

A photograph of four business professionals in a meeting. Three men and one woman are smiling and engaged in conversation. The woman is standing in the center, wearing a light blue blazer over a white top. The men are seated to her left, and another woman is seated to her right, wearing a blue and white striped shirt. The background is a dark wall with a large, abstract painting.

Cybersecurity toegepast op uw kantoor

Waarom de brancheorganisaties cybersecurity nu op #1 zetten

The logo for SRA, featuring a shield icon above the letters "SRA".

SRA

Waarom cybersecurity nu op #1 zetten

Cyber security is voor veel accountants een abstract en ongrijpbare onderwerp. Het heeft het imago geen directe bijdrage te leveren aan de kwaliteit van de dienstverlening van het kantoor en wordt daardoor vaak beschouwd als een bijzaak, een hinderlijke drempel of een separaat traject wat wordt overgelaten aan de (externe) IT-manager.

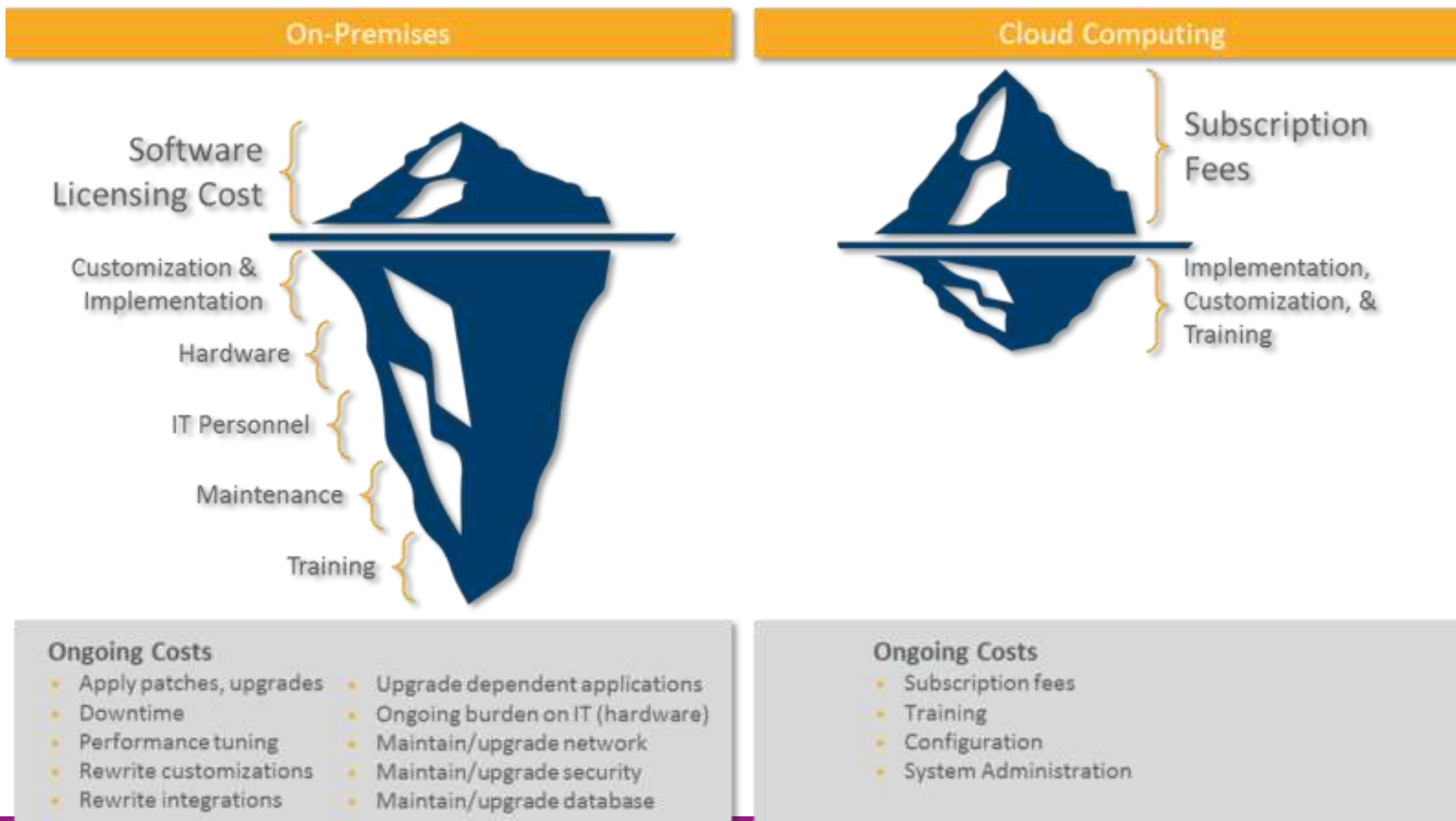
De digitale weerbaarheid van accountantskantoren staat onder druk door een toenemende complexiteit en connectiviteit in het IT-landschap, nieuwe ontwikkelingen en door te weinig aandacht voor digitale veiligheid bij nieuwe, innovatieve projecten. Om de digitale weerbaarheid van het kantoor te vergroten, is stilstaan is geen optie.



Het IT-landschap



Verschillende omgevingen





“Tech support says the problem is located somewhere between the keyboard and my chair.”

Vijf belangrijke IT-trends

- Cyber security
- Cloud / ...-as-a-service
- Data & Business Intelligence
- Digitale transformatie
- Thuiswerken



Waarom cybersecurity nu op #1 zetten?

Grootste uitdagingen op IT-gebied

1. **Informatiebeveiliging & Cybersecurity**
2. Beheersing van kosten
3. Migratie naar de cloud
4. Grip op data
5. Kennis van medewerkers
6. Innovatief vermogen van de organisatie
7. **AVG / Privacy**

Investeren in de komende twee jaar

1. Data-analyse / Process Mining
2. **Informatiebeveiliging, Cybersecurity & Privacy**
3. Vervanging van bestaande software
4. Elektronisch ondertekenen
5. Cloud / outsourcing
6. Workflow
7. Dashboards ontwikkelen voor klanten

Wat gebeurt er op het gebied van informatiebeveiliging, cybersecurity & privacy?



Cybersecuritybeeld Nederland

- Digitale dreiging is permanent; digitale risico's zijn onverminderd groot en niet fundamenteel veranderd
 - Sabotage en spionage (door statelijke actoren)
 - Cyberaanvallen door cybercriminelen
 - Afpersing door ransomware
- Digitale weerbaarheid is nog niet overal op orde
 - Basismaatregelen onvoldoende op orde
 - Complexiteit van IT (in de keten) neemt toe
 - Gebruikers gedragen zich 'onveilig'
- Digitale risico's staan niet los van ander risico's
- Vergroting van de weerbaarheid is het belangrijkste instrument
 - Technische, procedurele of organisatorische maatregelen
 - Wetgeving (o.a. AVG)

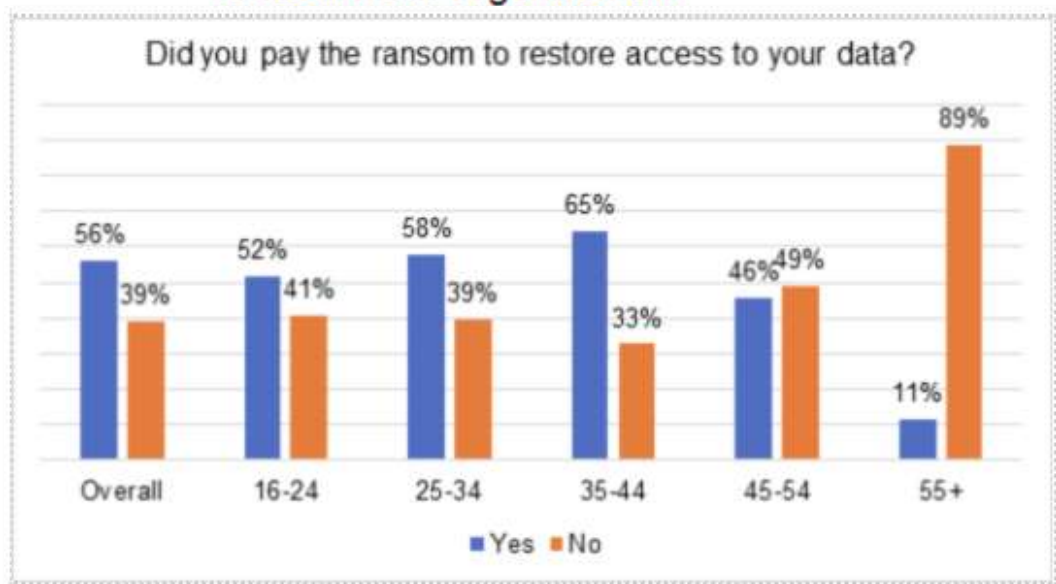


Bron: <https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland>

Onderzoek ransomware consumenten

Momenteel beweren ongeveer vier op de tien (39%) van de ondervraagden dat ze de afgelopen 12 maanden op de hoogte waren van ransomware. Het is belangrijk dat dit aantal stijgt naarmate werken op afstand productiever wordt. Om consumenten beter te helpen zichzelf te beschermen terwijl ze meer te weten komen over deze vorm van cyberaanval, is het essentieel dat ze begrijpen waar ze op moeten letten en wat ze moeten doen als ze ransomware tegenkomen.

