Festival CYBERSECURITY IN DE ZORG

Keep it Simple - weg met het risico-assessment!

20 juni 2023

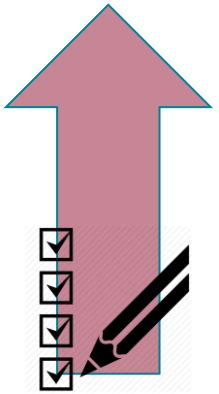
Werner Zuurbier – CIO Meander MC
Auteur van het boek “Cyber in the Board”

meander MEDISCH CENTRUM

IT & Cyber risico’s nemen toe

Dreigingsbeeld neemt toe

Digitale aanwezigheid neemt toe



Wet- en regelgeving neemt toe

Een paar voorbeelden van afgelopen maanden…

Paspoorten van dokters op straat na hack bij oudereninstelling Gelderland

Door Daniël Verlaan
7 maart 2023 12:42 • Aangepast 7 maart 2023 15:04

Ransomwaregroep publiceert naaktfoto's Amerikaanse borstkankerpatiënten

maandag 6 maart 2023, 17:29 door **Redactie**, 26 **reacties**

Een ransomwaregroep die vorige maand wist toe te slaan bij een Amerikaans ziekenhuis en daar allerlei gevoelige data buitmaakte is nu begonnen met het publiceren van naaktfoto's van Amerikaanse borstkankerpatiënten. De aanval op het Lehigh Valley Health Network (LVHN) in Pennsylvania was het werk van de ALPHV-ransomware, ook bekend als BlackCat.

Groot Spaans ziekenhuis annuleert duizenden afspraken wegens ransomware

dinsdag 7 maart 2023, 11:07 door **Redactie**, 6 **reacties**

Een groot Spaans ziekenhuis heeft drieduizend afspraken, honderdvijftig operaties en vierhonderd bloedtests geannuleerd wegens een ransomware-aanval die **afgelopen zondag** plaatsvond. Daarnaast worden inkomende patiënten en ambulances naar andere ziekenhuizen doorverwezen en is personeel van het Hospital Clinic de Barcelona voor alle achthonderd patiënten teruggevallen op pen en papier.

