INFRABEL

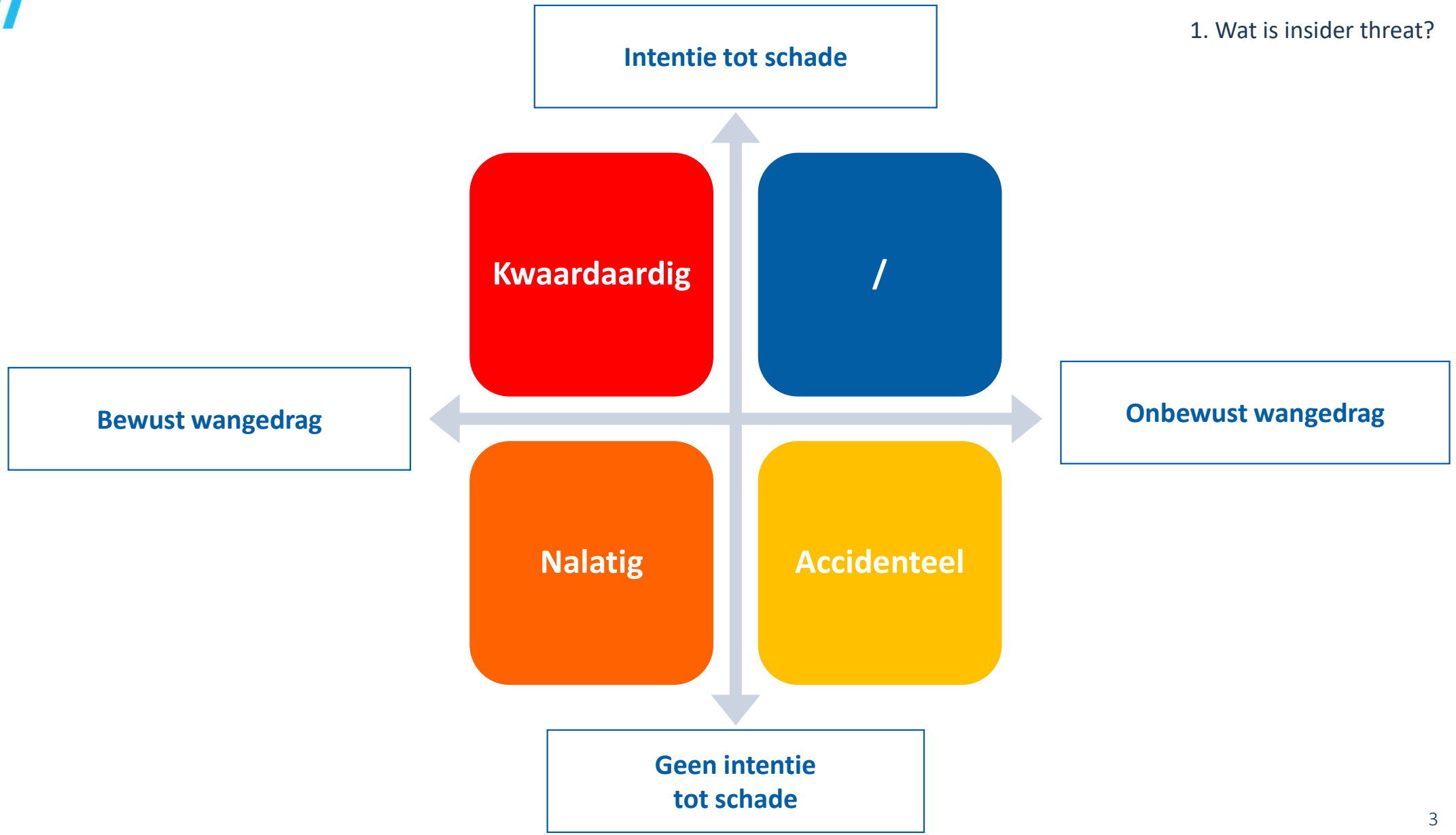
Insider threat

Security Convention 2024

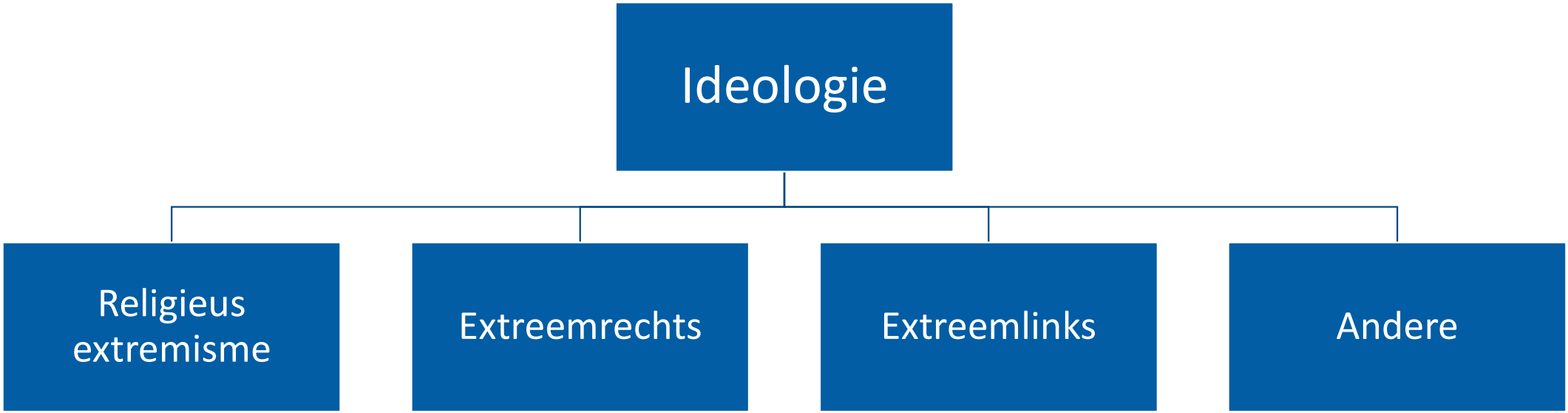
Dr. Mathias Reveraert – Security Adviseur Infrabel

24/10/2024

1. Wat is Insider Threat?


Intentie tot schade
Kwaardaardig
/
Bewust wangedrag
Onbewust wangedrag
Nalatig
Accidenteel
Geen intentie
tot schade

Radicalisering als potentiële motivatiefactor



Maar insider threat is meer dan radicalisering!

Ideologie	Ontevredenheid met de organisatie	Persoonlijke problemen	Hebzucht	Dwang
Nalatigheid	Manipulatie (‘Social engineering’)	Morele bezwaren	Liefde/empathie	Persoonlijkheidsstoornis
Sensatiezucht	Ego	Opportuniteit	…	

Perceptie Belgische veiligheidsofficieren - Motivatiefactoren

Factors behind insider threats	% of respondents
