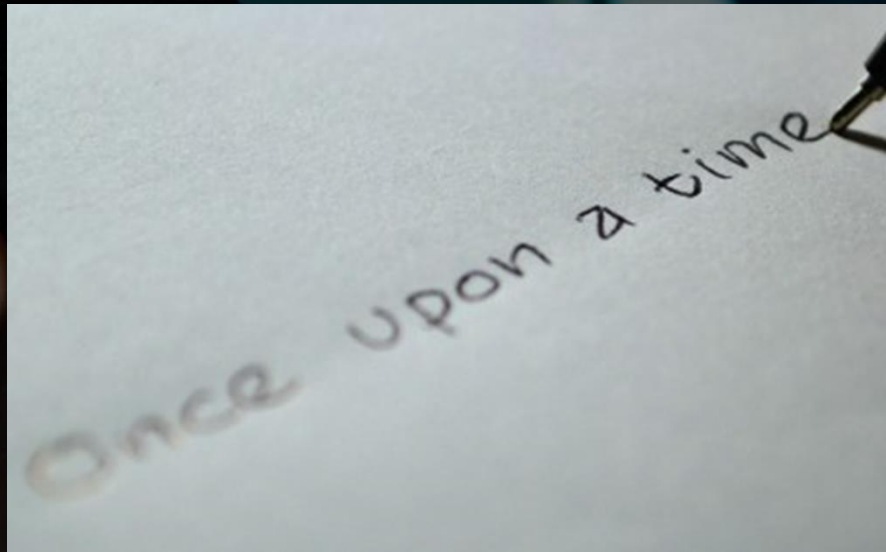
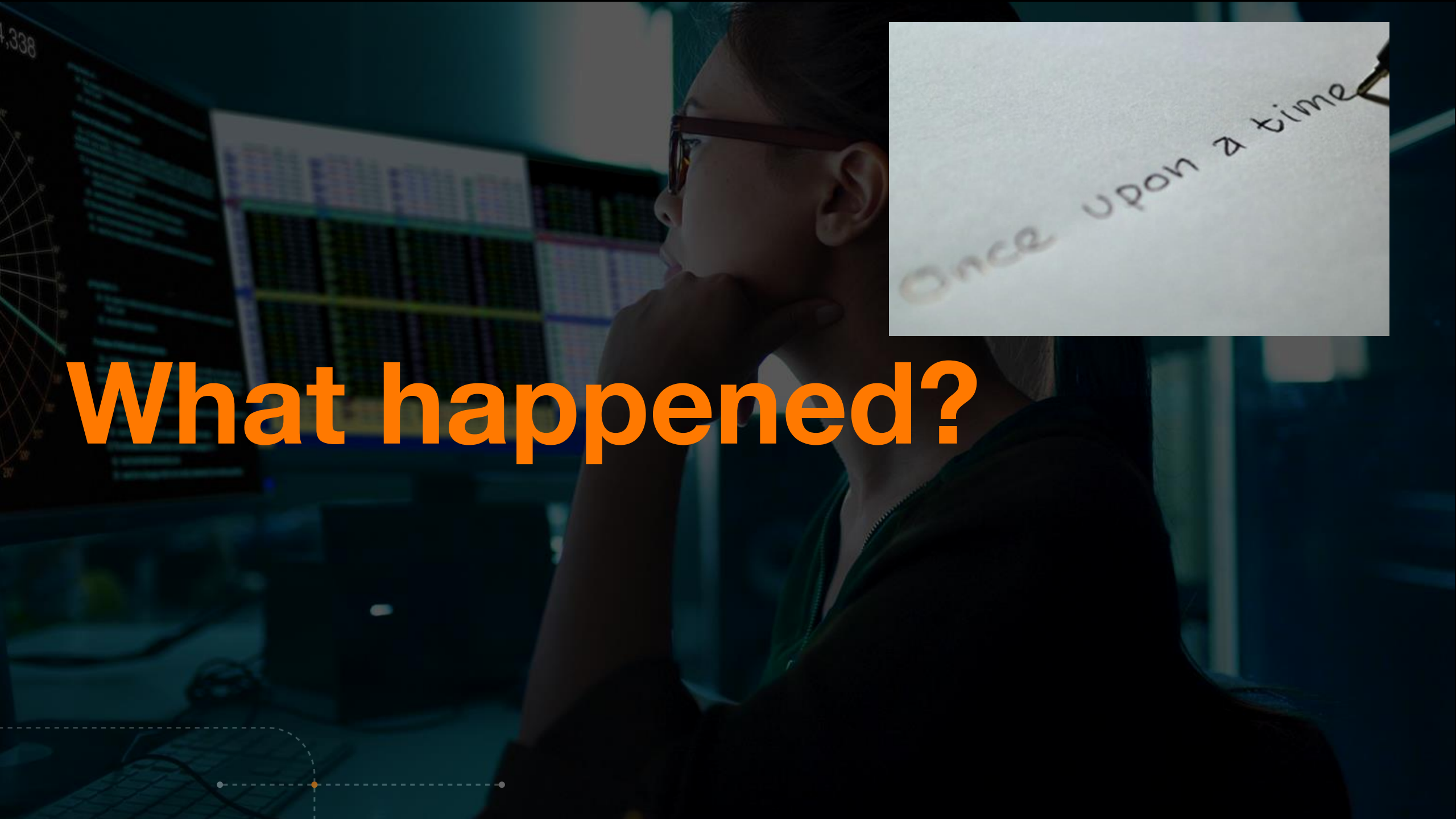


