H. HARTZIEKENHUIS MOL

SMR SYMPOSIUM MEDISCH RAMPENMANAGEMENT
26 oktober 2024

Cyber-attack: the day after (en veel langer…)

Ivo Jacobs
Managing Director, H.H. Hospital of Mol

H. HARTZIEKENHUIS
MOL

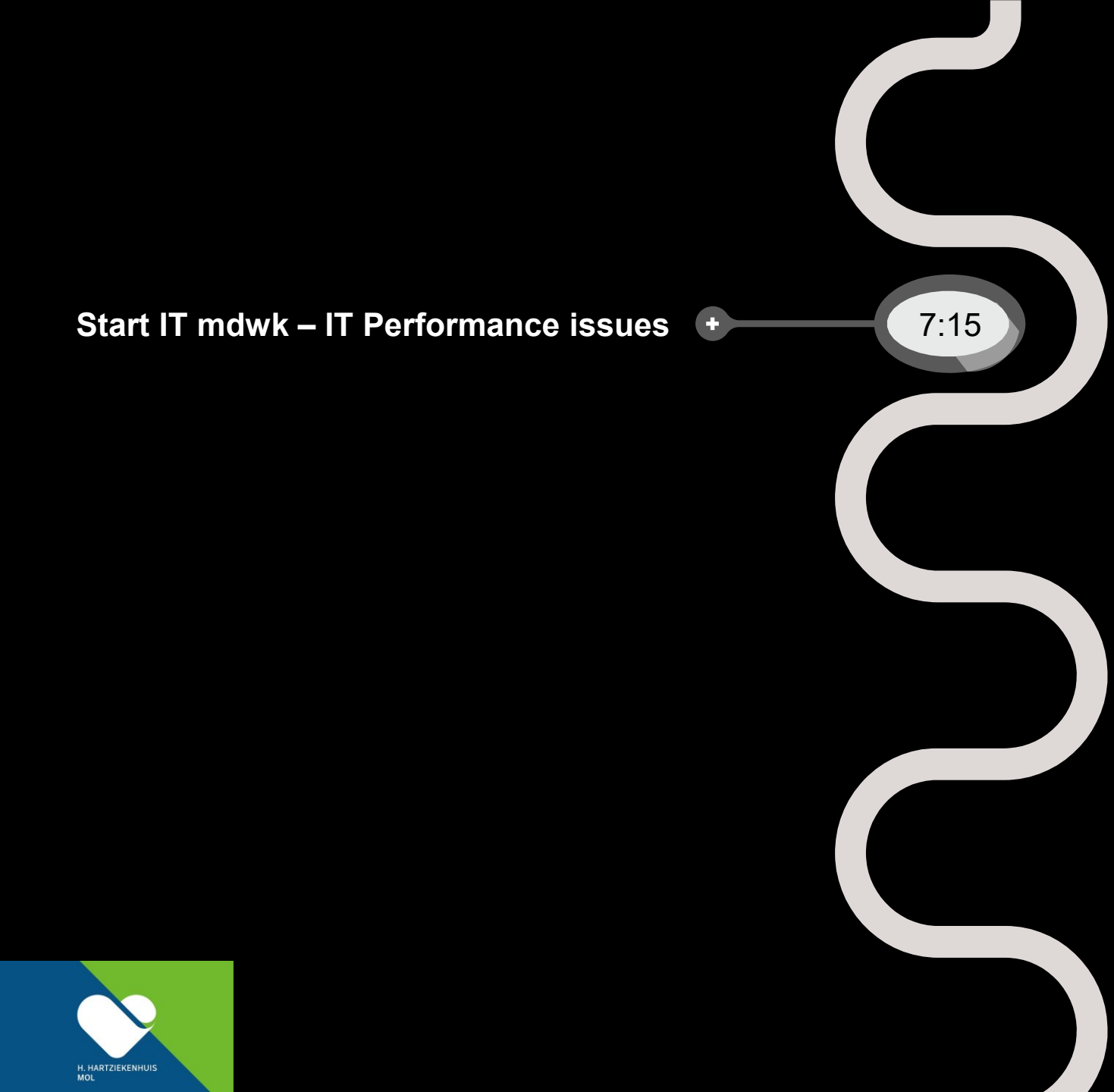
It en onze organisatie

- IT zou ons moeten ondersteunen, daar merk ik niet veel van.
- Ik wil snelle en onbeperkte toegang tot de systemen.
- Veel wisselen van wachtwoorden is ongemakkelijk.
- Ik weiger ‘2 factor authentificatie’ – het is pesterij.
- Waarom maken ze (IT) het mij zo moeilijk?
- Die ‘black screens’ binnen de 5’ moeten afgeschaft worden.
- ……

Once Upon a Time

H. HARTZIEKENHUIS
MOL

Start IT mdwk – IT Performance issues 7:15



H. HARTZIEKENHUIS
MOL

7:15

Start IT mdwk & performance issues

Performance issues

- Zabbix – management console – IT departement
  Performance indicator → vertraging van de systemen

- Ongewone activiteit van de DC (domain
  (scripts → account uitgeschakeld)