Kaspersky Consumer
IT Security Risks
Report 2021



Bron: media.kasperskydaily.com

- Betaal geen losgeld
- Schakel een security expert in
- Klik niet op onbekende, onveilige links
- Open geen onbekende bijlage
- Bezoek geen onbekende website
- Gebruik geen onbekende USB-sticks
- Maak regelmatig een back-up
- Installeer beschermingssoftware

YOUR COMPUTER HAS BEEN LOCKED!

COMPUTABLE

Juist op die uiterst belangrijke toegang was de twee-factor authenticatie uitgezet

Opzet, Bestaan & Werking!

Schade hack bij Hof van Twente loopt op

Negen op de tien gemeentes vrezen ook slachtoffer te worden

6 april 2021 12:10 | Alfred Monterie

Topic Security

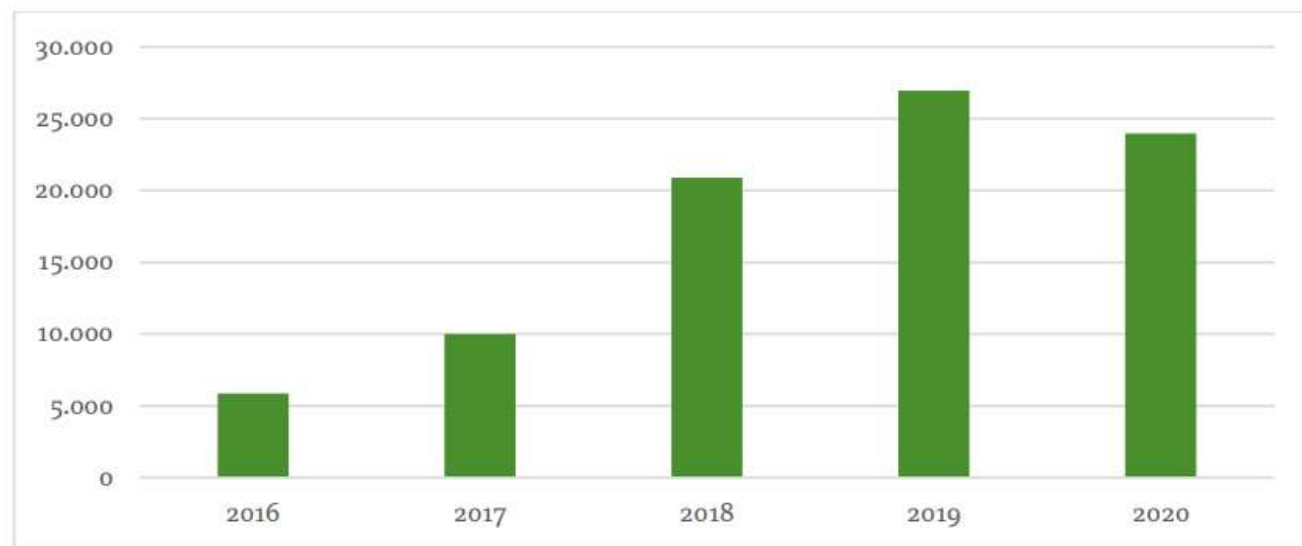
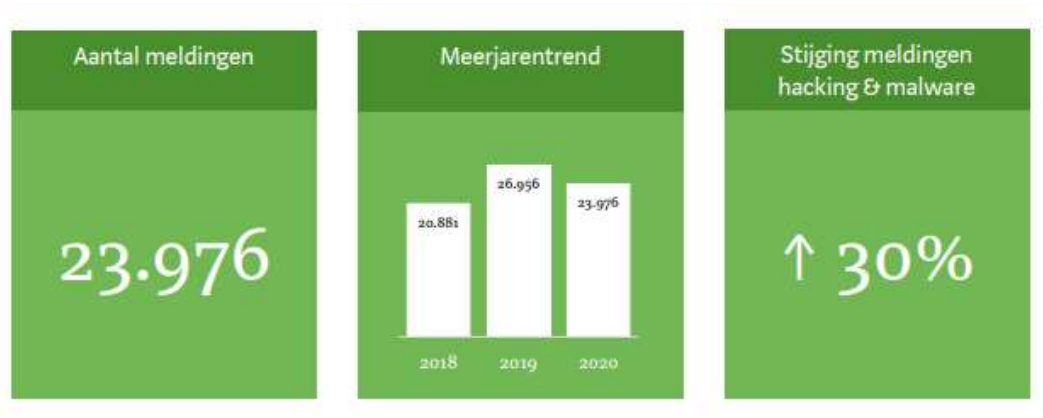


De gemeente Hof van Twente gaat minimaal drie à vier miljoen euro schade lijden als gevolg van de aanval met ransomware waardoor massaal basisdata verloren gingen. Per bewoner is dat zeker honderd euro verlies. De uiteindelijke strop kan nog behoorlijk oplopen.

Bewustzijn
Op papier leek alles behoorlijk goed te kloppen.

Het wachtwoord (Welkom2020) was te zwak.

Datalekken - feiten & cijfers



Totaal aantal datalek meldingen ontvangen door de AP 2016-2020

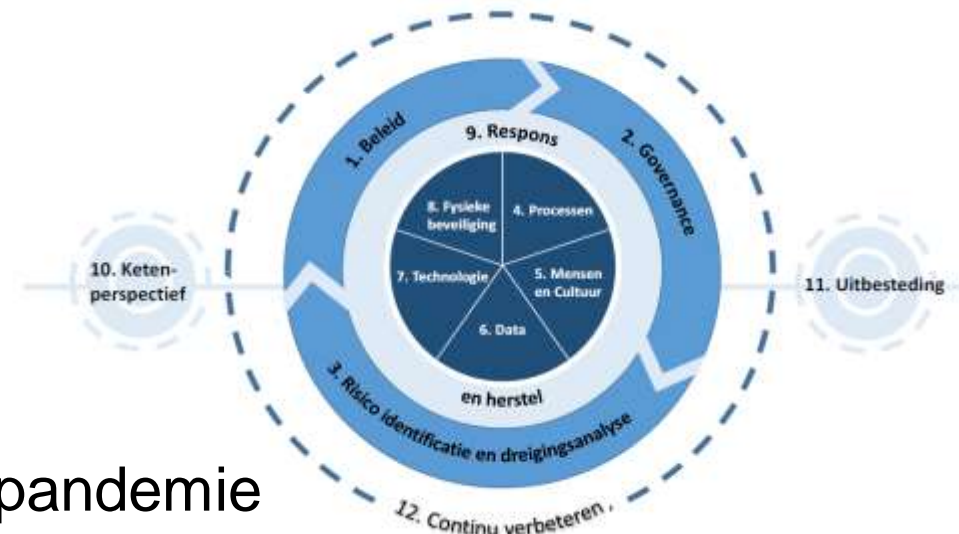
- Nederland in Top-3
- Toename door:
 - Hacking
 - Malware
 - Phishing
- Thema: MFA



Bron: [Autoriteit Persoonsgegevens](https://autoriteitpersoonsgegevens.nl)

Trends

- AFM “Principes voor Informatiebeveiliging”
- Uitvraag WTA-vergunninghouders
- NOREA IT-auditverklaring
- ISO 27001 certificering verplicht (bijvoorbeeld ARBO diensten)
- Enorme toename cybercrime tijdens de coronapandemie
- Veranderingen in wet- en regelgeving



Richtsnoeren AVG voor accountants, belastingadviseurs en salarisprofessionals

met betrekking tot de status als ‘verwerkingsverantwoordelijke’ of als ‘verwerker’ als bedoeld in de (Uitvoeringswet) Algemene verordening gegevensbescherming bij het verlenen van diensten aan klanten.