# Cyber-attack: the day after (and much longer)

**Ivo Jacobs**

Managing Director, H.H. Hospital of Mol





# What happened?

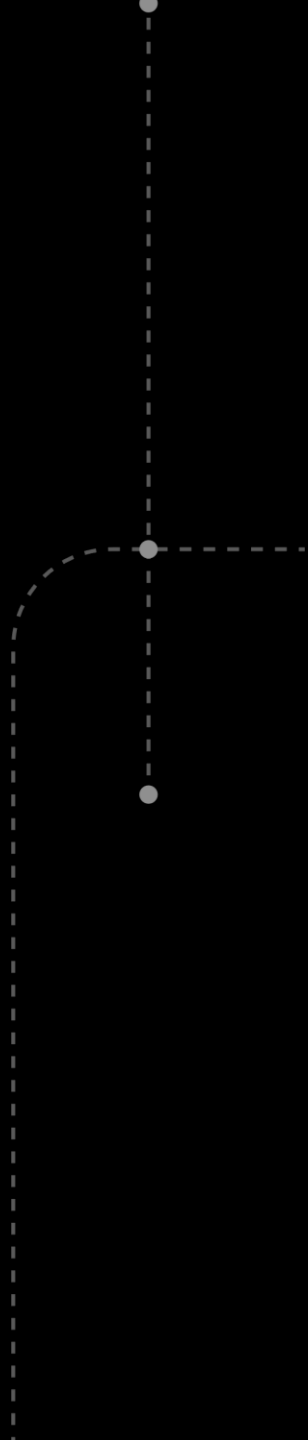
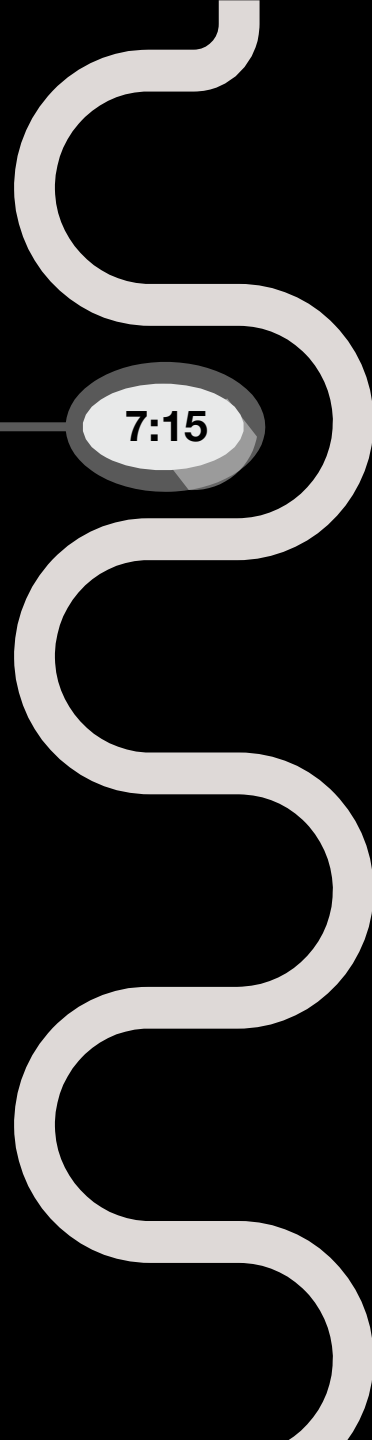