H. HARTZIEKENHUIS MOL

Dinsdag, 2 februari 2021

Start IT mdwk & performance issues — 7:15

8:00

- **Performance issues bevestigd**
- **Ransomware gevonden**

H. HARTZIEKENHUIS MOL

Dinsdag, 2 februari 2021

Start IT mdwk & performance issues — 7:15

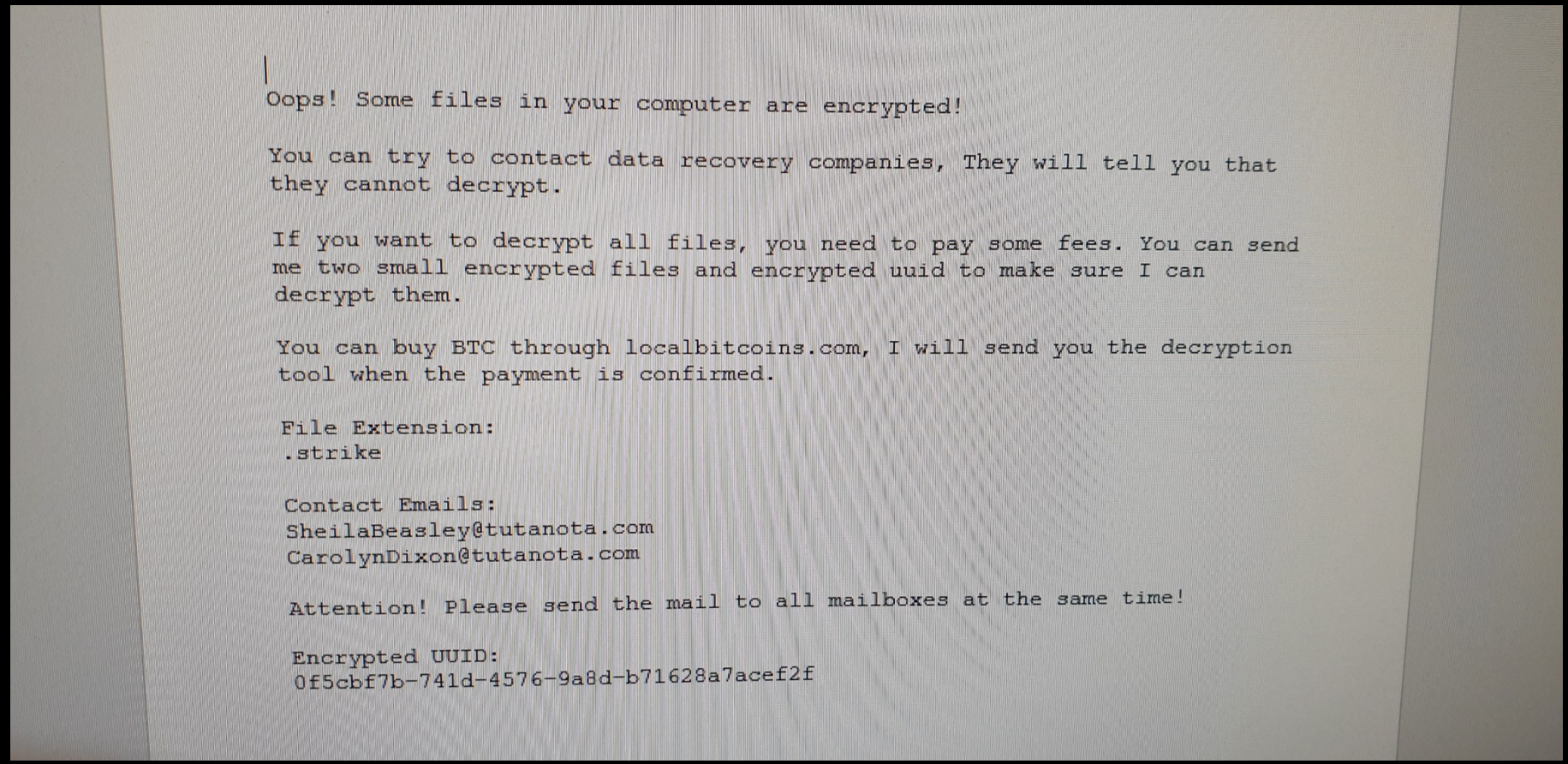
8:00

- **Performance issues bevestigd**
- **Ransomware gevonden**

H. HARTZIEKENHUIS MOL

8:00

Ransomware gevonden

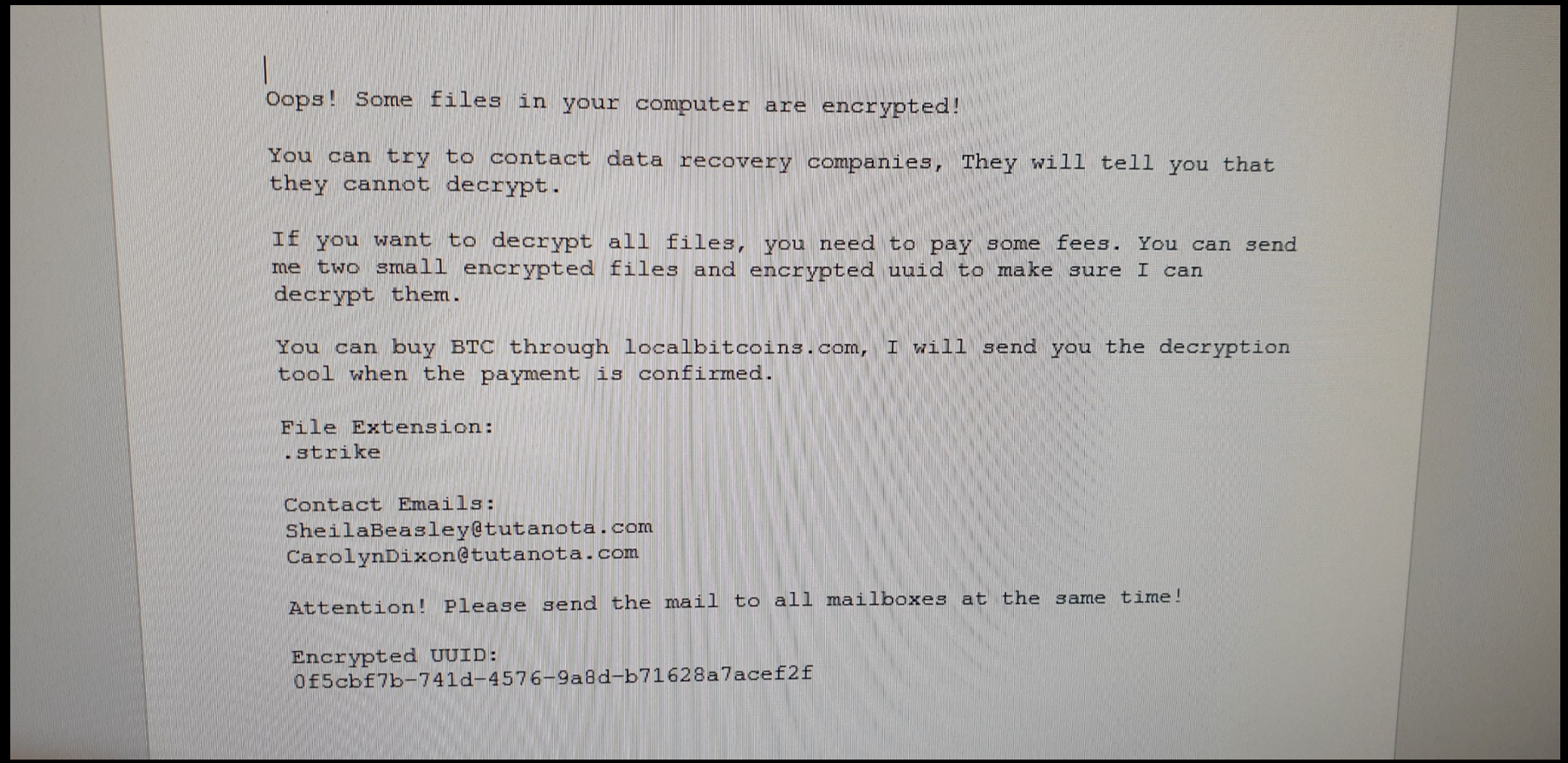


H. HARTZIEKENHUIS MOL

8:00

Ransomware gevonden

- EPD niet aangetast
- Stop internet, intranet, programma's, intern/extern email verkeer…
- Isolatie backup files



H. HARTZIEKENHUIS MOL

Dinsdag 2 februari 2021

Start IT mdwk & performance issues

7:15

8:00

Performance issues bevestigd

Ransomware gevonden

Crisis cell (management, vpken, artsen...): impact?

9:00

H. HARTZIEKENHUIS MOL

9:00

Crisis cell (management, verpleging, artsen, ...): impact?

- Activatie intern rampenplan (noodplannen – business continuity)
- Contact met verzekering (cyber insurance)
- Contact CERT – politie, overheid
- Intake & study environment → Installeren recovery plan→ Contact externe IT experts (verzekering).
  - Isolatie alle (mogelijk) geïnfecteerde systemen.
  - Complete IT shutdown

H. HARTZIEKENHUIS MOL

9:00

Crisis cel impact

Communicatie

- Intern: WhatsApp pyramide
  → noodmaatregelen voor aanwezige patiënten
  Cave: conflict IT veiligheid vs patient veiligheid
  Wie beslist?

- Extern → partners, overheid, ZNI (koepel).
  Via beveiligde internet connectie

Conflict

- IT afdeling: alles onmiddellijk stop zetten
- Artsen/verpleging: data over aanwezige patiënten toegankelijk houden (EPD)

→ Wie is ‘in the lead’?

H. HARTZIEKENHUIS MOL

Dinsdag 2 februari 2021

Start IT mdwk & performance issues

7:15

8:00

Performance issues bevestigd

Ransomware gevonden

Crisis cell (management, vpken, artsen, ...): impact?

9:00

16:00

Externe IT experts

Start recovery

H. HARTZIEKENHUIS MOL

16:00 **Externe IT experts**

Externe IT experts

- Objectieven
  - Definiëren ‘gecorrumpeerde systemen’ (50 van > 800)
  - Definiëren ransomware type
  - Definiëren backup and herstel opties
  - Definiëren en prioritiseren te herstellen systemen

→ IT crisis team: analyse van de technische problemen/oplossingen

H. HARTZIEKENHUIS MOL

16:00

Externe IT experts

- Operationele crisis cel → business continuity plan
  - Artsen, verpleging, administratie, receptie...
    - Planning, data verzameling, receptie, contacten, …

H. HARTZIEKENHUIS MOL

16:00

Externe IT experts

Start recovery

Start recovery plan (externe IT experts)

- Opdeling geïnfecteerde – niet geïnfecteerde systemen / Isolatie
- Re-installatie & cleaning: ‘Was straat’.
- Installeren complete antivirus software
  De-installeren antivirus ziekenhuis – nieuwe software
- Start installatie backup data

Contact met de aanvallers

H. HARTZIEKENHUIS MOL

De volgende dagen

Onderhandelen met de ‘aanvallers': IT experts + verzekering

- Ethische aspecten
- Schadekosten - recovery Wie beslist?
- Patiënt veiligheid in gevaar?

‘Business model’ cybercriminelen:

- Beloften?
- Veiligheidsissues?
- Data lekken?
- Geloofwaardigheid?

→ Eerlijke bedriegers

H. HARTZIEKENHUIS MOL

Hi,

It looks like you have encrypted our systems. We are a Belgium Hospital. Our patients are in serious danger. Can you provide us the decryption key please, so we can start recovering our environment?

Our UUID is: 0f5cbf7b-741d-4576-9a8d-b71628a7acef2f

H. HARTZIEKENHUIS
MOL

Hi,

It looks like you have encrypted our systems. We are a Belgium Hospital. Our patients are in serious danger. Can you provide us the decryption key please, so we can start recovering our environment?

Our UUID is: 0f5cbf7b-741d-4576-9a8d-b71628a7acef2f

Hello, if you want to decrypt all files, you need to pay BTC.

H. HARTZIEKENHUIS
MOL

Hi,

It looks like you have encrypted our systems. We are a Belgium Hospital. Our patients are in serious danger. Can you provide us the decryption key please, so we can start recovering our environment?

Our UUID is: 0f5cbf7b-741d-4576-9a8d-b71628a7acef2f

Hello, if you want to decrypt all files, you need to pay BTC.

Do you understand that you encrypted the network of a hospital? Lives of people could be at stake. I urge you to provide the decryptor for free and as soon as possible, so the impact is minimum.

H. HARTZIEKENHUIS
MOL

Hi,

It looks like you have encrypted our systems. We are a Belgium Hospital. Our patients are in serious danger. Can you provide us the decryption key please, so we can start recovering our environment?