<https://www.nba.nl/nieuws-en-agenda/nieuwsarchief/2019/oktober/nba-nirpa-nob-novak-en-rb-publiceren-richtsnoeren-avg/>

Informatiebeveiliging

Cybersecurity

AVG

Privacy

Compliance

Awareness

ISO27001

Security

Audit

Cobit Riskmanagement

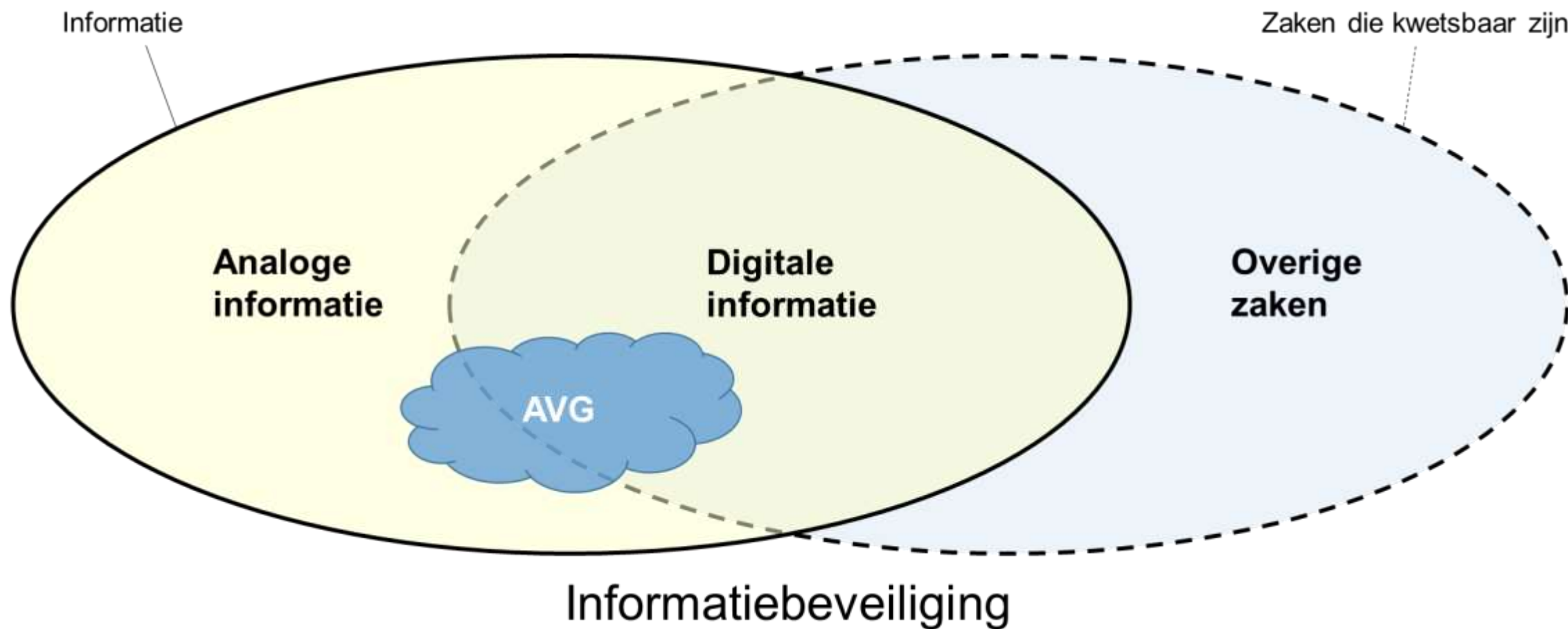
ITIL

FG

ISAE3402

Pointint

Kader - Informatiebeveiliging, Cyber Security & AVG



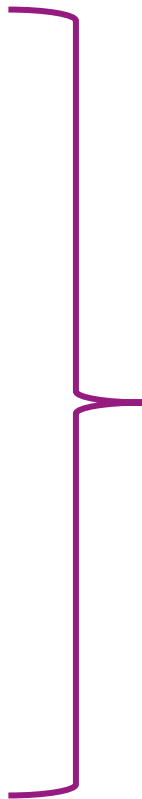
Informatiebeveiliging, Cyber Security & AVG

- Informatiebeveiliging kampt met imago
 - Meer dan ICT → Mens, Organisatie en Techniek
 - Beveiliging draagt onvoldoende bij aan de dienstverlening
- Inzicht in risico's niet integraal
 - Informatie over incidenten en maatregelen verspreid in de organisatie
 - Afhankelijkheid van externe partijen
 - Bekende risico's krijgen overmatig veel aandacht (AVG)
- Aanvallen succesvol door ontbreken basismaatregelen en bewustwording
- Onvoldoende risicomanagement; waan van de dag regeert
- Toenemende complexiteit en connectiviteit in het ICT-landschap
 - Schaduw-IT
 - Noodzaak voor multidisciplinaire aanpak en eigenaarschap



Beveiliging in vijf stappen

1. Stel het (beleids)kader vast; verdeel verantwoordelijkheden, bevoegdheden en taken
2. Breng risico's in kaart, bepaal het volwassenheidsniveau
3. Bepaal de gewenste maatregelen voor mens, techniek en organisatie
4. Omgaan met uitbesteden van IT-diensten
5. Beheersen en verbeteren

A large purple bracket on the right side of the slide groups steps 2, 3, and 4 of the list.

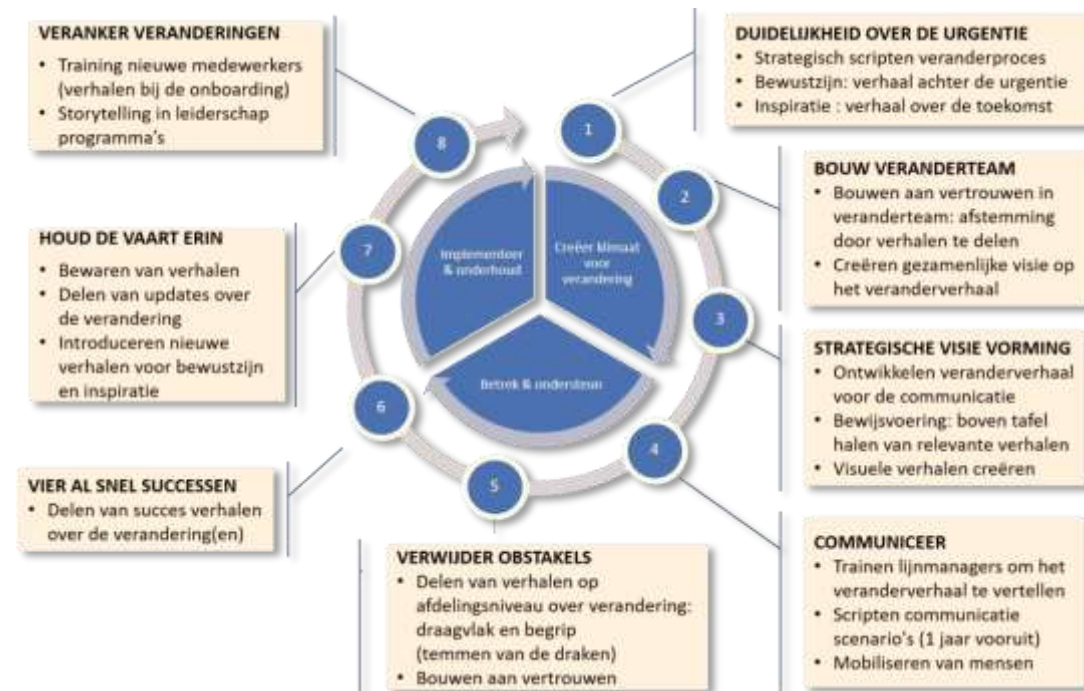
Selecteer de juiste hulpmiddelen en tools om in zetten



GOVERNANCE

Informatie(beveiligings)beleid

- Directieverantwoordelijkheid
- Uitgangspunten en risicobereidheid vaststellen (in lijn met organisatiebeleid en –doelstellingen)
- Eisen ten aanzien van:
 - Beschikbaarheid
 - Integriteit
 - Vertrouwelijkheid
- Periodieke evaluatie
- Beveiligingsbewustzijn bevorderen



Beleid en doelstellingen

- Bepaal het gewenste niveau
 - Management → Continue betrokkenheid / draagvlak
 - Cultuurverandering → Informatieveiligheid moet tweede natuur worden

- Inventariseer hoe ver u van het doel bent verwijderd
 - Meldingen als indicator
 - Proef op de som nemen (nulmeting)

- Bepaal hoe u de 'awareness gap' gaat overbruggen.
 - Basisgebieden: kennis, houding en gedrag
 - Gebruik momentum
 - Let regels uit

- Plan activiteiten
 - Communiceer (per doelgroep)
 - Varieer (vb: awareness games, informele bijeenkomsten)
 - Beloon positief gedrag; security is niet vrijblijvend.

- Evalueer, stel bij en herhaal.