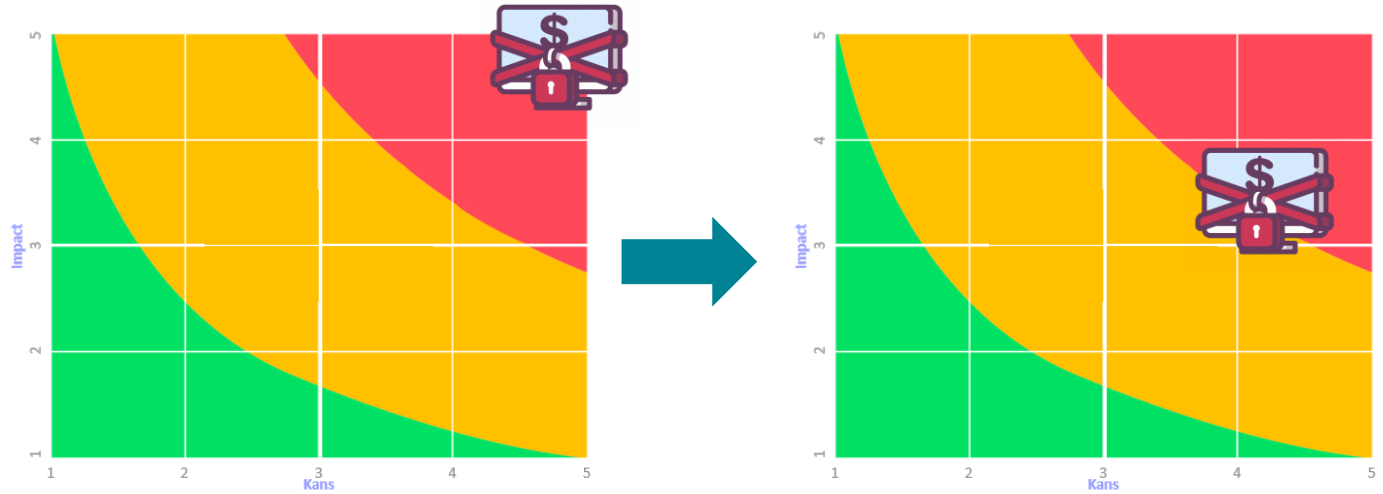
Keep it Simple

- Stop met het inventariseren van risico's en het doen van gewichtige risico-assessments
- Er zijn per saldo 28 unieke IT-risico's om te onderkennen (die zijn voor elke organisatie gelijk)
- Stop met de gangbare security frameworks
- Er zijn gewoon 32 typen IT-beheermaatregelen om de risico's af te dekken
- Stop met het verantwoorden van je security-activiteiten
- Toon enkel het werkelijke mitigerende effect op een risico van je activiteiten aan

Ransomware is nr. 1 cyber risico…

… en inmiddels hard op weg om nr. 1 business risico te worden

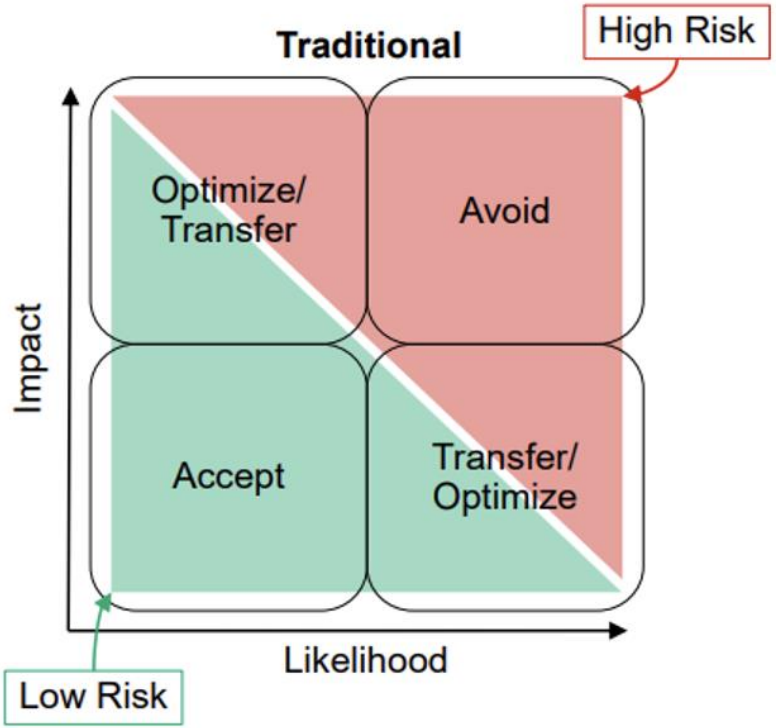
Security risico: hoe dan?