Our UUID is: 0f5cbf7b-741d-4576-9a8d-b71628a7acef2f

Hello, if you want to decrypt all files, you need to pay BTC.

Do you understand that you encrypted the network of a hospital? Lives of people could be at stake. I urge you to provide the decryptor for free and as soon as possible, so the impact is minimum.

If you don't want to pay, please don't bother me.

H. HARTZIEKENHUIS
MOL

Hi,

It looks like you have encrypted our systems. We are a Belgium Hospital. Our patients are in serious danger. Can you provide us the decryption key please, so we can start recovering our environment?

Our UUID is: 0f5cbf7b-741d-4576-9a8d-b71628a7acef2f

Hello, if you want to decrypt all files, you need to pay BTC.

Do you understand that you encrypted the network of a hospital? Lives of people could be at stake. I urge you to provide the decryptor for free and as soon as possible, so the impact is minimum.

If you don't want to pay, please don't bother me.

Ok, let me discuss this with the board of the Hospital.

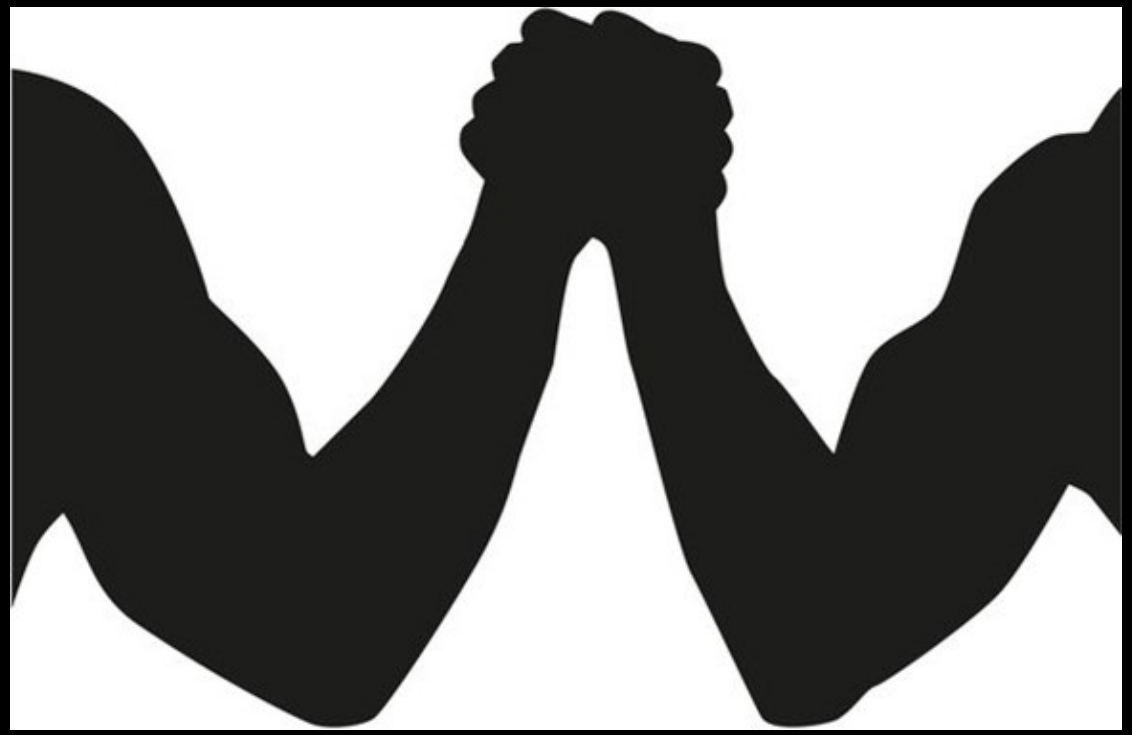
H. HARTZIEKENHUIS
MOL

Conclusie

- Het zijn beleefde jongens, die criminelen….
- Maar je kan er niet mee onderhandelen….

H. HARTZIEKENHUIS
MOL

Conclusie

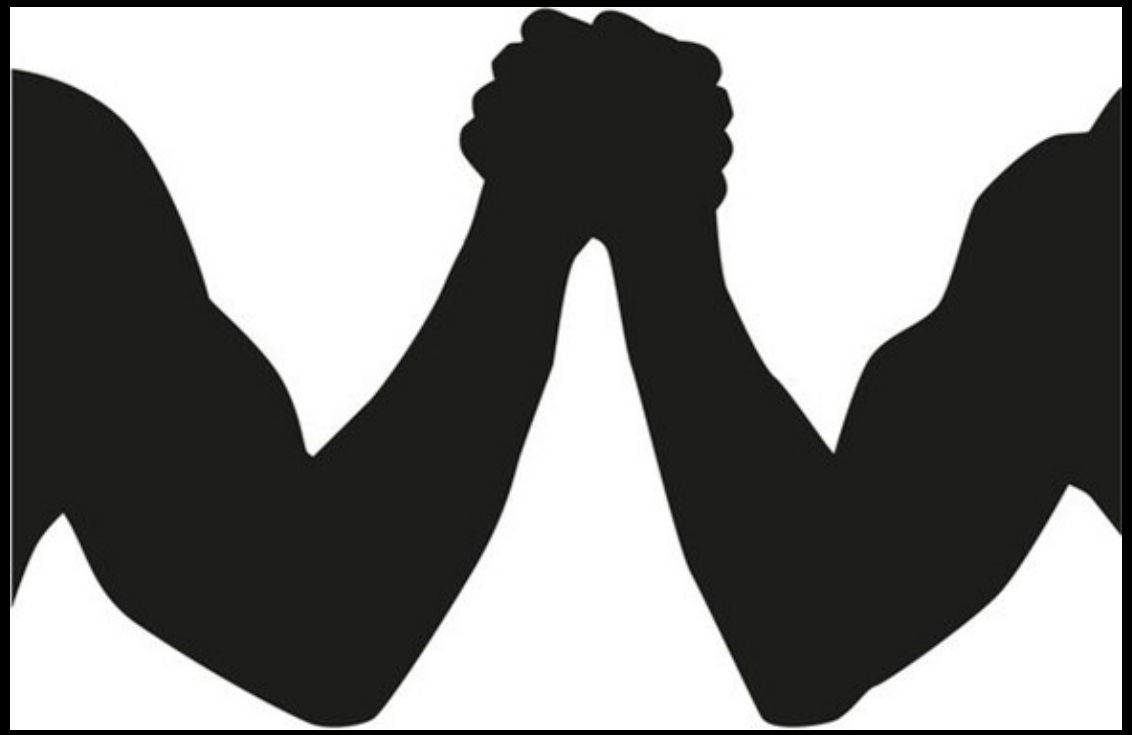


- Het zijn beleefde jongens, die criminelen….
- Maar je kan er niet mee onderhandelen….

TENZIJ….

H. HARTZIEKENHUIS
MOL

Conclusie



- Het zijn beleefde jongens, die criminelen….
- Maar je kan er niet mee onderhandelen….

TENZIJ….

→ De gevraagde ‘ransom’ daalt snel.