Social engineering	44,76%
Revenge out of disgruntlement with the organization	43,81%
Negligence	37,46%
Greed	36,83%
Personal problems (like addictions)	35,56%
Coercion by external party	32,38%
Ideology or religion	20,63%
Personal relationship (love, empathy, …)	13,65%
Personality disorder (like narcissism or psychopathy)	13,02%
Concerns with organizational security practices	12,06%
Our organization is not concerned about insider threats	11,11%
Moral concerns with organizational activities	10,79%
Other	4,44%

Table 6.11: What are the main factors behind insider threats (multiple answers possible)? (N=315)

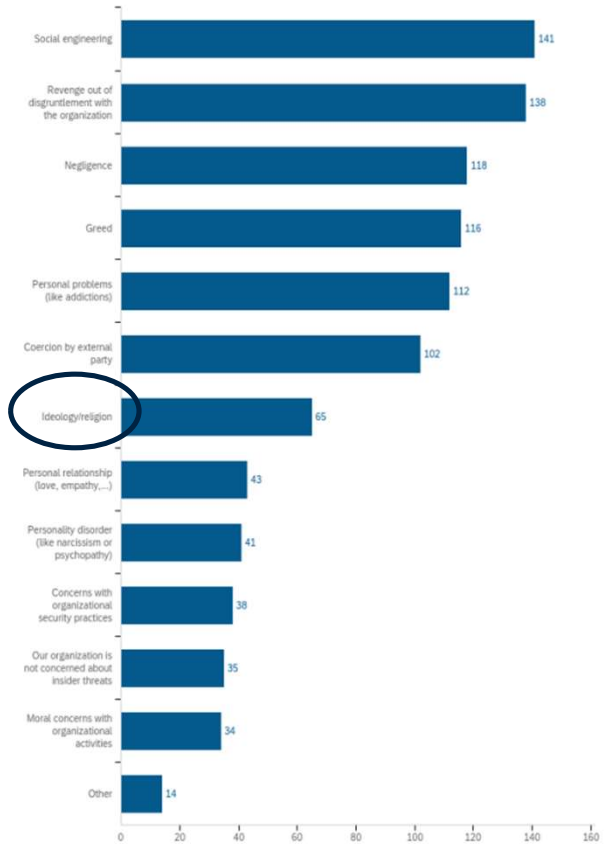


Figure 6.44: What are the main factors behind insider threats (multiple answers possible)?