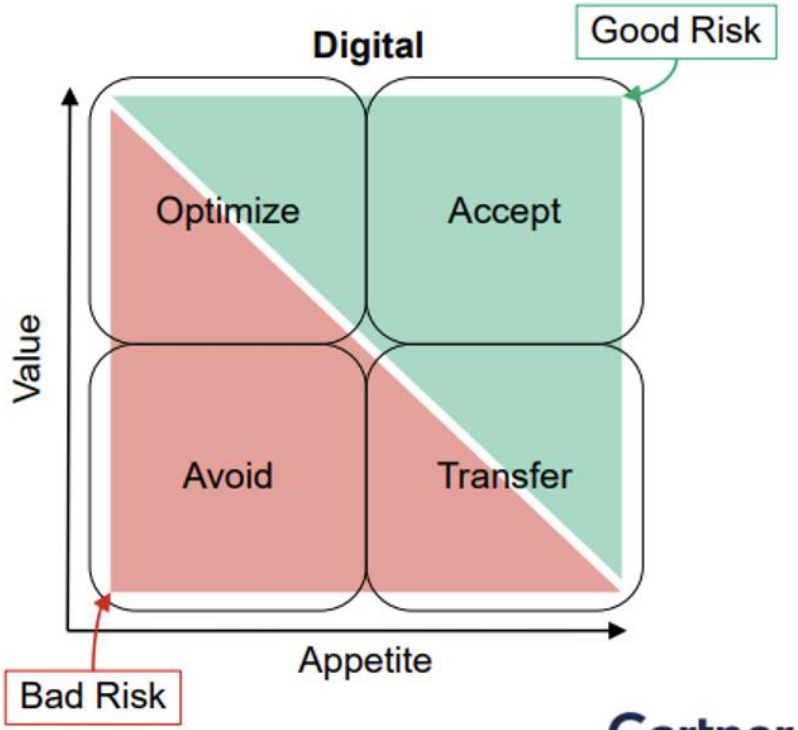


Inherent risico voor maatregelen

Restrisico na mitigerende maatregelen

Risico blijft hoog: helaas geen duidelijk richtsnoer voor prioritering of investering





Gartner

meander MEDISCH CENTRUM

Herken je dit?

- Het risico op een geldboete van de Autoriteit Persoonsgegevens
- Het risico op een cyberhack
- Het risico op een datalek
- Dit is een risico-gevolg
- Dit is een risico-oorzaak
- Dit is het daadwerkelijke risico

Risico-assessment heeft beperkte toegevoegde waarde

1. Risico's worden onzuiver op verschillende niveaus beschreven. Snel wordt niet het risico zelf maar een oorzaak of gevolg van dat risico benoemd.
2. Risico's worden vaak door het laatste nieuws of incident ingegeven.
3. Risico's worden veelal onterecht alleen geplot op de processen en systemen die *top-of-mind* zijn of in de *front-office* herkenbaar zijn.
4. Risico's worden door verschillende functionarissen vertaald naar hun eigen wereld. CFO (financiële impact), COO (bedrijfscontinuïteit), CEO (reputatieschade), CIO (beschikbaarheid, integriteit en vertrouwelijkheid van informatie), compliance-officer (juridische consequenties).

Risk Event Model: Er zijn slechts 28 unieke IT-risico's

	Availability	Integrity	Safety	Performance
Data	Incomplete or unavailable data	Inconsistent or invalid data	Leaked or misused data	No accurate or timely data
Systems	Non- or less functional system	Bad configured system	Compromised system	Bad performing system
Facilities	Insufficient or missing facilities	Unreliable facilities	Unsafe facilities	Unhealthy facilities
Processes	Poor outcome or delivery	Poor design	Poor command & control	Poor throughput
People	Shortage of people	Malicious insider	Unintended careless employee	Failing attitude, knowledge, skills
Third parties	Discontinuity of service	Unreliable service	Non-compliance of service	Poor quality of service
Strategy	Lack of vision	Wrong direction	Poor adoption	Poor execution