→ Desinteresse

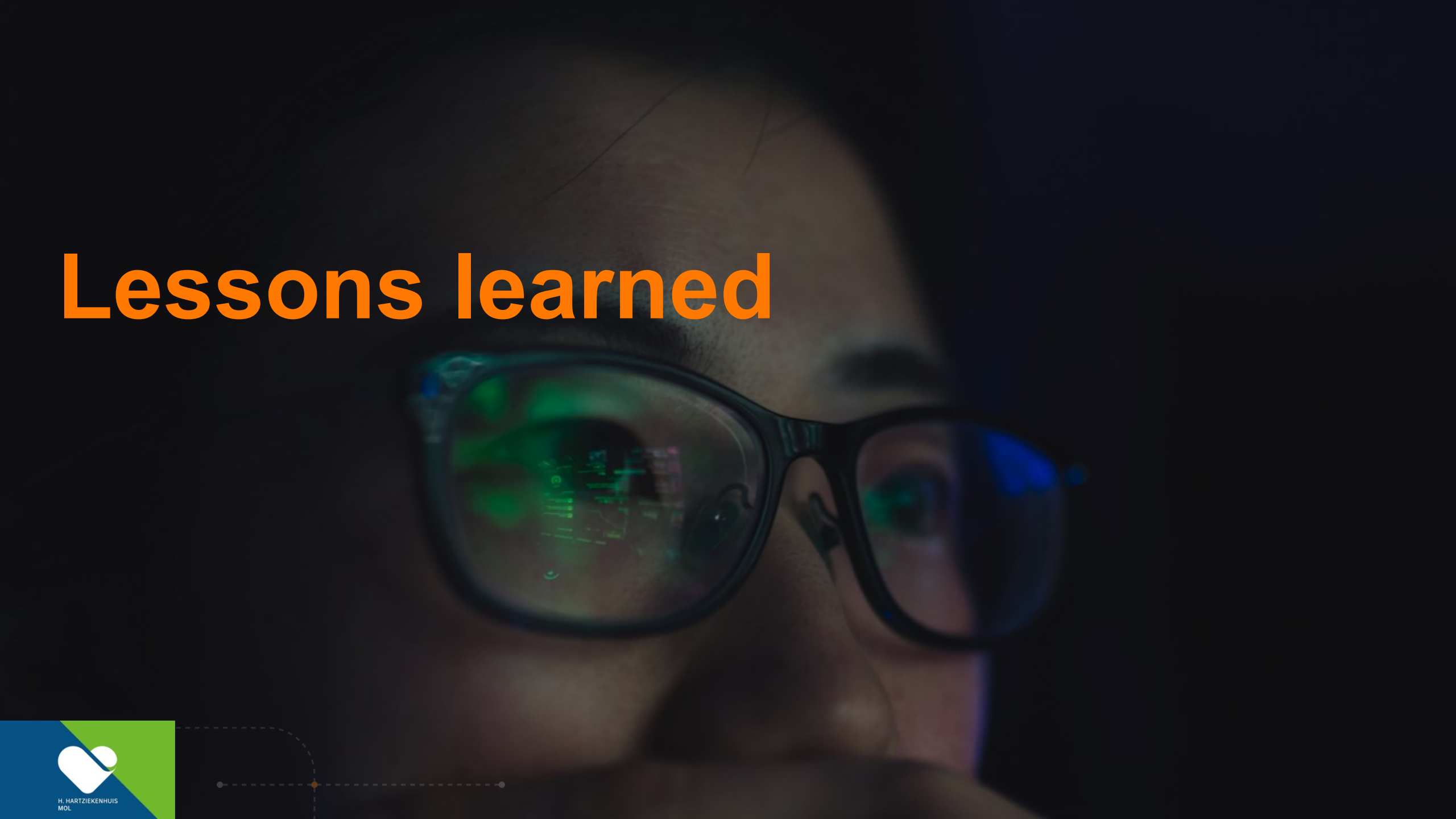
H. HARTZIEKENHUIS MOL

De volgende dagen

Root cause analysis.	Probleem: service account suppliers & remote support	Externe communicatie	Uitvoeren recovery plan (vervolg)
• Hacking website (Sharepoint) → toegang via een oud DC account (op systeem niveau)		• Wat is er ge-beurd? • Impact intern • Impact op patiënten? • Wat hebben we gedaan om snel herop te starten? • Timing van recovery?	• Reinstalleren van alle connecties • Nieuwe username and password ‘big bang’ (papier!)… • 2 Factor Authentication

H. HARTZIEKENHUIS MOL

Lessons learned



H. HARTZIEKENHUIS
MOL

Lessons learned

Organisatie

- Information Security Management System (PDCA cyclus) ISO27001 of NEN7510
- Investeer in IT-team (training in cybersecurity en recovery)
- Fysieke veiligheid (access control)
- Business Continuity Plan
- Procedure Cyber Verzekering – wees klaar voor het ‘CERT’ (network description)

Policy

- Policy (clean-desk, accurate passwoord policy, incident readiness, …)

Gedrag

- Awareness!

Technisch

H. HARTZIEKENHUIS MOL

Lessons learned

Technisch

- Nieuwe website
- Investeer in security monitoring, detectie and antwoord
- Office 365 migratie
- MFA (multi factor authentification)
- Uitzuiveren Active directory & remote support & service (SilverFort)
- Vulnerabilities en patches
- Netwerk segmentatie
- Netwerk toegangscontrole (802.1x)
- Backup & recovery (belang van off-line backup)
- Uitzuiveren IAM (bvb. Na ontslag!)
- Verbeter werkstation security (Anti virus next level - EDR solution)
- Forensic readiness (controle logs)
- Backup internet en telefoon lijnen
- (RDP – Citrix – Office macro’s - ….)

H. HARTZIEKENHUIS
MOL

Financiële schade…

Directe kosten

- IT Experts – 450 €/u…
  5 dagen, 12 u/dag, 4 pers + remote… → Totale kost van 180K
- Eigen (human) resources (MDs, secretariaten, receptie...)
- Aanschaf nieuwe software/hardware

Indirecte kosten

- Onmiddellijke schade: stop medische activiteiten (bvb alle onderzoeken, operaties,…)
- Toekomstige schade: gemiste (nieuwe) afspraken
- Verlies van informatie (rekeningen, …?)
- Herstellen van gemiste informatie
- Reputatie schade
- Medische schade?
- Wat als vragen (data lekken, …)

→ Totale kost: 700 – 1.000 K.

H. HARTZIEKENHUIS MOL

We hebben nu geen verzekering meer …

- Onmiddellijke stopzetting huidige polis
- Eerst de exacte schade (claim) bepalen, vooraleer nieuwe ‘offerte’
- Geen andere maatschappijen meer bereid gevonden
- Strenge voorwaarden (offers you can’t refuse)…
- Externe supervisie – controle?

Outsource IT?

H. HARTZIEKENHUIS MOL

Actie plan

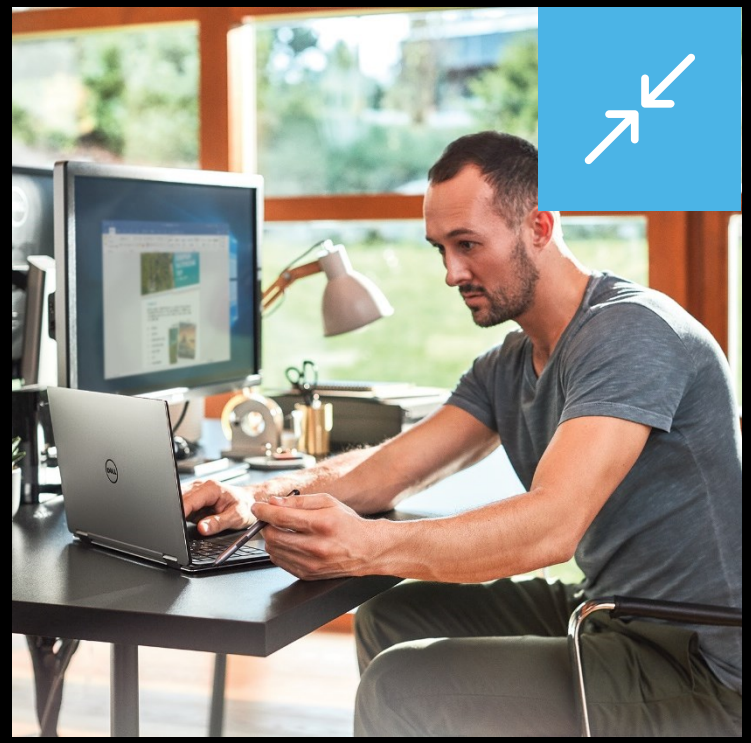
H. HARTZIEKENHUIS
MOL

Tijd voor een ‘Zero Trust’ benadering….

H. HARTZIEKENHUIS
MOL

Zero Trust: een nieuwe realiteit noopt tot nieuwe principes…

Verify explicitly



Use least privileged access

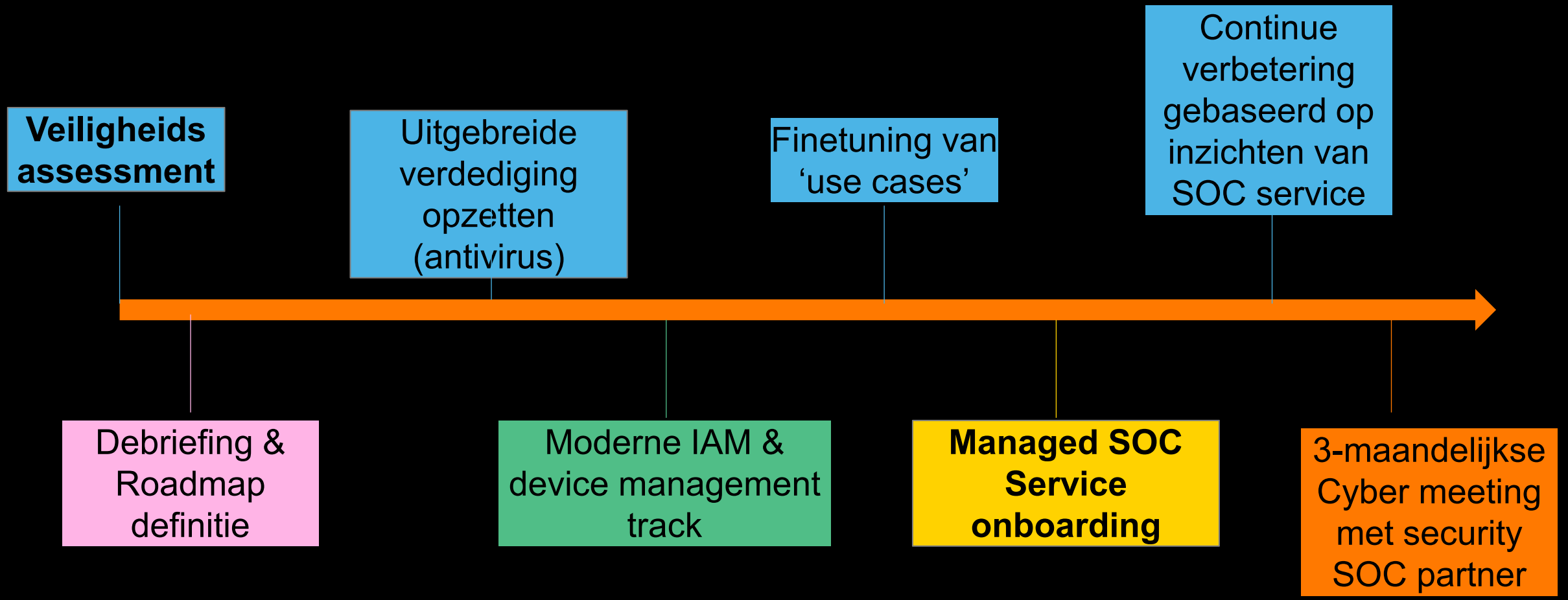
Assume breach

H. HARTZIEKENHUIS
MOL

Zero Trust set-up H.H. Mol

H. HARTZIEKENHUIS
MOL

Tijdslijn H.H. Mol



H. HARTZIEKENHUIS MOL

Waarom SOC as-a-service?

