren; - een zodanig niveau van veiligheidsbewustzijn verwerven, als nodig voor hun rollen en verantwoordelijkheden binnen de organisatie. Indien werknemers, ingehuurd personeel en externe gebruikers niet in kennis zijn gesteld van hun beveiligingsverantwoordelijkheden, kunnen ze een organisatie aanzienlijke schade berokkenen. Gemotiveerd personeel is naar verwachting betrouwbaarder en zal minder informatiebeveiligingsincidenten veroorzaken.
Bewustmakingprogramma's; effectieve communicatie	De ervaring leert dat de volgende factoren vaak van wezenlijk belang zijn voor een geslaagde implementatie van informatiebeveiliging in een organisatie:

	- effectieve marketing van informatiebeveiliging naar alle managers, werknemers en andere partijen om beveiligingsbewustzijn te creëren; - verzorgen van geschikte training en opleidingen en creëren van beveiligingsbewustzijn.
Betrokkenheid management	De directie behoort plannen en programma's te initiëren om het informatiebeveiligingsbewustzijn levend te houden.
Effectieve communicatie informatiebeveiligingsbeleid	Een document met informatiebeveiligingsbeleid behoort door de directie te worden goedgekeurd en gepubliceerd en kenbaar te worden gemaakt aan alle werknemers en relevante externe partijen. Het beleidsdocument behoort ten minste de volgende informatie te bevatten: - eisen met betrekking tot beveiligingsscholing, -training en bewustwording.
Gebruikersbewustzijn	De naleving van de beveiligingsvoorschriften blijft mensenwerk en vereist de voortdurende aandacht. Deugdelijke procedures en technische maatregelen zijn niet voldoende. Beveiliging is vooral een kwestie van mentaliteit waarbij lering trekken uit fouten essentieel is. Het is belangrijk dat beveiliging op natuurlijke wijze is ingebed in de normale gang van zaken en niet als iets aparts wordt ervaren. Het veranderen van de mentaliteit van medewerkers kan slechts geleidelijk gerealiseerd worden, bijvoorbeeld door middel van periodieke voorlichting.

Compliance informatiebeveiliging

Aandachtsgebied	Resultaat
Betrokkenheid management	De rijksbeveiligingsambtenaar is verantwoordelijk voor de realisatie van rijksbreed toezicht op de naleving van de Rijksbrede kaders. Hij bevordert een gezamenlijke aanpak van beveiligingsissues en -belangen wanneer deze bij meerdere departementen spelen.
Gedrag beïnvloeden	Er behoort een formele en gecommuniceerde disciplinaire procedure te zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging.
Betrokkenheid management	De directie behoort regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied te beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.
Betrokkenheid management	De directie behoort van alle medewerkers en contractanten te eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie.
Betrokkenheid management	De ervaring leert dat de volgende factoren vaak van wezenlijk belang zijn voor een geslaagde implementatie van informatiebeveiliging in een organisatie: een van die factoren is het verstrekken van richtlij-

	nen over informatiebeveiligingsbeleid en normen aan alle managers, werknemers en andere partijen.
Betrokkenheid management; gedrag beïnvloeden	Een beknopte uiteenzetting van beleid, uitgangspunten, normen en nalevingeisen ten aanzien van de beveiliging, die voor de organisatie van specifiek belang zijn, waaronder: gevolgen van het niet naleven van informatiebeveiligingsbeleid.
Gedrag beïnvloeden	De naleving van de beveiligingsvoorschriften blijft mensenwerk en vereist de voortdurende aandacht. Deugdelijke procedures en technische maatregelen zijn niet voldoende. Beveiliging is vooral een kwestie van mentaliteit waarbij lering trekken uit fouten essentieel is. Het is belangrijk dat beveiliging op natuurlijke wijze is ingebed in de normale gang van zaken en niet als iets aparts wordt ervaren. Het veranderen van de mentaliteit van medewerkers kan slechts geleidelijk gerealiseerd worden, bijvoorbeeld door middel van periodieke voorlichting.