2. Hoe wil Infrabel insider threat mitigeren?

Dreigingsanalyse

Domein	Vraag	Radicalisering/Extremisme/Terrorisme
Doel	**Wat** wil de insider bereiken?	• Schade toebrengen aan Infrabel is een doel op zich • Infrabel wordt gebruikt als middel om schade toe te brengen aan derde partijen (bv. treinreigers)
Betrokkenen	**Wie** is betrokken bij het incident?	• Slachtoffers = enkel Infrabel of ook derde partijen (treinreizigers/klanten/buurtbewoners/bedrijven in spooromgeving, …) • Begunstigden = insider(s) + eventueel derde partij(en) (bv. terreurorganisatie)
Motivatie	**Waarom** wil de insider de toegang tot onze waardevolle bezittingen misbruiken?	• Ideologie • Andere onderliggende oorzaken zoals ontevredenheid ten aanzien van Infrabel, persoonlijke problemen of sensatiezucht met ideologie als drogreden • Medewerker die onder dwang wordt gezet door terroristen/extremisten om schade toe te brengen
Tijd	**Wanneer** wordt de insider onbetrouwbaar?	• Voor de tewerkstelling al onbetrouwbaar (= infiltratie) • Tijdens de tewerkstelling onbetrouwbaar geworden (= lone actor/rekrutering/'outreach')

Dreigingsanalyse (2)

Domein	**Vraag**	**Radicalisering/Extremisme/Terrorisme**
Modus operandi	**Hoe** kan de insider de toegang tot onze waardevolle bezittingen misbruiken?	• Geweld (bv. aanslag met explosieven/wapens of trein als wapen gebruiken) • Sabotage spoorweginfrastructuur/treinverkeer • Spionage/Diefstal gevoelige informatie (bv. militair transport) • …
Ernst	**Hoe groot** is de impact van het incident?	• Potentieel hoge directe schade (personeel/infrastructuur), zeker indien Nationaal Kritieke Infrastructuur (NKI) • Mogelijke indirecte schade (bv. reputatieschade)
Aantal	**Hoeveel** insiders zijn betrokken bij het incident?	• 1 insider alleen • 1 insider met hulp van buitenaf • Meerdere insiders zonder hulp van buitenaf • Meerdere insiders met hulp van buitenaf
Betrokkenheid	**In hoeverre** is de insider betrokken bij het incident?	• Actief (bv. medewerker voert zelf een sabotageactie uit) • Passief (bv. medewerker voorziet cruciale informatie aan externe handlanger die sabotage kan uitvoeren)

Maatregelen voor de tewerkstelling

Doel	Vereiste actie	Aandachtspunten
Vermijden dat onbetrouwbare medewerkers worden tewerkgesteld	‘Pre-employment screening’	Risicobenadering
	Veiligheidsadviezen Federale Politie	Training aanwervend personeel
		Ook bij interne mobiliteit

Maatregelen tijdens de tewerkstelling

Doel

Vermijden dat medewerkers onbetrouwbaar worden tijdens de tewerkstelling

Vereiste actie

- Socialisatie van (nieuwe) medewerkers
- Waakzaamheid ‘red flags’
- Onderzoeken en anticiperen van ‘red flags’

Aandachtspunten

- Security culture maar ook welzijn
- Valkuilen ‘red flags’
- Informatie-uitwisseling

Maatregelen na de tewerkstelling

Doel

Vermijden dat voormalige onbetrouwbare medewerkers nog een bedreiging kunnen vormen

Vereiste actie

- Recuperatie organisatiemiddelen
- Afsluiten virtuele/fysieke toegangen
- Exitgesprek

Aandachtspunten

- Sociaal netwerk van de oud-medewerker
- Open bronnen (bv. Sociale media)
- Extra aandacht gedwongen vertrek

3. Conclusie

Conclusie

- **Insider threat**
  - Er bestaat niet zoiets als ‘de’ insider threat, het is een verzameling van verschillende soorten bedreigingen waarvan radicalisering/extremisme/terrorisme er één van is.
- **Insider threat mitigation**
  - Aandacht nodig voor mitigatie van aanwerving tot ontslag (voor, tijdens én na tewerkstelling).
  - Geen ‘one-size-fits-all’ oplossing maar tailor-made.
  - Niet enkel preventie en detectie, ook reactie en herstel

Bedankt voor uw aandacht!