- **Ontlasten eigen diensten: cybersecurity follow-up is complex: gespecialiseerde kennis en & ‘resources’ zijn vereist**
- **Follow-up is nodig**

Proactief

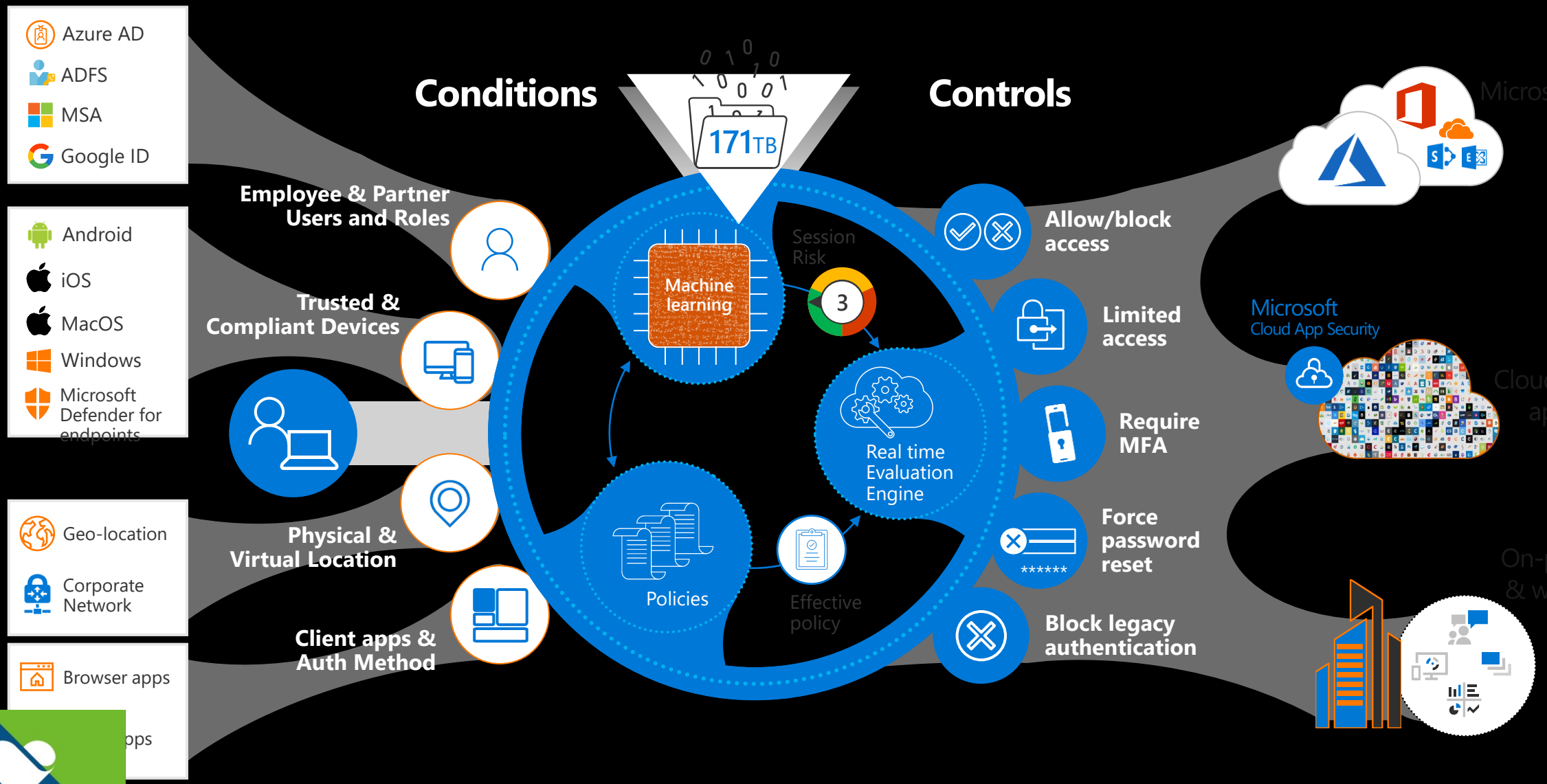
- Inzichten van SOC zijn de basis voor steeds evoluerende verbeteracties, door zowel technologische evolutie als door (toenemende kennis van) ‘secops’ (security operationals).
- Maandelijks SOC rapport + 3-maandelijkse meeting waarbij open kwetsbaarheden en aanbevelingen opgelijst en bediscussieerd worden.

Reactief
Incidenten worden niet altijd ‘automatisch’ opgelost door de technologie – manuele opvolging en interventie zijn (soms) nodig.
Wendbaardheid is belangrijk in cybersecurity.