Accepteer de beperking van het bepalen van het dreigingsrisico…

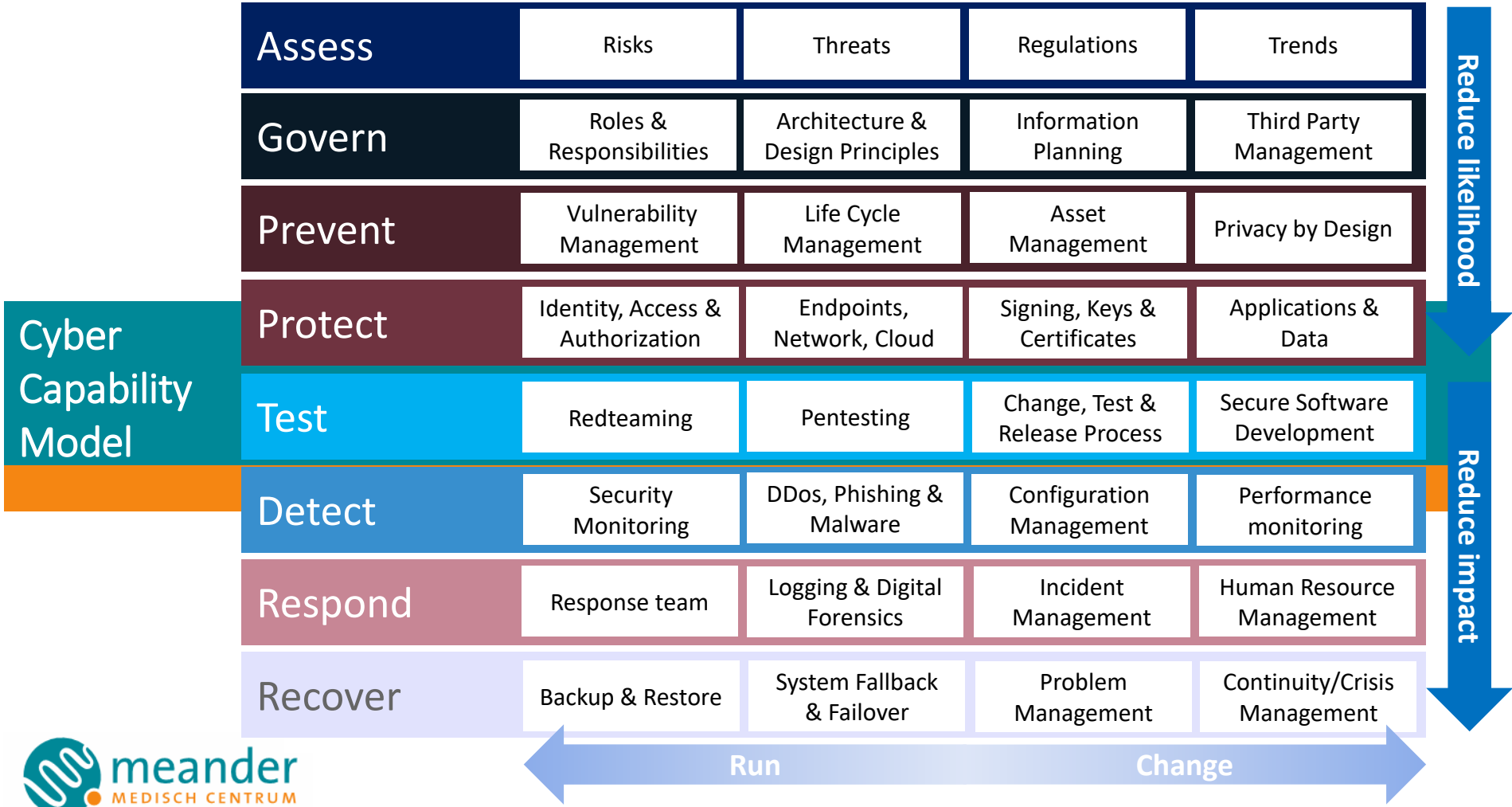
Meet daarom de effectiviteit van de juiste bekwaamheden voor de optimale weerbaarheid…