# Tuesday, February 2, 2021

Start IT employee & performance issues



7:15



7:15

+

## Start IT employee & performance issues

### Performance issues

- Zabbix – management console – IT department  
Performance indicator → slowdown of systems
- Unusual activity from DC (domain controller)  
(scripts → account disabled)



# Tuesday, February 2, 2021

Start IT employee & performance issues

7:15



8:00

Performance issues confirmed

Ransomware found

8:00



## Performance issues confirmed

- All activity halted
- Word message on some PCs

8:00



## Ransomware found

- EPD not corrupted
- Disabling internet, intranet, programs, internal/external email traffic...
- Isolate backup files

Oops! Some files in your computer are encrypted!

You can try to contact data recovery companies, They will tell you that they cannot decrypt.

If you want to decrypt all files, you need to pay some fees. You can send me two small encrypted files and encrypted uuid to make sure I can decrypt them.

You can buy BTC through localbitcoins.com, I will send you the decryption tool when the payment is confirmed.

File Extension:  
.strike

Contact Emails:  
SheilaBeasley@tutanota.com  
CarolynDixon@tutanota.com

Attention! Please send the mail to all mailboxes at the same time!

Encrypted UUID:  
0f5cbf7b-741d-4576-9a8d-b71628a7acef2f

# Tuesday, February 2, 2021

Start IT employee & performance issues

7:15

Performance issues confirmed

8:00

Ransomware found

Crisis cell (management, nurses,  
doctors...): impact?

9:00



9:00



## Crisis cell (management, nurses, doctors...): impact?

- Activate internal disaster plan (emergency procedures – business continuity)
- Activate insurance (cyber insurance)
- Contact CERT – police government
- Intake & study environment → Install recovery plan → Contact external IT experts (insurance)
  - Isolate all (possibly) infected systems
  - Complete IT shutdown



9:00

## Crisis cell impact

### Communication

- Internal: WhatsApp pyramid  
→ Emergency measures – patients present  
Cave: conflict IT security vs patient security  
Who's in charge?
- External → partners, government, ZNI  
Via secure internet connection

### Conflict

- IT department: shut down everything immediately
  - Doctors/nurses: keep access open to consult essential data of patients present
- Who has 'the lead'?



# Tuesday, February 2, 2021

Start IT employee & performance issues

7:15

Performance issues confirmed

8:00

Ransomware found

Crisis cell (management, nurses,  
doctors...): impact?

9:00

External IT experts

16:00

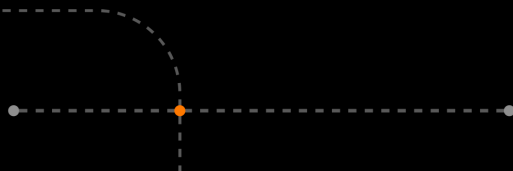
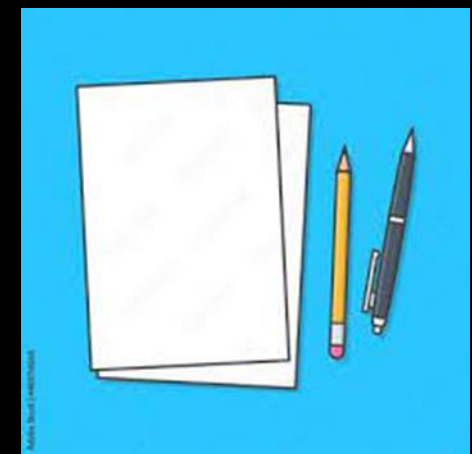
Start recovery

16:00

## External IT experts

### External IT experts

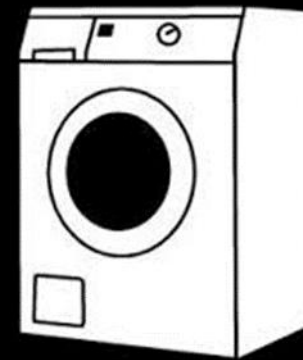
- Objectives
  - Define corrupted systems (50 out of > 800)
  - Define ransomware type
  - Define backup and recovery options
  - Define repair priority systems
- IT crisis team: analysis of technical solutions
- Operational crisis cell → business continuity plan
  - Doctors, nurses, administration, reception...
  - Planning, data collection, reception, contacts