- **SOC is (vaak) een voorwaarde voor (betaalbare) cybersecurity verzekering**

H. HARTZIEKENHUIS MOL

Azure AD Conditional Access + Identity Protection



H. HARTZIEKENHUIS MOL

Algemene conclusies

H. HARTZIEKENHUIS
MOL

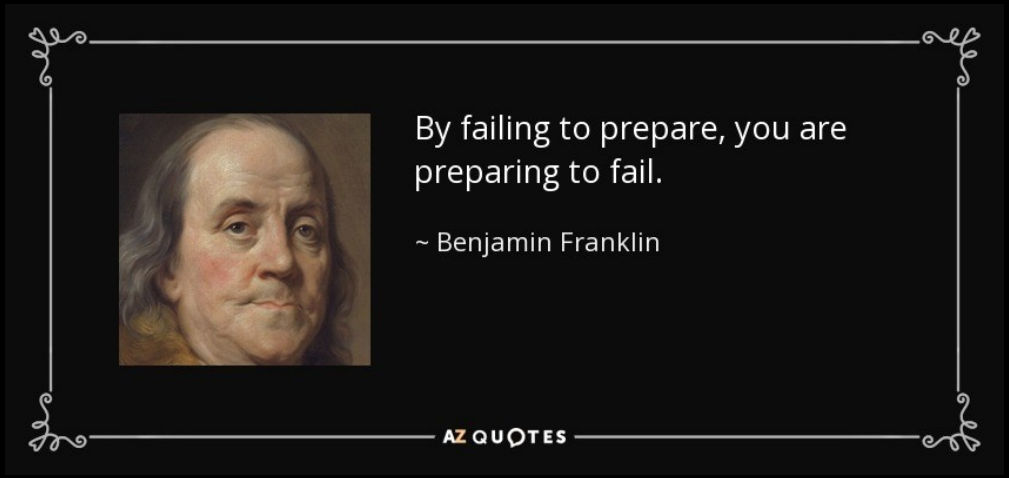
Algemene conclusies

H. HARTZIEKENHUIS
MOL

Algemene conclusies

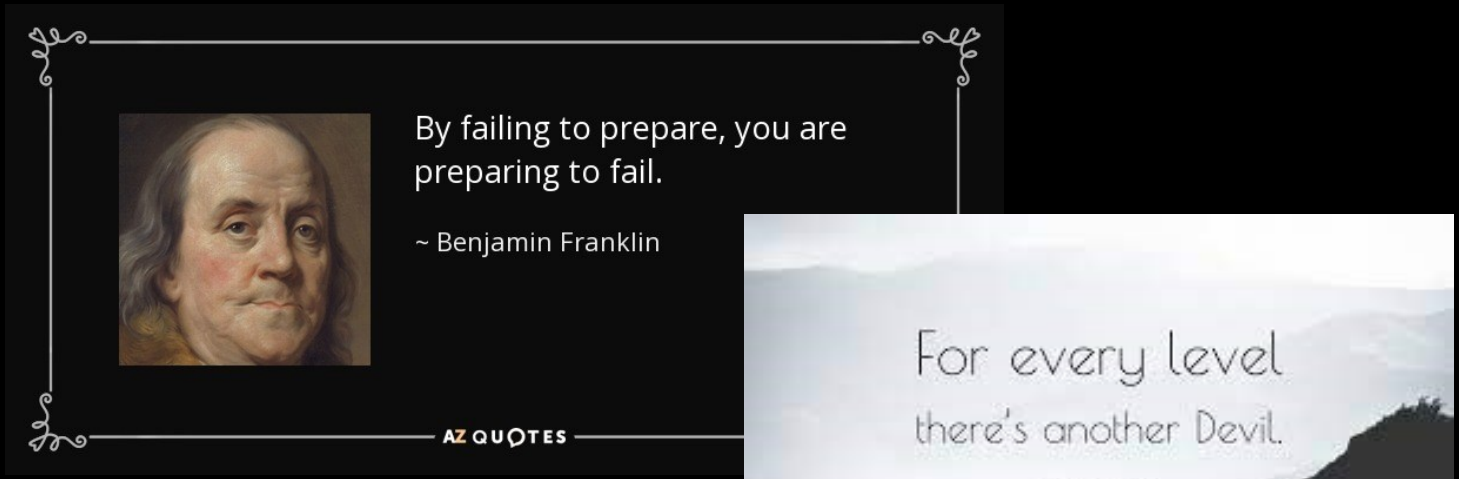
H. HARTZIEKENHUIS
MOL

Take home message



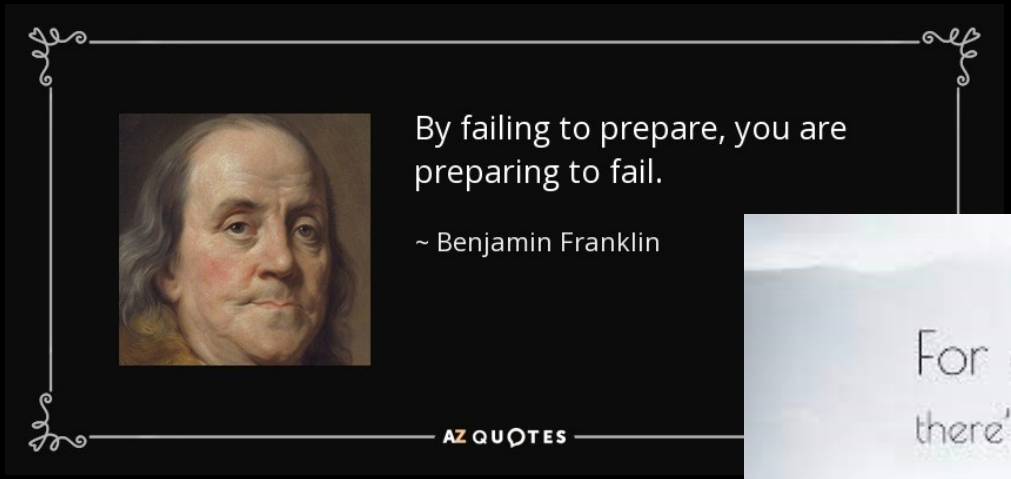
H. HARTZIEKENHUIS