Security frameworks zijn te complex en te veel

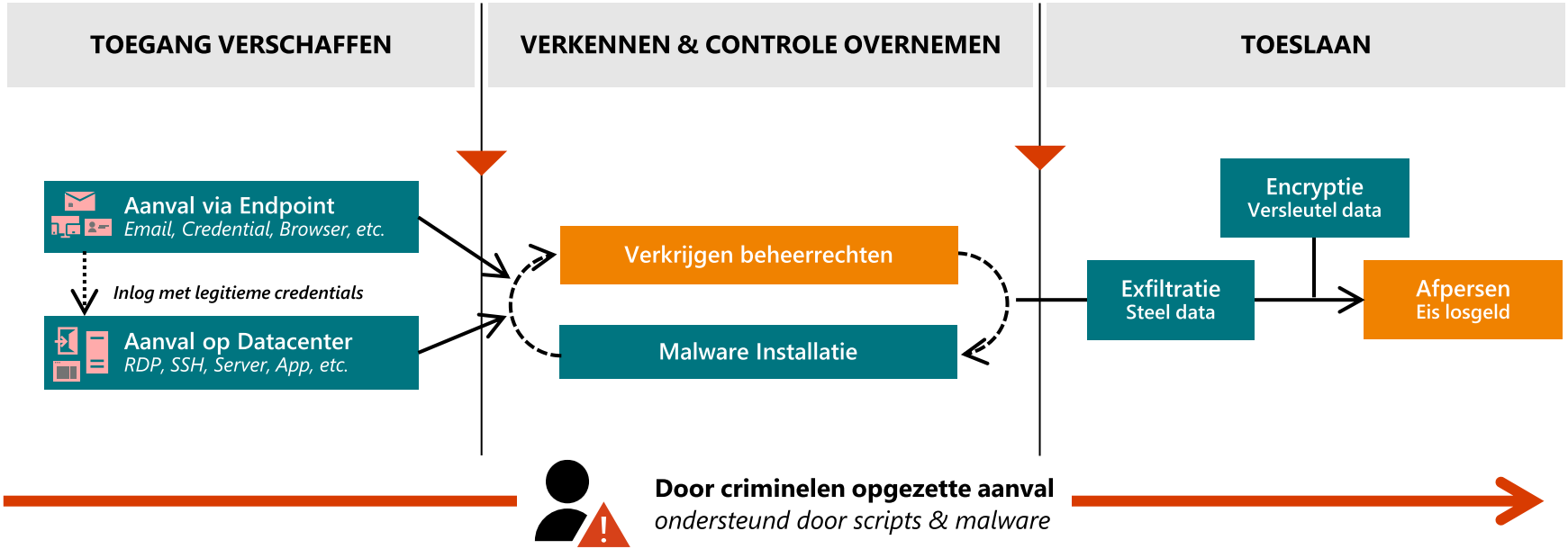
- ISO27001, NEN7510, NIST, BIO, COBIT, etc: zelfde wijn in andere zakken
- Blinken uit in complexiteit en technische details
- Zitten soms op procesniveau en dan weer harde technische maatregelen
- Vaak te voorschrijvend: niet alleen WAT je moet doen maar ook HOE

Wat verbindt ze? Bekwaamheden (Capabilities)