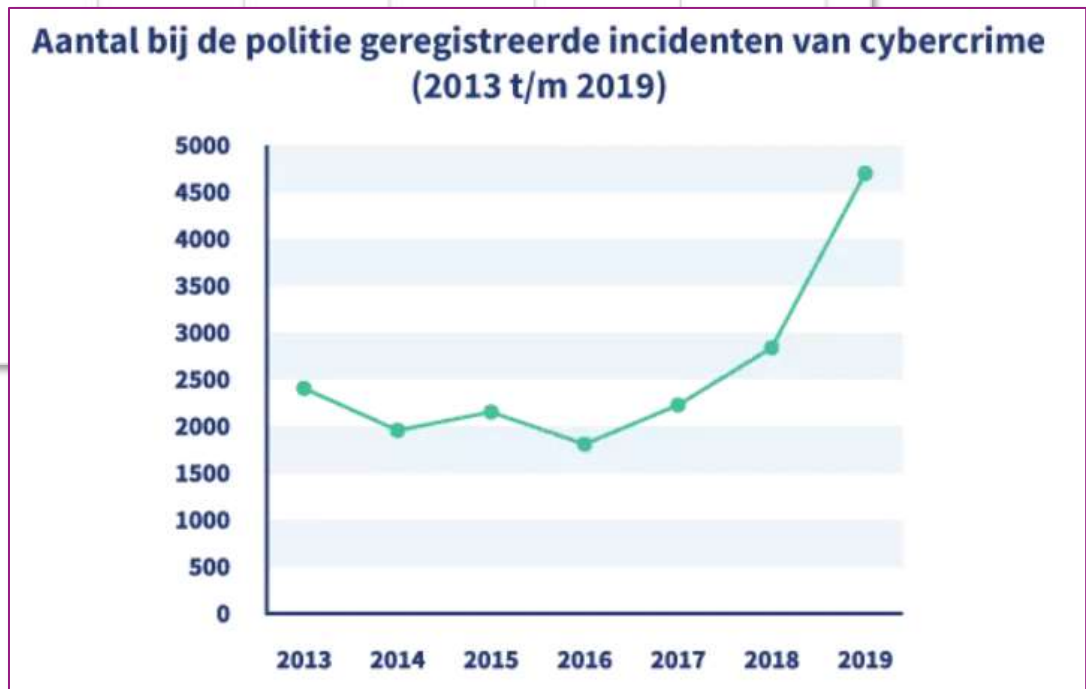
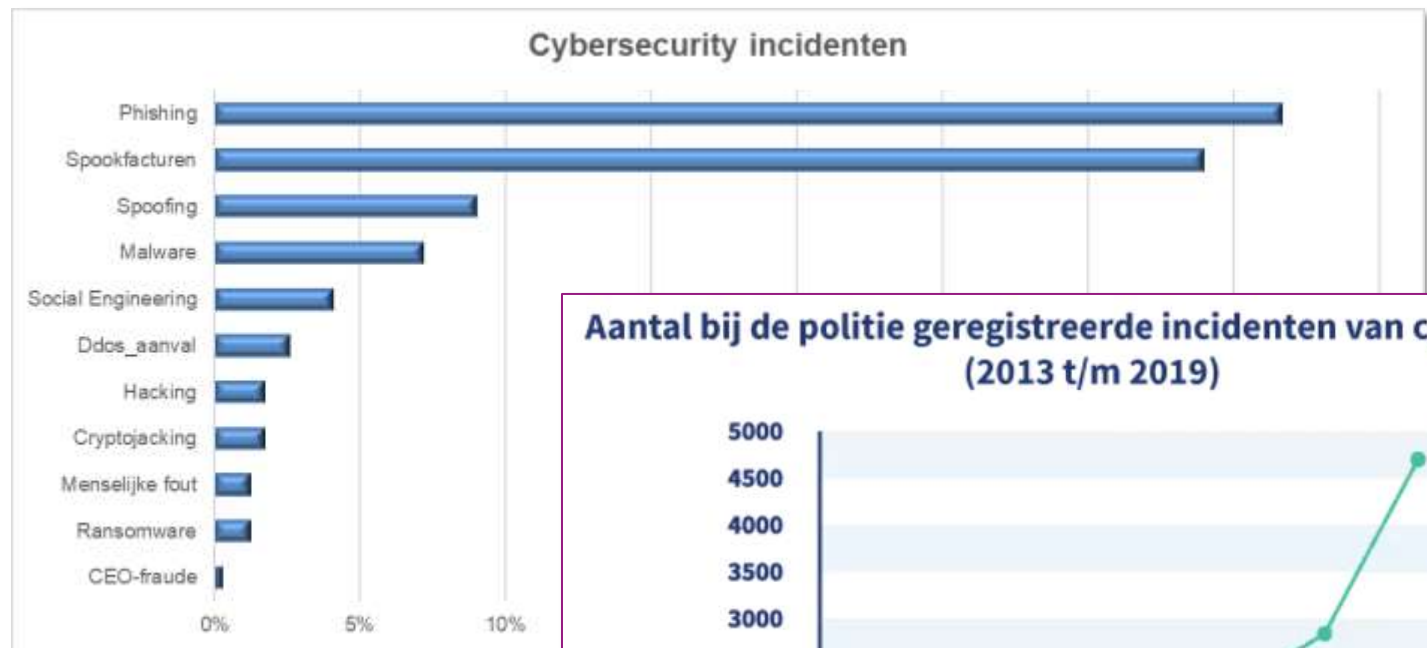


Risk Assessment

Severity	Disaster	High	Medium	Minimal
Probability				
Regularly	Critical	Critical	High	Medium
Probable	Critical	High	Medium	Medium
Occasional	Critical	High	Low	Low
Rarely	High	Medium	Medium	
Improbable	Medium			

Veelvoorkomende dreigingen op een rij

- Phishing
- Ransomware
- Netwerkaanvallen
- CEO-fraude
- Spoofing
- Cryptojacking
- DDoS-aanvallen



Voorbeeld



Geachte relatie,

Wij nemen contact met u op om u te laten weten dat wij met ingang van 1 januari 2020 enkele wijzigingen hebben doorgevoerd in ons privacybeleid. Deze wijzigingen weerspiegelen de striktere privacy en wetgeving eisen van de Algemene Gegevensbescherming (bekend als de AVG) die banken in Nederland moeten voldoen.

Als bank mogen wij onze producten en dienstverlening alleen openstellen voor klanten van wie wij de identiteit hebben vastgesteld. Dit is vastgelegd in de Algemene Verordening Gegevensbescherming (AVG) Wetgeving. Deze wet helpt ons om onze klanten te beschermen en hun veiligheid te waarborgen.

Uit ons klantenbestand is naar voren gekomen dat uw contactgegevens niet compleet zijn. Het is belangrijk dat wij uw meest actuele contactgegevens in bezit hebben, zodat wij u kunnen bereiken indien het nodig is.

Wij verzoeken u om de juiste contactgegevens aan ons door te geven. Doet u dit niet, dan kunt uw rekening geblokkeerd worden: u kunt dan niet meer betalen of geld van opnemen. Klik hier om uw contactgegevens bij te werken. Is uw rekening al geblokkeerd? Dan is het van noodzaak om uw te identificeren, zodat u weer volledig gebruik kunt maken van uw rekening.

Heeft u nog vragen?

Meer informatie vindt u op [rabobank.nl/privacy](https://www.rabobank.nl/privacy). Staat het antwoord er niet bij? Neem dan contact met ons op. Wij helpen u graag!

Alvast hartelijk dank voor uw medewerking.

Met vriendelijke groet,
Rabobank



Dit bericht lijkt gevaarlijk

Het bericht bevat een verdachte link die is gebruikt om persoonlijke informatie van mensen te stelen. Klik niet op links en beantwoord het bericht niet met persoonlijke informatie.



Linda van Dijk | SRA



Van: Linda Van Dijk <lvandijk@sra.lu>
Verzonden: donderdag 5 november 2020 15:56
Aan: Tony van Oorscot | SRA <tvanoorscot@sra.nl>
Onderwerp: Sollicitatiepagina probleem

icitiatiepagina
<https://sra.lu/nl/vergeten/?sid=eshsousjbbxnmyhhtx8alckbyymqtspj>
Ctrl+klikken voor koppeling
om [deze pagina](#) te laden? Voor mij lukt het, maar v

Hoi Tony,

Lukt het voor jou om [deze pagina](#) te laden? Voor mij lukt het, maar voor een potentiële sollicitant dan weer niet..

Met vriendelijke groet,

Linda Van Dijk
HR Adviseur



Rijnzathe 14
3454 PV Utrecht
www.sra.nl

T 030 656 60 60

E lvandijk@sra.nl

Let op:

- Afzender
- Aanhef
- Open geen onbekende bijlage(n)
- Klik niet op onbekende, onveilige links
- Bezoek geen onbekende website
- Taalgebruik en –fouten
- Urgentie
- Vraag naar persoonlijke gegevens

Heeft u al eens te maken gehad met een datalek?