MOL

Take home message

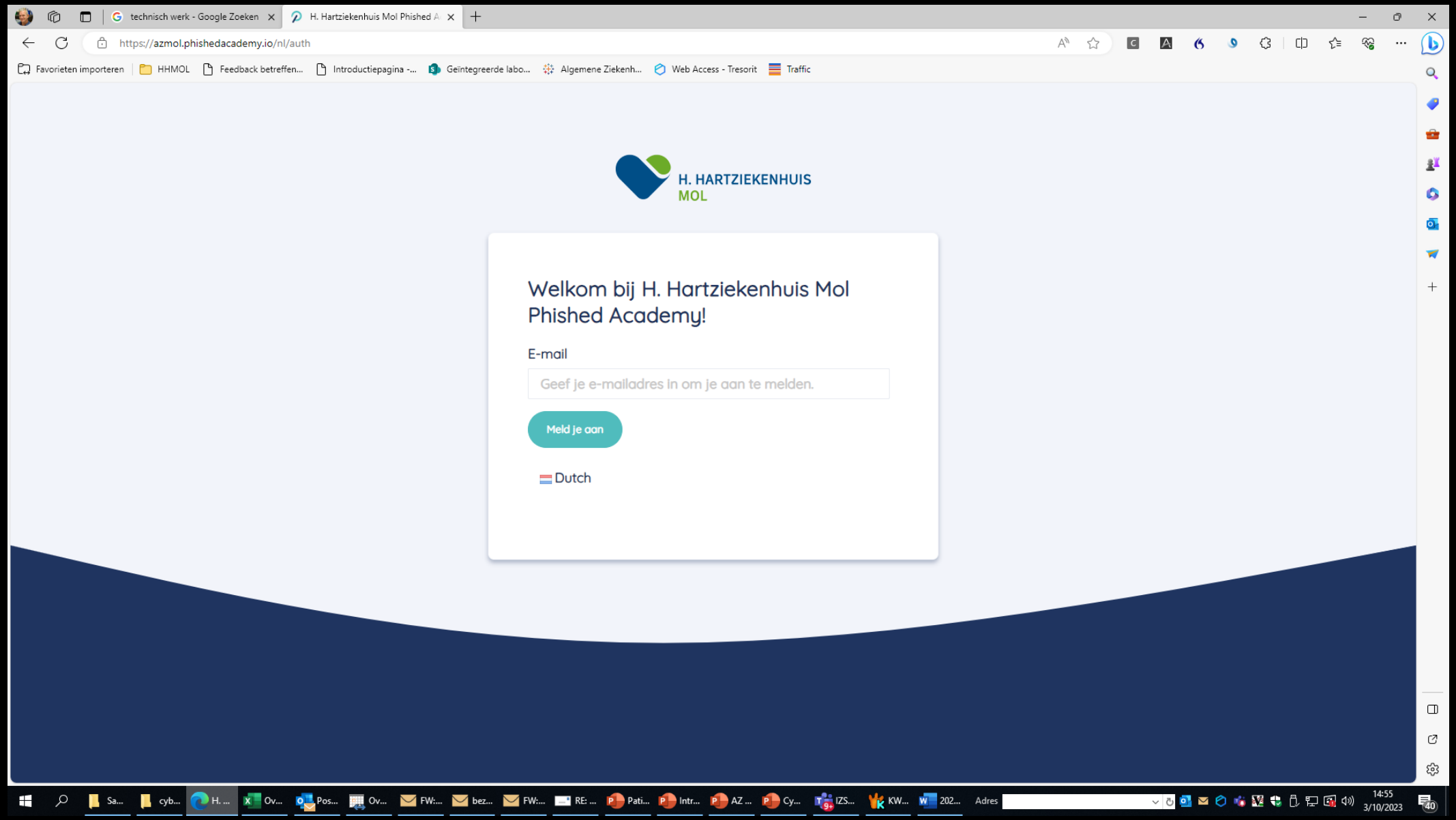


H. HARTZIEKENHUIS
MOL

Take home message

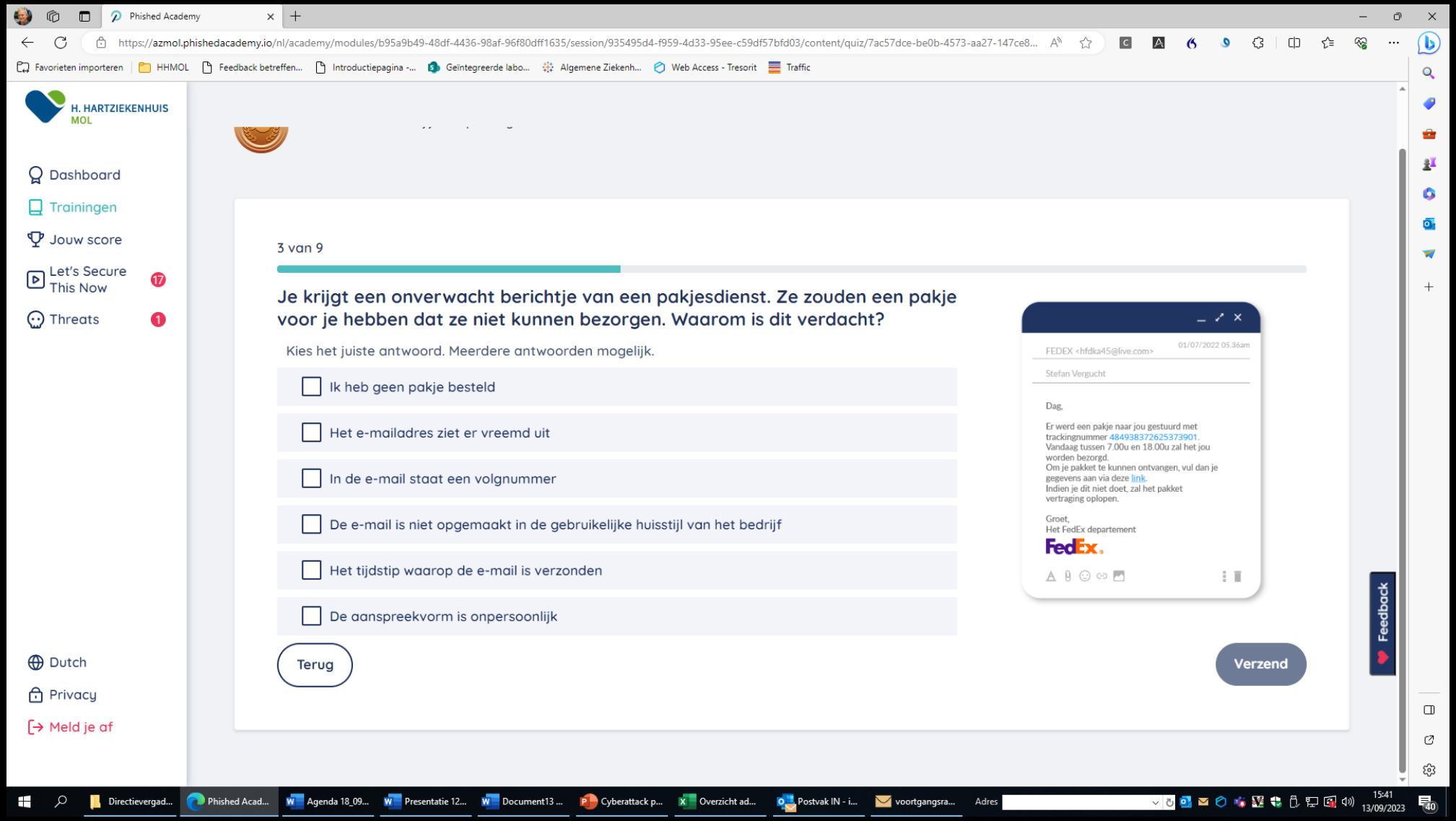


H. HARTZIEKENHUIS
MOL



H. HARTZIEKENHUIS
MOL

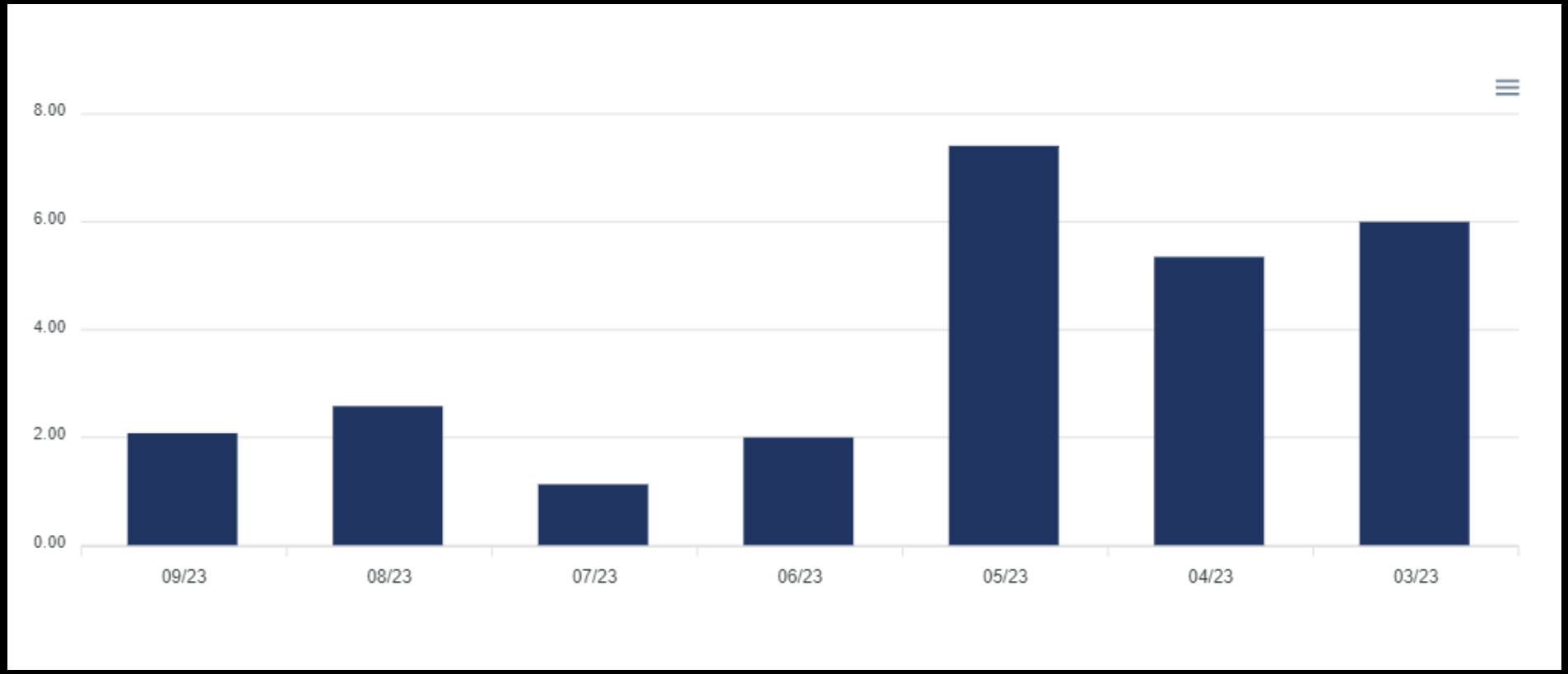
Awareness: opleidingen.



H. HARTZIEKENHUIS MOL

‘phished’….

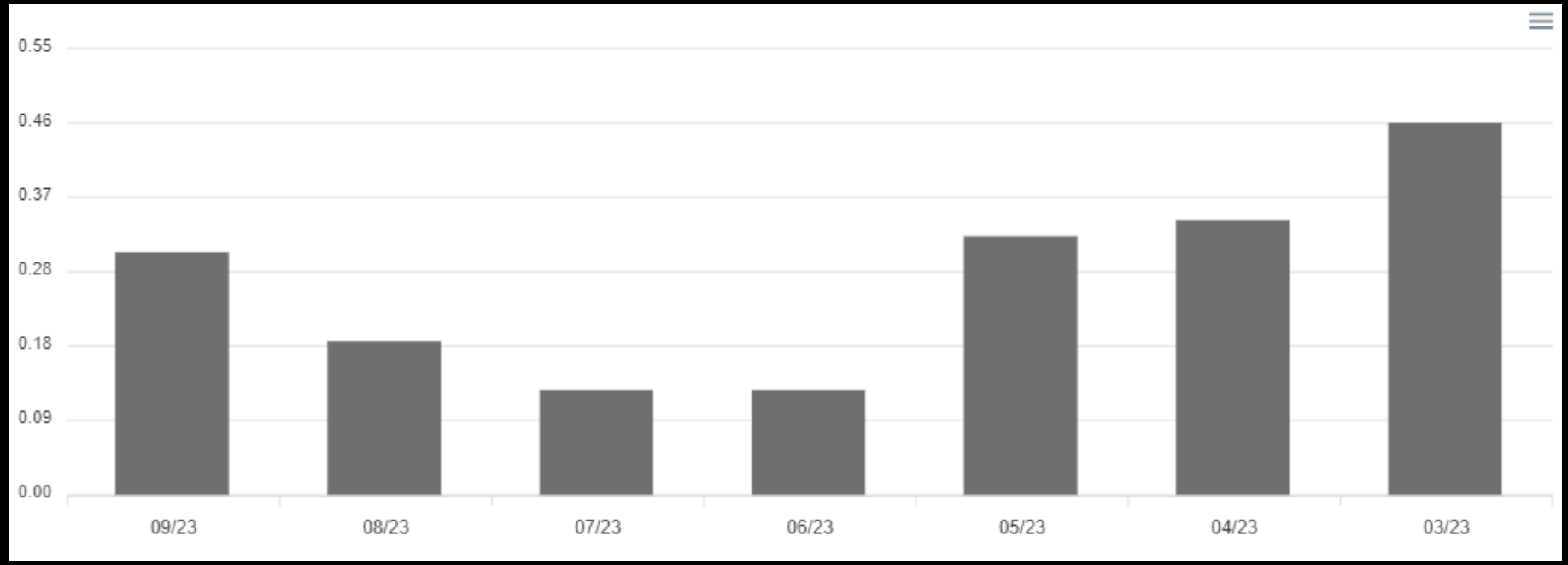
% personen die op link geklikt hebben.



H. HARTZIEKENHUIS
MOL

‘phished’….

% personen die bijlage geopend hebben.