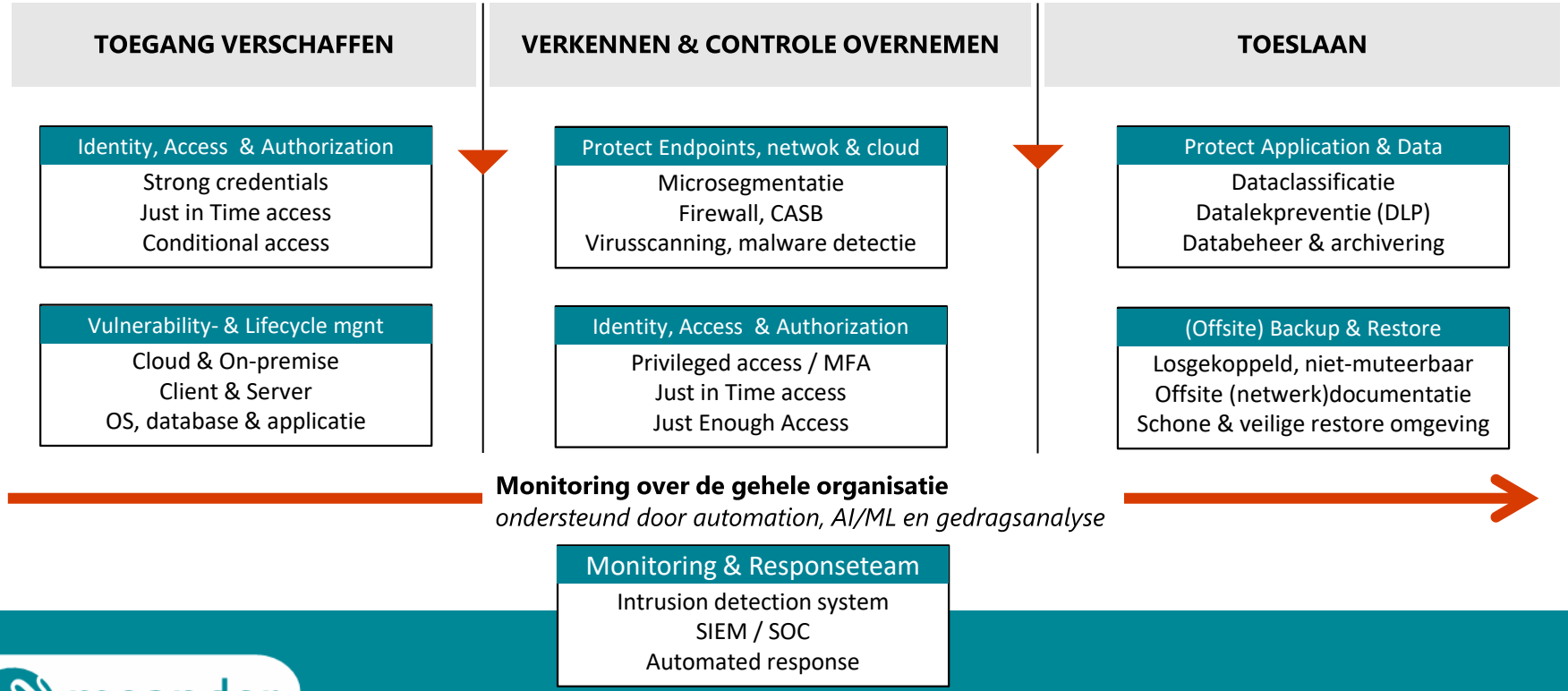
Het zijn er (slechts?) 32


Cyber Capability Model
Assess
Risks
Threats
Regulations
Trends
Govern
Roles & Responsibilities
Architecture & Design Principles
Information Planning
Third Party Management
Prevent
Vulnerability Management
Life Cycle Management
Asset Management
Privacy by Design
Protect
Identity, Access & Authorization
Endpoints, Network, Cloud
Signing, Keys & Certificates
Applications & Data
Test
Redteaming
Pentesting
Change, Test & Release Process
Secure Software Development
Detect
Security Monitoring
DDos, Phishing & Malware
Configuration Management
Performance monitoring
Respond
Response team
Logging & Digital Forensics
Incident Management
Human Resource Management
Recover
Backup & Restore
System Fallback & Failover
Problem Management
Continuity/Crisis Management
Reduce likelihood
Reduce impact
Run
Change
meander
MEDISCH CENTRUM

Hoe werkt Ransomware ?