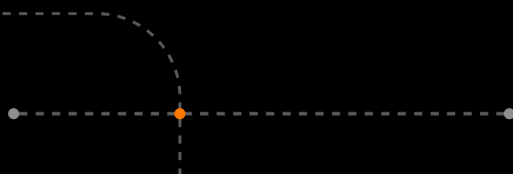


### Start recovery plan (external IT experts)

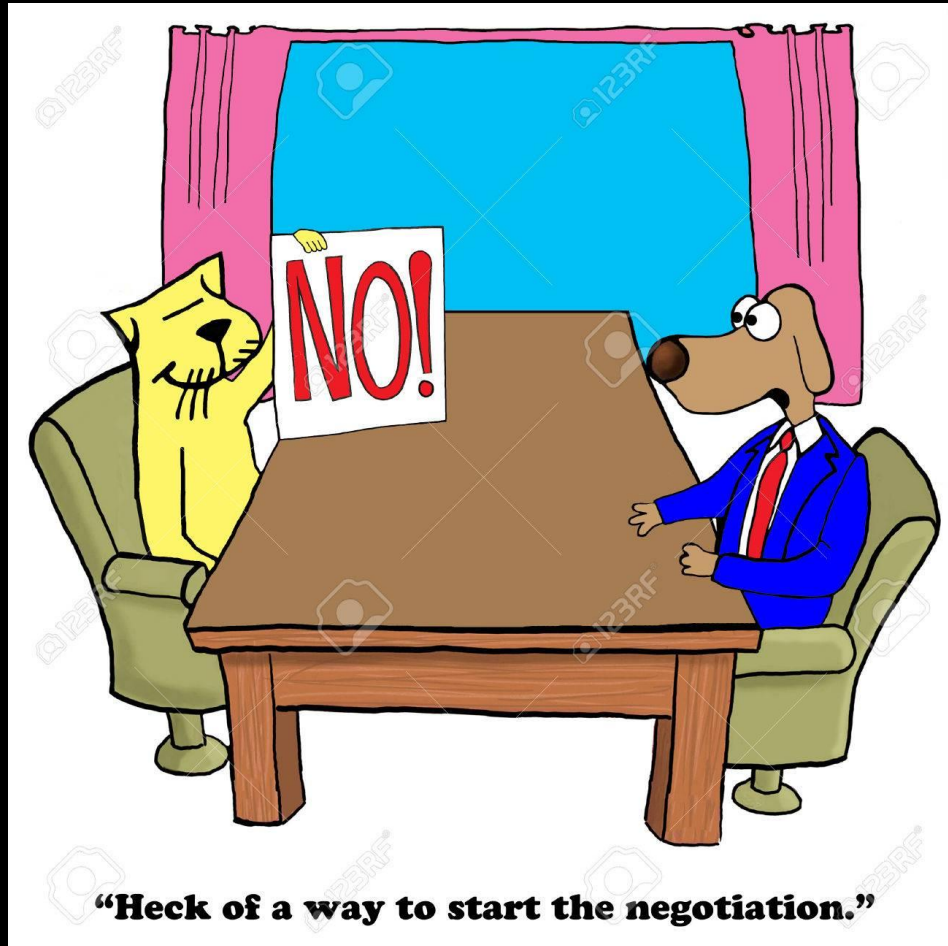
- Dividing infected / non-infected systems – isolation
- Re-installation & cleaning: ‘Wash street’
- Install comprehensive antivirus software  
Uninstall antivirus hospital – new software
- Start installing backup data



Contact with the attackers



## The next days



Negotiating with the 'attackers': IT experts + insurance

- Ethical aspects!
- Costs of damage - recovery □ Who has 'the lead'?
- Threat to patient safety?

'Business model' cybercriminals:

- Promises
- Safety issues
- Credibility
  - Honest deceivers
- Data leakage?

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



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.



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.

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.

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.



# Conclusion



- They're polite boys those hackers.
- You can't negotiate with them.

UNLESS....