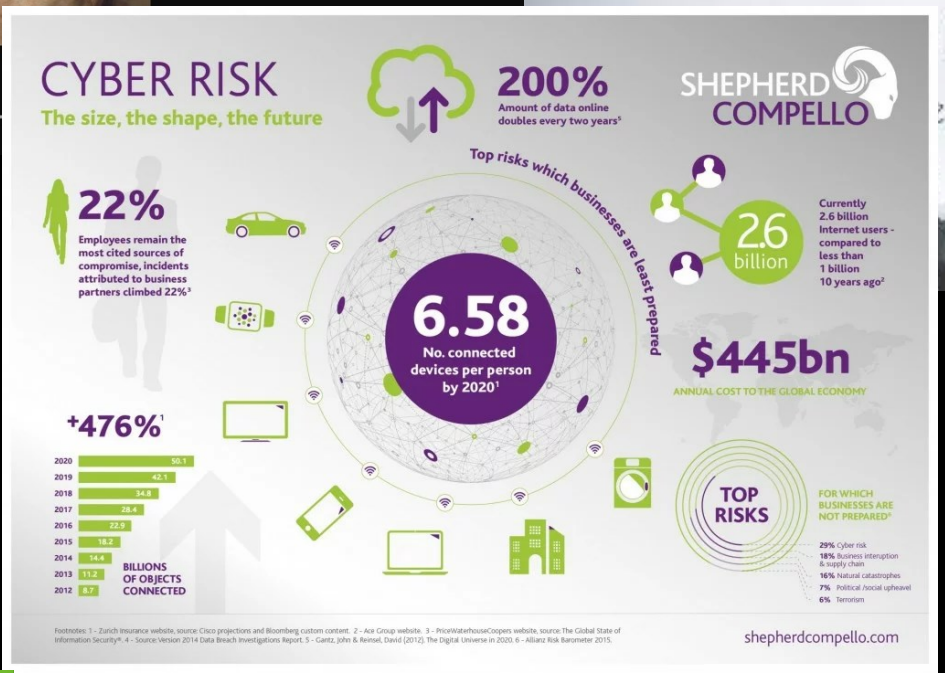


H. HARTZIEKENHUIS
MOL

Take home message

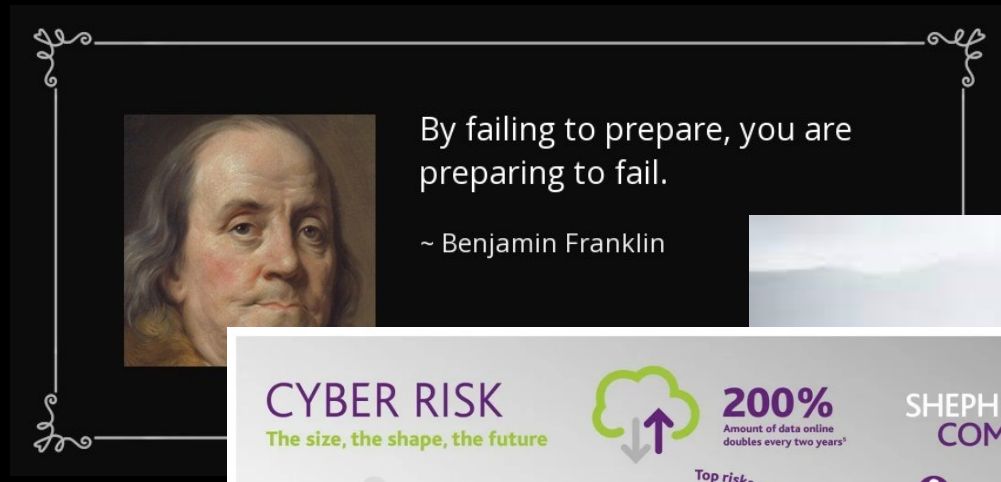
By failing to prepare, you are preparing to fail.

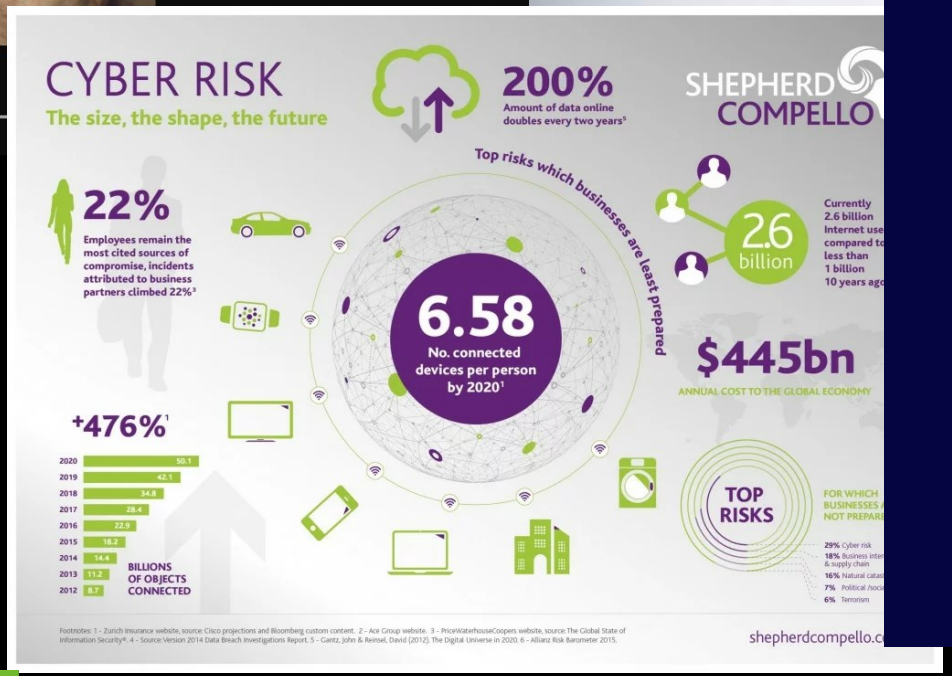
~ Benjamin Franklin

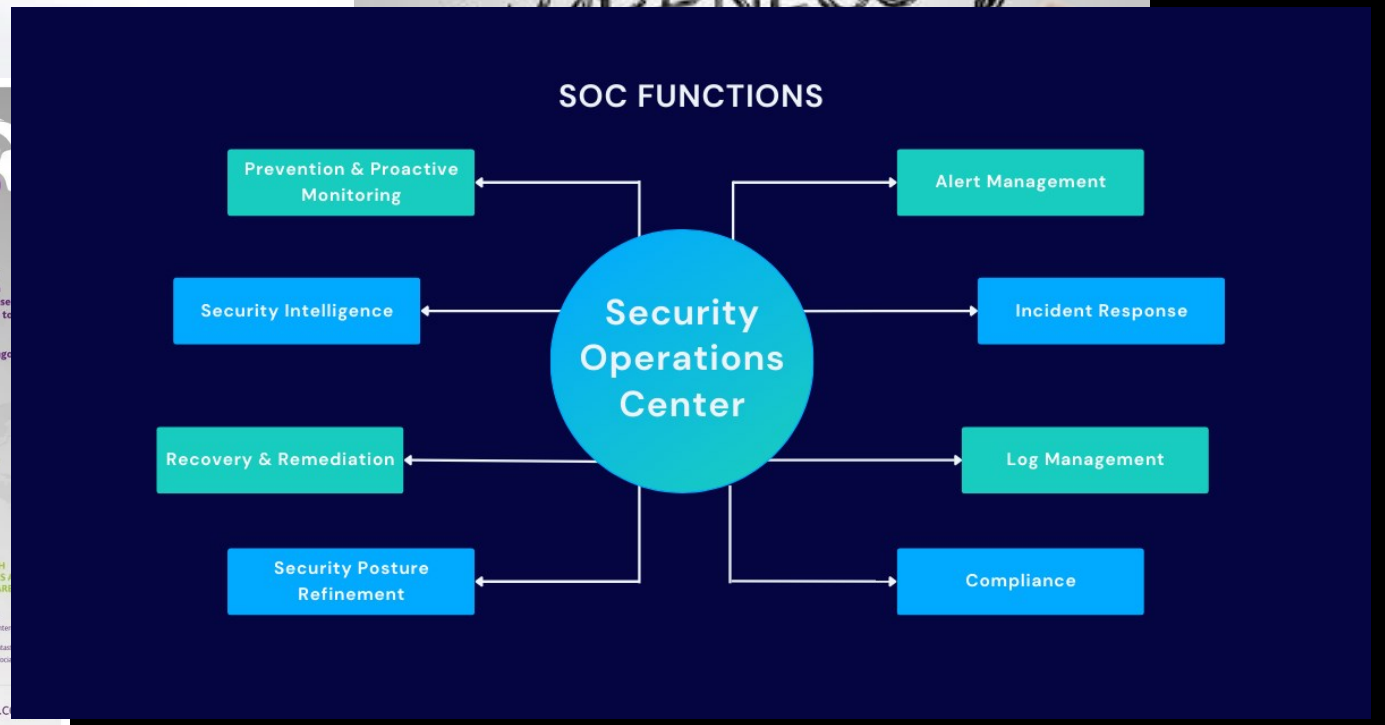


H. HARTZIEKENHUIS
MOL

Take home message







H. HARTZIEKENHUIS MOL

Dank voor uw aandacht!

H. HARTZIEKENHUIS
MOL

Q&A

H. HARTZIEKENHUIS
MOL