YES



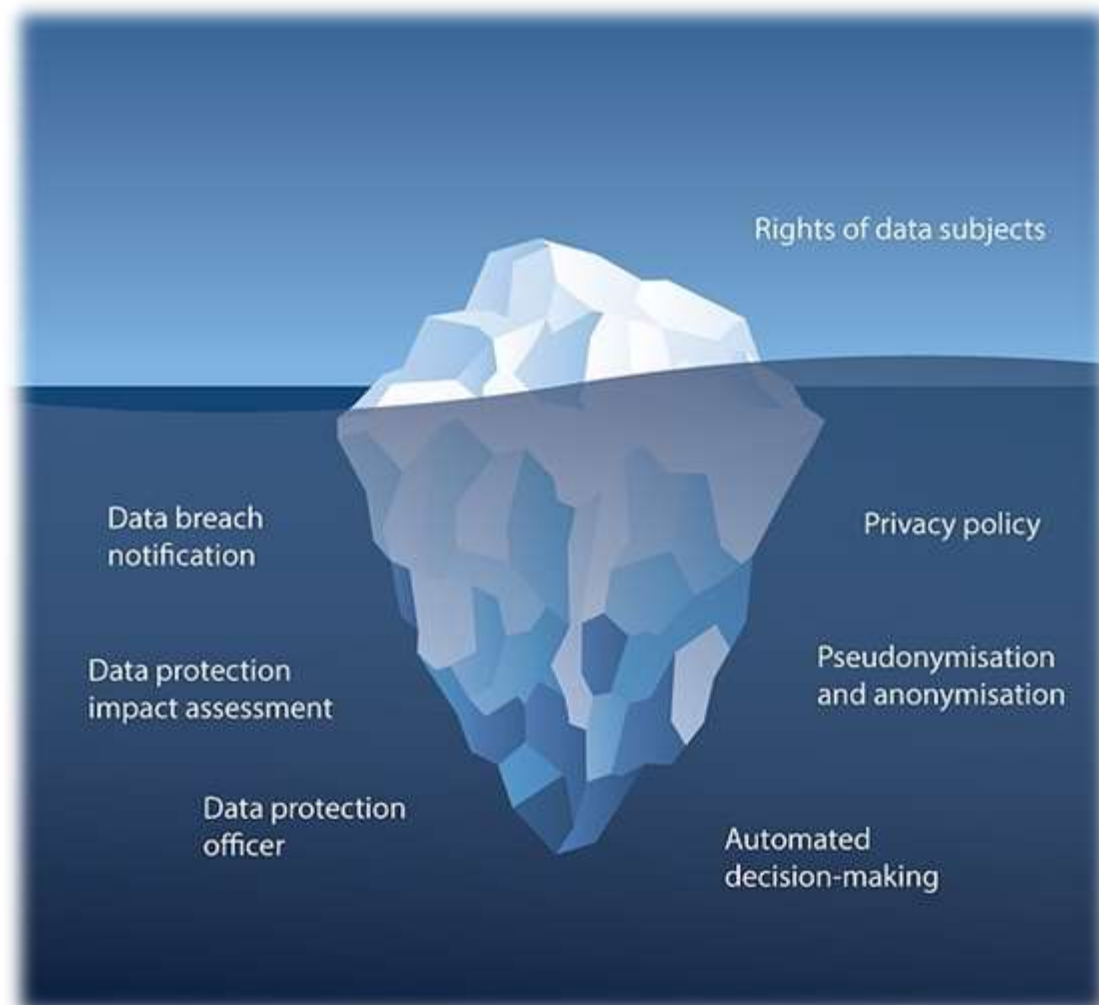
NO



MAYBE

De juiste volgorde

- Risico-analyse
 - Mitigeren
 - Delen ('cyberriskverzekering')
 - Vermijden (stoppen)
 - Accepteren (inclusief onbekende risico's)
- Maatregelen:
 - Controls op de belangrijkste risico's
 - Dataclassificatie
 - Disaster recovery plan
- Tools



Risico-analyse

■ Impact analyse

- Hoe belangrijk is deze informatie / dit systeem voor de organisatie?
- Wat is de impact voor de organisatie bij een probleem?



Mogelijke risico's

Voor de organisatie

- Negatieve publiciteit en imagoschade.
- Dwangmaatregelen en/of boetes opgelegd door de toezichthouder.
- Schadeclaims door betrokkenen.
- Hogere kosten bij het achteraf nemen van privacy maatregelen.
- Slechte datakwaliteit leidt tot slechtere performance van de business.
- Datalekken leiden tot wantrouwen.
- Ziekte van medewerkers
- Rem op innovatief vermogen
- Personeelstekort



Bij uitbesteding van IT

- Verlies van kennis en skills van medewerkers
- Afname flexibiliteit
- Verlies van contact met eindgebruikers
- Bepalen van de toegevoegde waarde
- Interpretatieverschillen over contract / SLA
- Kosten voor issues buiten contract / SLA
- Afhankelijkheid ('vendor lock-in')
- Verkeerde verwachtingen over geleverde (niveau) van diensten
- Uit elkaar groeien van partijen; botsende visies en culturen

Risico's waar we vaak niet aan denken

- Bestanden belanden in de prullenbak
- Chaos op de (thuis)werkplek
- Delen van mailboxen en wachtwoorden
- Een eenvoudig centraal wachtwoord voor iedereen voor alles
- Gastvrijheid op het kantoor “Kom binnen!”
- Gebruik van privé USB-sticks, externe harde schijven, enz
- Gebruik van persoonlijke e-mailaccounts voor het werk
- Incidenten en datalekken verzwijgen
- Ontbreken van voorwaarden in contracten over data en privacy
- Onduidelijkheid over bewaartermijnen
- Te veel informatie verstrekken (via de telefoon)



Risico-analyse

■ Impact analyse

- Hoe belangrijk is deze informatie / dit systeem voor de organisatie?
- Wat is de impact voor de organisatie bij een probleem?

■ In kaart brengen van de stakeholders en actoren

- Extern : cybercriminelen, leveranciers en klanten
- Intern : directie en medewerkers

■ De dreigingsanalyse

- Kans en impact bepalen
- Bepalen hoe moet worden omgegaan met het risico (incl. het restrisico)
- Maatregelen:
 - Huidige situatie / huidige maatregelen
 - Gewenste situatie / te nemen acties



Request Identification Number

W-9

File (Department 2010)
 Issued by the Internal Revenue Service

Name (Print or type name, if different from above)

Address (Print or type name, if different from above)

City, State, and ZIP code

Check appropriate box for federal tax withholding:

Individual proprietor
 Limited liability company
 Sole proprietor
 Partnership
 Trust
 Estate
 Beneficiary of a trust (other than a grantor trust)
 Nonresident alien individual
 U.S. citizen or resident alien who has elected to be treated as a nonresident alien for tax purposes

Signature (Print or type name, if different from above)

Date

1040 U.S. Individual Income Tax Return

For the year ended Dec. 31, 2011, or other tax year beginning

Your last name and initial

Last name

If a joint return, spouse's first name and initial

Last name

Home address (number and street), if you have a P.O. box, use subdivisions

City, State or post office, state, and ZIP code, if you have a foreign address, also include country

Foreign country name

Filing Status

1 Single
 2 Married filing jointly
 3 Married filing separately
 4 Head of household
 5 Qualifying widow(er)

Check only one box

Department of the Treasury
 Internal Revenue Service

Publication 3
 Cat. No. 40072M

Armed Forces' Tax Guide

in preparing returns

Department of the Treasury
 Internal Revenue Service

Publication 17
 Catalog Number 10011A

For use in preparing 2010 Returns

Your Federal Income Tax
 For Individuals



TAX GUIDE 2011

Internal Revenue Service
 1201 N. Milwaukee Motorway
 Bloomington, IL 61705-6613

Tax questions. If you have information available on IRS.gov, we cannot answer tax questions above addresses.

Useful Items
 You may want to see:

- Publication**
- 54 Tax Guide for Armed Forces
 - 463 Travel Expenses
 - 501 Excess Income
 - 503 Charitable Contributions
 - 505 Tax Expenditures
 - 516 Tax Expenditures
 - 519 Tax Expenditures



Your Federal Income Tax For Individuals

Contents

What's New for 2010

Reminders

Introduction

Part One. The Income Tax Return

- 1 Filing Information
- 2 Filing Status
- 3 Personal Exemptions and Dependents
- 4 Tax Withholding and Estimated Tax

Part Two. Income

- 5 Wages, Salaries, and Tax Tips Income
- 6 Dividends
- 7 Annuities
- 8 Capital Gains and Dividends
- 9 Retirement Income
- 10 Social Security
- 11 Unemployment Compensation
- 12 Other Income
- 13 Tax on Income
- 14 Tax on Income
- 15 Tax on Income
- 16 Tax on Income
- 17 Tax on Income
- 18 Tax on Income
- 19 Tax on Income
- 20 Tax on Income
- 21 Tax on Income
- 22 Tax on Income
- 23 Tax on Income
- 24 Tax on Income
- 25 Tax on Income
- 26 Tax on Income
- 27 Tax on Income
- 28 Tax on Income
- 29 Tax on Income
- 30 Tax on Income
- 31 Tax on Income
- 32 Tax on Income
- 33 Tax on Income
- 34 Tax on Income
- 35 Tax on Income
- 36 Tax on Income

Your Rights as a Taxpayer

This section explains some of your most important rights as a taxpayer, including the examination, appeal, collection, and refund processes.

Declaration of Taxpayer Rights

Protection of your rights. IRS employees will explain and protect your rights as a taxpayer through our contact with us.

Privacy and confidentiality. The IRS will not disclose to anyone the information you give us, except as authorized by law. You have the right to know why we are asking you for information, how we will use it, and what will happen if you do not provide requested information.

Professional and courteous service. If you believe that an IRS employee has not treated you in a professional, fair, and courteous manner, you should file a complaint with your supervisor. If the supervisor's response is not satisfactory, you should write to the director for your area or the center where you filed your return.