- A reduction in the requested ransom
- Desinterest

# The next days

## Root cause analysis

- Hacking website (Sharepoint) → access via old DC account system-level

## Problem: service account suppliers & remote support

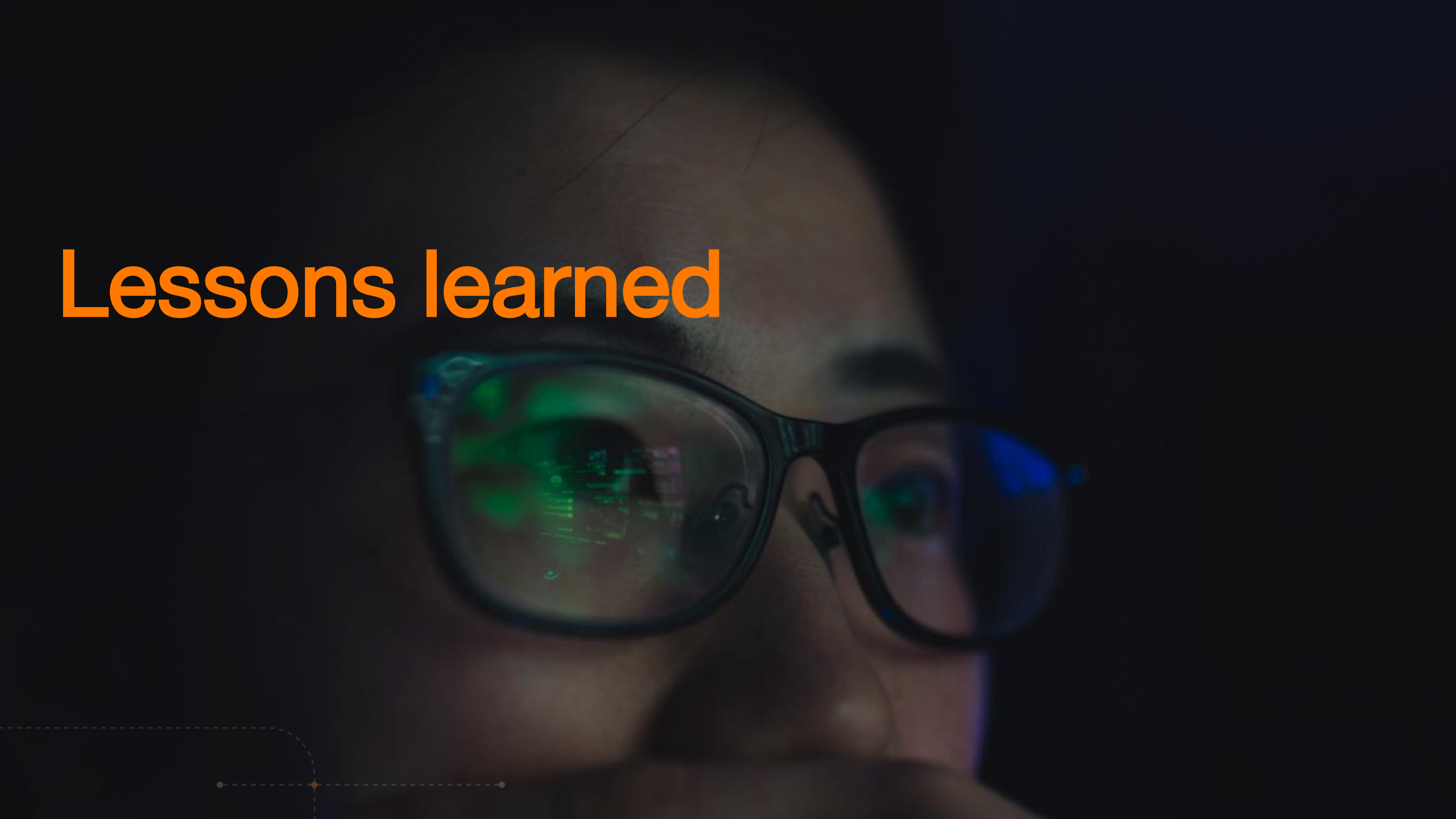
## External communication problem

- What happened
- Impact inside
- Impact on patients
- What did we do to recover?
- Timing of recovery?

## Execute recovery plan (ctd)

- Reinstall all connections
- New username and password policy
  - ‘big bang’ (paper!)...
- 2 Factor Authentication

# Lessons learned





# Lessons learned

## Organization

- Information Security Management System (PDCA cycle) □ ISO27001 of NEN7510
- Invest in IT-team (training in cybersecurity and recovery)
- Physical security organization (access control)
- Business Continuity Plan
- Procedure Cyber Insurance – be ready for ‘CERT’ (network description)

## Policy

- Policy (clean-desk, accurate password policy, incident readiness,...)