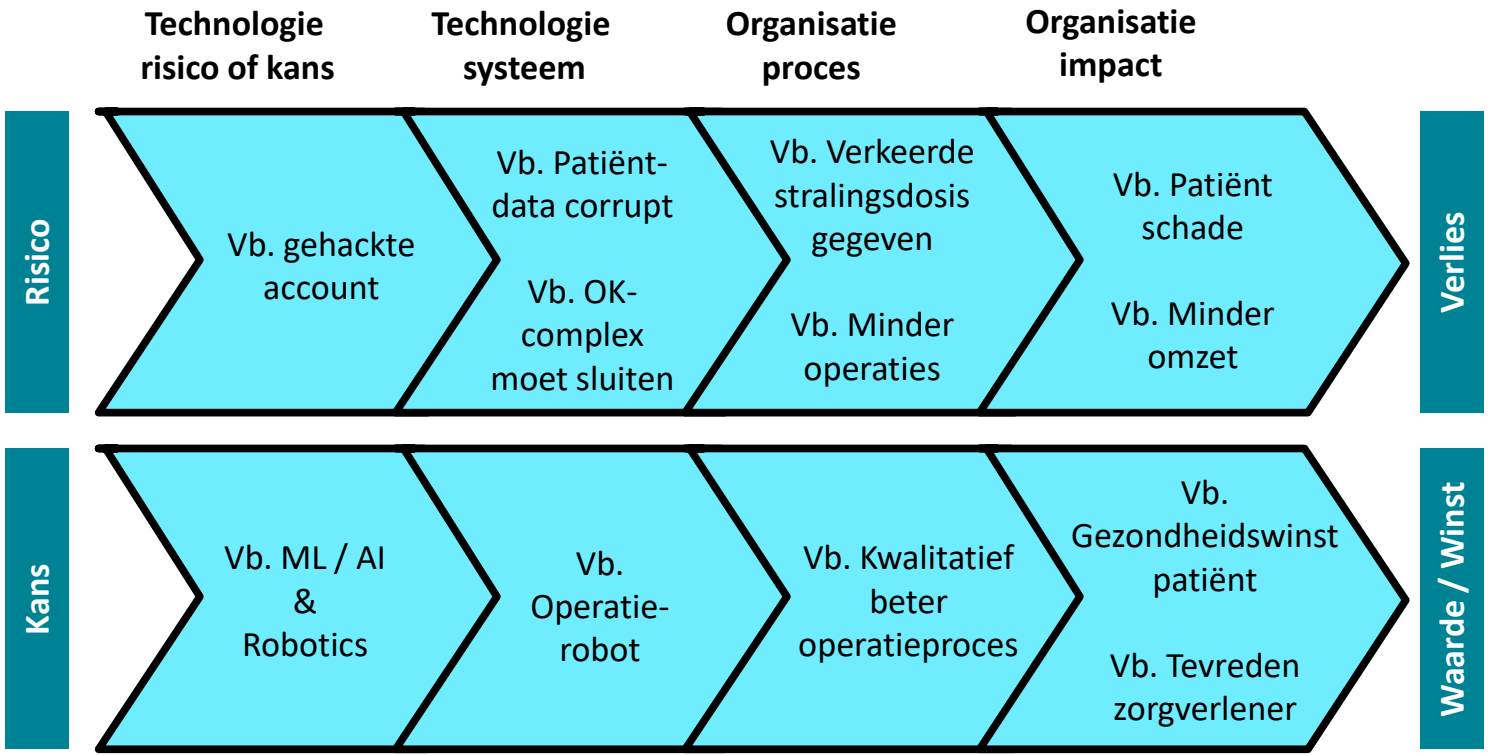
Hoe weer je je tegen Ransomware ?



Van beheersing van het proces naar effectieve risicomitigatie

Control is effectief	Risico is effectief gemitigeerd
We hebben awareness modules aangeboden aan alle medewerkers	Minimaal 80% van alle medewerkers hebben alle awareness modules doorlopen Minder dan 10% van alle medewerkers klikt op een phishing-link (nu is dat nog 18%)
We scannen periodiek op kwetsbaarheden in onze IT-omgeving	Alle hoog-kritieke kwetsbaarheden zijn binnen 5 werkdagen gepatcht
We draaien dagelijks back-ups voor onze kernsystemen	Alle backups zijn geslaagd en een restore kan plaatsvinden binnen 24 uur
We hebben continuïteitsplannen	Het crisisscenario “ransomware” is recent geoefend met het CMT en IT-partners. Leerervaringen zijn verwerkt in de crisisplannen
We laten ons periodiek ethical hacken	Ethical hack heeft geen hoog-risico zwakheden geconstateerd. Hacker is niet zonder hulp binnengedrongen in ons netwerk
We toetsen periodiek of medewerkers de juiste rechten hebben	Er zijn geen ex-medewerkers die nog beschikken over een actief account met rechten

Hoe voer je het juiste gesprek over IT en Cybersecurity met het bestuur?



meander MEDISCH CENTRUM

Contact:

Werner Zuurbier
+31 6 14279450
werner@zuurbier.nl
www.linkedin.com/in/zuurbier

Boek Cyber in the Board bestellen?
https://www.bravenewbooks.nl/wernerzuurbier

meander MEDISCH CENTRUM