Representation. You may either represent yourself or, with proper written authorization, have someone else represent you in your place. Your representation must be a person allowed to practice before the IRS, such as an attorney, certified public accountant, or enrolled agent. If you are an interviewee and ask to consult with a person, then we must stop and reschedule the interview in most cases.

Payment of only the correct amount of tax. You are responsible for making accurate calculations of your tax liability or certain collection actions, you have the right to ask the Appeals Office to review your case. You may also ask a court to review your case.

Relief from certain penalties and interest. The IRS will waive penalties and interest if you can show you acted reasonably and in good faith or relied on the incorrect advice of an IRS employee. We will waive interest that is the result of certain errors or delays caused by an IRS employee.

Examinations (Audits)

We accept most taxpayers' returns as filed. If we inquire about your return or select it for examination, it does not suggest that you are dishonest. The inquiry or examination may or may not result in more tax. We may close your case without change or you may receive a refund.

The process of selecting a return for examination usually begins in one of two ways. First, we use computer programs to identify returns that may have incorrect amounts. These programs may be based on information returns, such as Forms 1099 and W-2, on studies of past examinations, or on certain issues identified by compliance projects. Second, we use information from outside sources that indicate that a return may have incorrect amounts. These sources may include newspapers, public records, and individuals. If we determine that the information is accurate and reliable, we may use it to select a return for examination.

Publication 556, Examination of Returns, Appeal Rights, and Claims for Refund, explains the rules and procedures that we follow in examinations. The following sections give an overview of how we conduct examinations.

By mail. We handle many examinations and inquiries by mail. We will send you a letter with either a request for more information or

an examiner proposes any changes to your return, he or she will explain the reasons for the changes. If you do not agree with these changes, you can meet with the examiner's supervisor.

Repeat examinations. If we re-examine your return for the same items as either of the 2 previous years and proposed no change to your tax liability, please contact us as soon as possible so we can use it as soon as possible to the examination.

Appeals

If you do not agree with the examiner's proposed changes, you can appeal them to the Appeals Office of IRS. Most differences can be settled without expensive and time-consuming court trials. Your appeal rights are explained in detail in both Publication 5, Your Appeal Rights and How To Prepare a Protest If You Don't Agree, and Publication 556, Examination of Returns, Appeal Rights, and Claims for Refund.

If you do not wish to use the Appeals Office of disputes with its findings, you may be able to take your case to the U.S. Tax Court, U.S. Court of Federal Claims, or the U.S. District Court where you live. If you take your case to court, the IRS will have the burden of proving certain facts if you keep adequate records to show your tax liability, incorporated with the IRS, and meet certain other conditions. If the court agrees with you on most issues in your case and finds that our position was largely justified, you may be able to recover some of your administrative and litigation costs. You will not be eligible to recover these costs unless you first to resolve your case administratively, including going through the appeals system, and you give us the information necessary to resolve the case.

Refunds

You may file a claim for refund if you think you paid too much tax.

Potential Third Party Contacts

Generally, the IRS will deal directly with you or your duly authorized representative. However, we sometimes talk with other persons if we need information that you have been unable to provide, or to verify information we have received. If we do contact other persons, such as a neighbor, bank, employer, or employer, we will generally need to tell them limited information, such as your name. The law prohibits us from disclosing any more information than is necessary to obtain or verify the information we are seeking. Our need to contact other persons may continue as long as there is activity in your case. If we do contact other persons, they have a right to request a list of those contacted.

Introduction

This publication covers the special tax situations of active members of the U.S. Armed Forces, military pensions, and rules that

Introduction

This publication covers the special tax situations of active members of the U.S. Armed Forces, military pensions, and rules that

Introduction

This publication covers the special tax situations of active members of the U.S. Armed Forces, military pensions, and rules that

Introduction

This publication covers the special tax situations of active members of the U.S. Armed Forces, military pensions, and rules that

Introduction

This publication covers the special tax situations of active members of the U.S. Armed Forces, military pensions, and rules that

Part Five. Standard Deduction and Limited Deductions

- 20 Standard Deduction
- 21 Medical and Dental Expenses
- 22 Charitable Contributions
- 23 Interest Expense
- 24 Contributions
- 25 Miscellaneous Casualty and Theft Losses and Other Expenses
- 26 Work-Related Expenses
- 27 Deductions
- 28 Deductions
- 29 Tax
- 30 Tax
- 31 Tax
- 32 Tax
- 33 Tax
- 34 Tax
- 35 Tax
- 36 Tax

Part One. The Income Tax Return

- 1 Filing Information
- 2 Filing Status
- 3 Personal Exemptions and Dependents
- 4 Tax Withholding and Estimated Tax

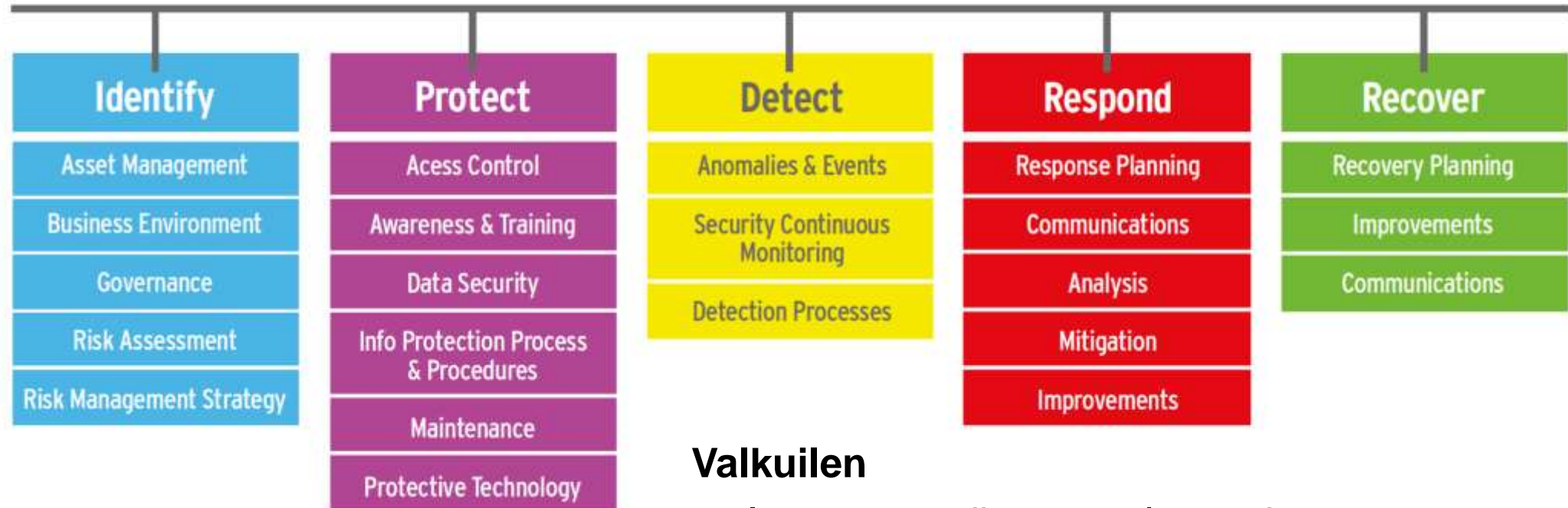
Part Two. Income

- 5 Wages, Salaries, and Tax Tips Income
- 6 Dividends
- 7 Annuities
- 8 Capital Gains and Dividends
- 9 Retirement Income
- 10 Social Security
- 11 Unemployment Compensation
- 12 Other Income
- 13 Tax on Income
- 14 Tax on Income
- 15 Tax on Income
- 16 Tax on Income
- 17 Tax on Income
- 18 Tax on Income
- 19 Tax on Income
- 20 Tax on Income
- 21 Tax on Income
- 22 Tax on Income
- 23 Tax on Income
- 24 Tax on Income
- 25 Tax on Income
- 26 Tax on Income
- 27 Tax on Income
- 28 Tax on Income
- 29 Tax on Income
- 30 Tax on Income
- 31 Tax on Income
- 32 Tax on Income
- 33 Tax on Income
- 34 Tax on Income
- 35 Tax on Income
- 36 Tax on Income



Maatregelen

NIST Cyber Security Framework



Bron: <https://www.nist.gov>

Valkuilen

- Iets eenvoudigs complex maken
- Alles willen oplossen
- Niet eens zijn over het risico
- De ultieme oplossing willen hebben
- Te complexe oplossing

Best practices

■ Identificeer

- Awareness, de menselijke firewall
- Bedrijfscontinuïteit, maak een plan
- Kroonjuwelen bepalen

■ Bescherm

- Train de medewerkers
- Zorg voor digitale hygiëne
- Backup, volgens de 3-2-1-1-0-regel

■ Ontdek

- Installeer detectiesystemen
- Plaats virtuele struikeldraden

■ Reageer

- Zorg voor een incident-respons plan
- Wees kalm en betrouwbaar

■ Herstel

- Maak een herstelplan
- Ontwerp je herstel



Bron: Veeam

Medewerkers



- Vertel de medewerker duidelijk wat deze moet doen.
- Pas op dat je niet ongeduldig wordt als het niet snel genoeg gaat.
- Coach de medewerker.
- Pas op dat je de medewerker niet betuttelt of niet serieus neemt.
- De medewerker weet wat te doen.
- Pas op met teveel opdrachten omdat deze medewerkers al weten wat ze moeten doen.
- Naar deze medewerker heb je geen omkijken.
- Pas op met teveel vrijheid, dit kan leiden tot verlies aan betrokkenheid.

Dan willen we nu een tool!



What the customer really needed



How the customer explained it



How the project leader understood it



How the analyst designed it



How the programmer wrote it



What the beta testers received



How the business consultant described it



How the project was documented



What operations installed



How the customer was billed



How it was supported



What marketing advertised



When it was delivered



What the digg effect can do to your site



The disaster recover plan

Iedereen heeft z'n eigen perspectief

- Eenvoud
- Voldoen aan administratieve (privacy) verplichtingen
- Verantwoording (“zijn we compliant?”)
- Bescherming van data (encryptie, logische toegang)
- Kennis
- Forensische tooling (“wat is er gebeurd?”)



Aandachtspunten

- Veel (nieuwe) marktpartijen
- Terminologie; wat is wat?

Tools

- Gebruiksvriendelijkheid; wie zijn de gebruikers?
- Ondersteuning bij implementatie
- Wat kun je met de resultaten?
- Hoe zit het met de kosten?
 - Aanschaf / abonnement
 - Implementatie
 - Gebruik en beheer
- Een hele suite? Ga je alles wel echt gebruiken





Moderne Internetstandaarden zorgen voor meer betrouwbaarheid en verdere groei van het Internet.
Gebruik jij ze al?

Test je website

Modern adres? Ondertekend domein?
Beveiligde verbinding? Beveiligingsopties?
[over de test >](#)

Jouw website-domeinnaam:

[Start test](#)

Test je e-mail

Modern adres? Ondertekend domein? Anti-phishing? Beveiligde verbinding?
[over de test >](#)

Jouw e-mailadres:

[Start test](#)

Test je verbinding

Moderne adressen bereikbaar?
Domein-handtekeningen gecontroleerd?
[over de test >](#)

[Start test](#)



You are here: [Home](#) > [Projects](#) > SSL Server Test

SSL Server Test

<https://www.ssllabs.com/ssltest/>

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. **Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.**

Hostname:

[Submit](#)

Do not show the results on the boards



Risicoklassen

1 Inventarisatie van Kwetsbaarheden			
		Het vergroten van de weerbaarheid tegen cyberincidenten begint bij inzicht. Inzicht in de kwetsbaarheden van bedrijfssystemen en de risico's. Begin daarom met een inventarisatie en denk na over wat je wel en niet moet doen bij een cyberincident.	
		Inventarisatie van kwetsbaarheden	
1a		Maak en onderhoud een inventarisatielijst van alle computers, software, clouddiensten, slimme apparaten etc., voorzien van bijbehorende software-versies en serienummers. Zie voor een voorbeeld bijlage 1. Maak deze inventarisatie ook als je zaken hebt uitbesteed aan een leverancier.	Actualiseer minimaal elke 3 maanden.
1b		Controleer of onbekende apparaten en software in de omgeving aanwezig zijn en geef hier opvolging aan.	Controleer in een continue proces en volg indien nodig op.
1c		Maak een inventarisatie van onderdelen en informatie die bedrijfskritisch en gevoelig zijn. Denk hierbij aan eigen vindingen, formules, modellen en andere concurrentiegevoelige informatie.	Actualiseer minimaal elke 3 maanden.
		Back-up en recovery Door een cyberincident kan bedrijfsdata verloren gaan of geïnfecteerd raken. Hierdoor kunnen de primaire bedrijfsprocessen stil komen te liggen. Het consequent maken van back-ups, draagt bij aan het snel herstellen van de verloren gegevens, zodat de onderneming vlot weer aan de slag kan.	

Risicoklasse

11 vragen te
maatregelen die bij

<https://tools.digitaltrustcenter.nl/check-je-risicoklasse/>

Wachtwoorden



Tips over wachtwoorden

- Test je wachtwoord(en)



- Gebruik tweetrapsverificatie



Google Authenticator



- Gebruik een password manager



KeePass



MIND
YOUR
PASS



Hoe eenvoudig is jouw wachtwoord te kraken?

Beantwoord de volgende vragen

1 Hoe lang is jouw wachtwoord? (Tel alle letters, cijfers en/of andere tekens op.)

Progress bar showing 22 characters

2 Welke karakters staan er in jouw wachtwoord? (Meer opties mogelijk.)

<input checked="" type="checkbox"/> Kleine letters (a-z)	<input checked="" type="checkbox"/> Hoofdletters (A-Z)
<input checked="" type="checkbox"/> Cijfers (0-9)	<input checked="" type="checkbox"/> Speciaal (#,&,!)

<https://veiliginternetten.nl/wachtwoordkraak-test/>

Thuiswerken - Het kantoor als ontmoetingsplek



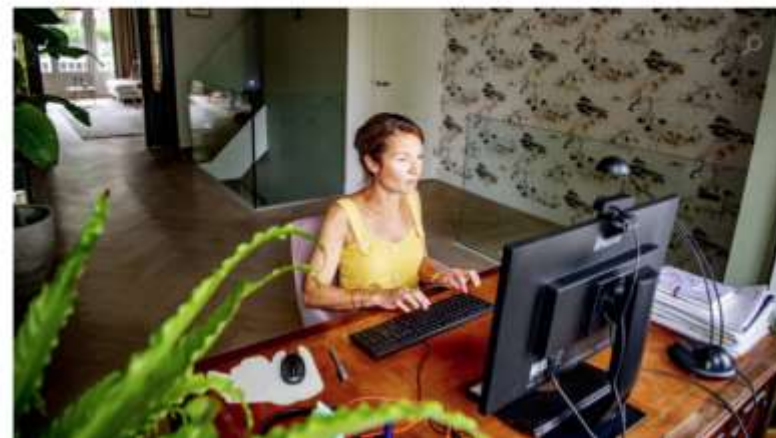
Aandachtspunten voor thuiswerken

- Gebruik van privé computers en (wifi)netwerk
 - Updates en upgrades
 - Antivirus
- Gebruik van online software en websites
- Toegang tot vertrouwelijke bestanden
- Veilige verbindingen (kantoor en applicaties)
- Procedures en richtlijnen:
 - Wat deel je wel / niet
 - Gebruik van vertrouwelijke bestanden
 - Afsluiten (🔒 + L)
 - Opname videovergaderingen
 - ...
- Wees je bewust van valse e-mails / phishing

“Hoe weet ik dat medewerkers via een veilig (wifi) netwerk werken (thuis, bij klanten of elders) of hoe kan dat goed beveiligd worden?”

ROE NIEUWS • ECONOMIE • VRIJDAG, 15 SEP • AANGEPAST VRIJDAG, 16 SEP

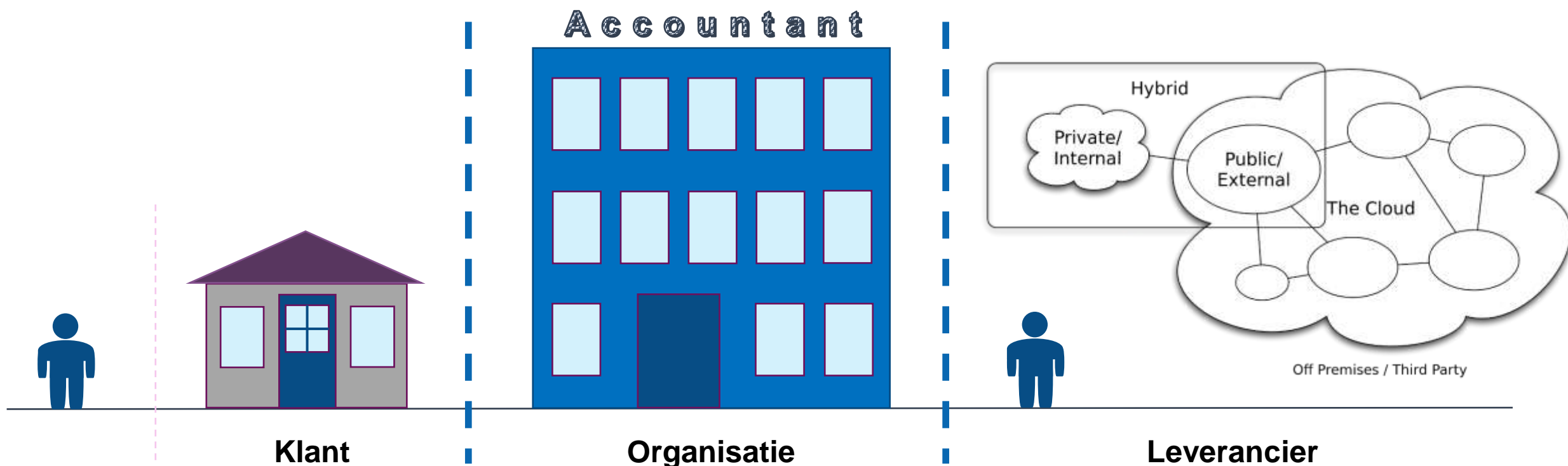
Het thuiswerkadvies vervalt, maar we gaan niet direct naar kantoor



<https://www.digitaltrustcenter.nl/thuiswerken>

(CI)outsourcing

- Integrale ketenbenadering bij het bepalen van informatiebeveiligingsrisico's en beheersmaatregelen
- Afspraken met klanten en leveranciers



Werken in de cloud

*Als je gehost bent: wat is dan het hackrisico?
Waar moet je op letten of wat kan je verlangen?*

Algemeen

- Multi-factor authenticatie
 - Beheerders
 - Gebruikers
- Rollen en rechten
- Logging
- Alerts
- Verouderde protocollen en applicaties
- Afspraken m.b.t. thuiswerken

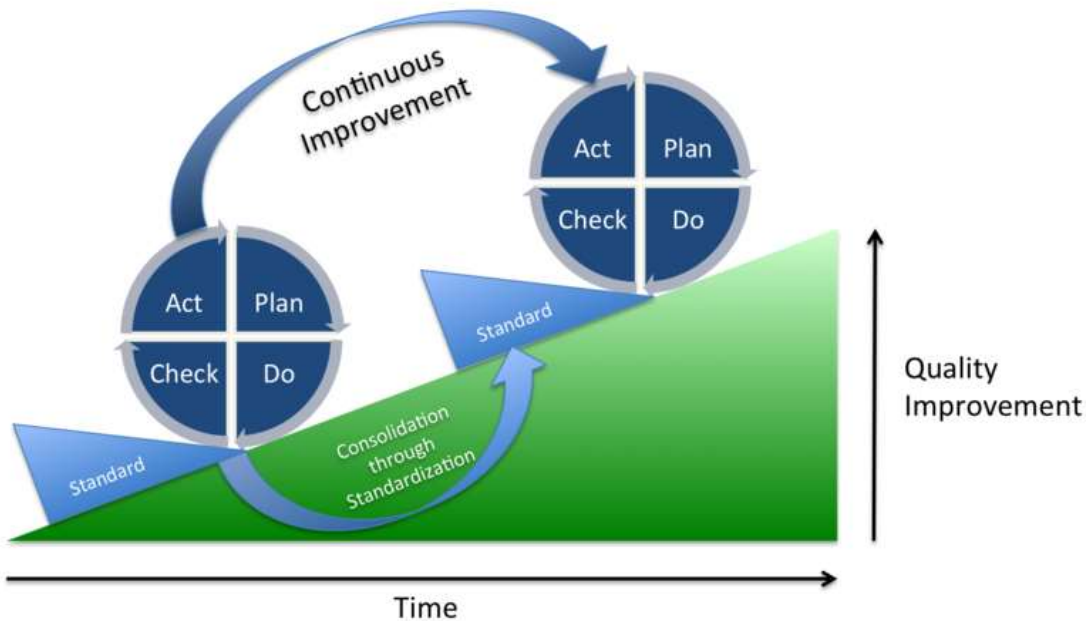
Meer info: <https://www.digitaltrustcenter.nl/nieuws/veilig-werken-in-cloud-werkomgevingen>

Afspraken met je leverancier

- Uitbestede producten en diensten
- Onderhoudswerkzaamheden
- Getroffen beveiligingsmaatregelen
- Werkplekondersteuning en –beveiliging
- Gegevensbescherming
- Omgaan met incidenten en datalekken
- Service levels en rapportage
- Exit-procedure

Meer info: <https://www.digitaltrustcenter.nl/informatie-advies/afspraken-maken-met-een-it-leverancier>

Evaluëren en verbeteren



- Plan een evaluatie
- Zorg voor inhoud
 - Incidenten en resultaten
 - Impact op het proces
- De juiste mensen aan tafel
- Bepaal de verbeterpunten; maak een lijst (korte en lange termijn)
- Benoem verantwoordelijken voor verbeterpunten
- Communiceer over het oplossen van verbeterpunten
- Plan een (her)test

Tips voor betere cyber weerbaarheid

Alertheid

- Vergroot bewustzijn bij medewerkers
- Volg actuele ontwikkelingen

Preventie

- Organiseer de back-up en test de back-up procedure regelmatig
- Oefen herstelprocedures
- Zorg voor een actief update beleid; voer updates zo snel mogelijk uit
- Beperk toegang tot data; toegang van medewerkers afhankelijk hun rol, functie en daarbij behorende rechten.

Detectie

- Monitor systemen en de dagelijkse operatie
- Test jezelf!

Valkuilen bij selectie van oplossingen / leveranciers

- Aandacht voor security & privacy
- Flexibiliteit / schaalbaarheid
- Ervaring
- Omgaan met hybride omgevingen
- Exit-strategie



Samengevat



Aan de slag

- Zet informatiebeveiliging op de agenda; benut de kansen vanuit de AVG
- Maak mensen verantwoordelijk
- Budgetteer informatiebeveiliging
- Rapporteer en analyseer incidenten
- Blijf zorgen voor bewustwording
- Zorg voor security by design (en privacy by design)



**“Tech support says the problem is located
somewhere between the keyboard and my chair.”**

Source: <http://www.glasbergen.com/>

Geiger-project

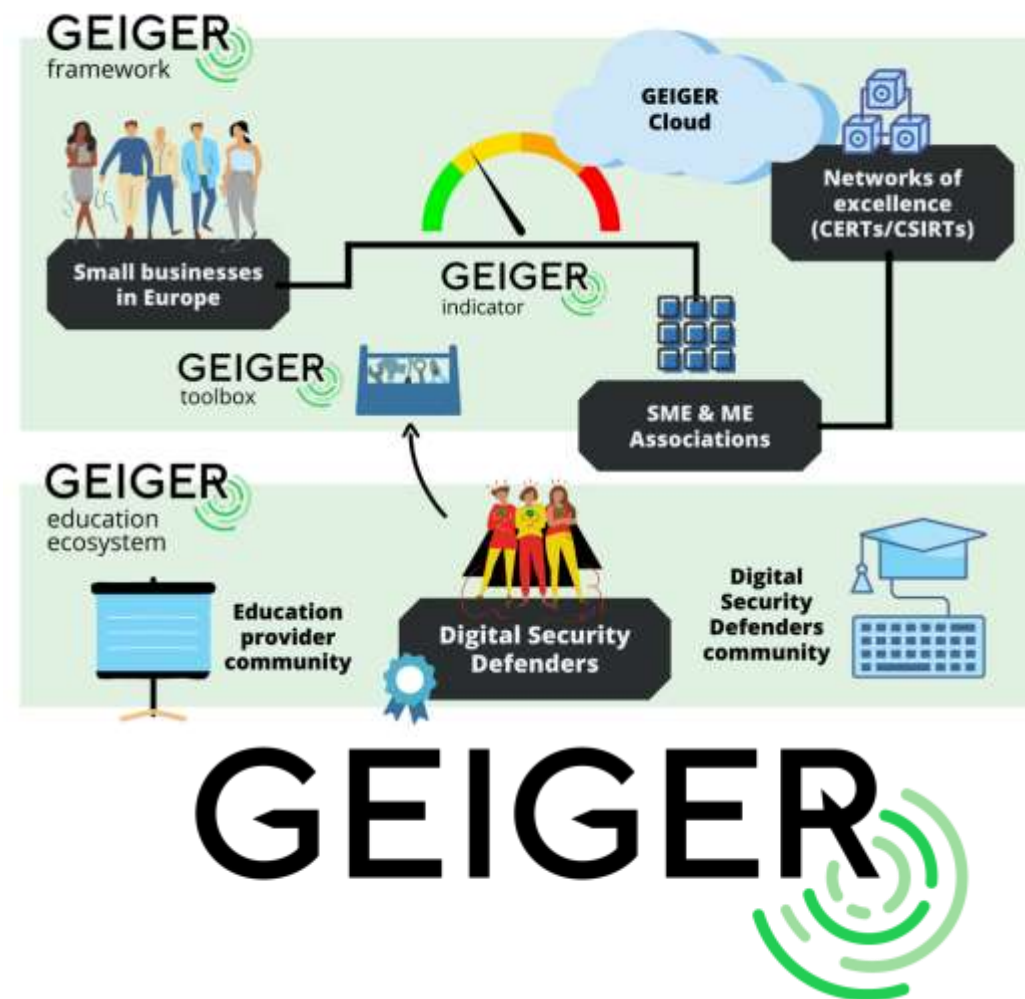
Innovatieproject voor het mkb op het gebied van cyberbeveiliging

- Tool: 'Geigerteller' voor cyberbeveiliging
- Opleidingsprogramma

In Nederland

- Accountant als trusted advisor
- Kick-off meeting 18 november

➤ Meer informatie: <https://www.sra.nl/geiger/>





Bedankt voor uw aandacht.