## Behavior

- Awareness



# Lessons learned

## Technical

- Rebuild website
- Invest in security monitoring, detection and response
- Office 365 migration
- MFA (multi factor authentication)
- Clean Active directory & remote support & service (SilverFort)
- Vulnerabilities and patches
- Network segmentation
- Network access control (802.1x)
- Backup & recovery (importance of off-line backup)
- Clean up IAM (i.g. after resignation)
- Improve workstation security (Anti virus next level - EDR solution)
- Forensic readiness (control logs)
- Backup internet line and telephone
- (RDP – Citrix – Office macro's - .)



# A word about the cost of an attack...

## Direct costs

- IT Experts – €450/hour...  
5 days, 12 hours/day, 4 pple + remote... → Total cost of 180K
- Own (human) resources (MDs, secretary, reception...)
- Additional software/hardware



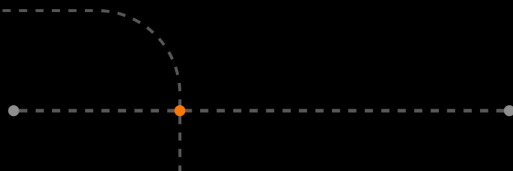
## Indirect costs

- Immediate damage costs: stop medical activities (e.g. all examinations, operations,... )
  - Future damage costs: missed future appointments
  - Loss of information (lost billings,...?)
  - Restore missed information
  - Reputation damage
  - Medical damage?
  - What if questions (data leakage, ...)
- Total cost estimated 700 – 1.000 K

# We no longer have an insurance...

- Immediate cancellation existing insurance
- Need to define damage claim before new proposal
- No other insurance company 'willing'
- Conditions (you can't refuse)...
- External supervision/control

Outsource IT?



# Action plan





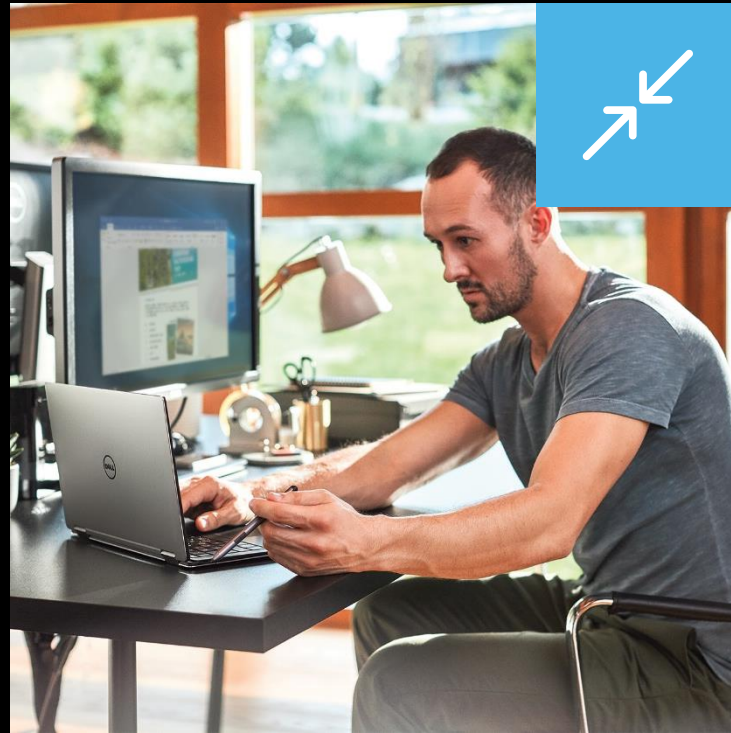
A person is seen from behind, sitting at a desk in a dimly lit room. They are looking at several computer monitors. The top-left monitor shows a list of items. The top-right monitor displays a complex network diagram with nodes and connections. The bottom-left monitor shows a world map with data points. The bottom-right monitor shows a world map with a grid overlay. The person's right hand is raised, pointing at the top-left monitor. The text "Time for a Zero Trust approach" is overlaid in a large, orange font across the center of the image. In the bottom-left corner, there is a decorative graphic consisting of a dashed line with a small orange dot at its end.

Time for a Zero Trust approach

# Zero Trust: a new reality needs new principles



**Verify explicitly**



**Use least privileged access**



**Assume breach**

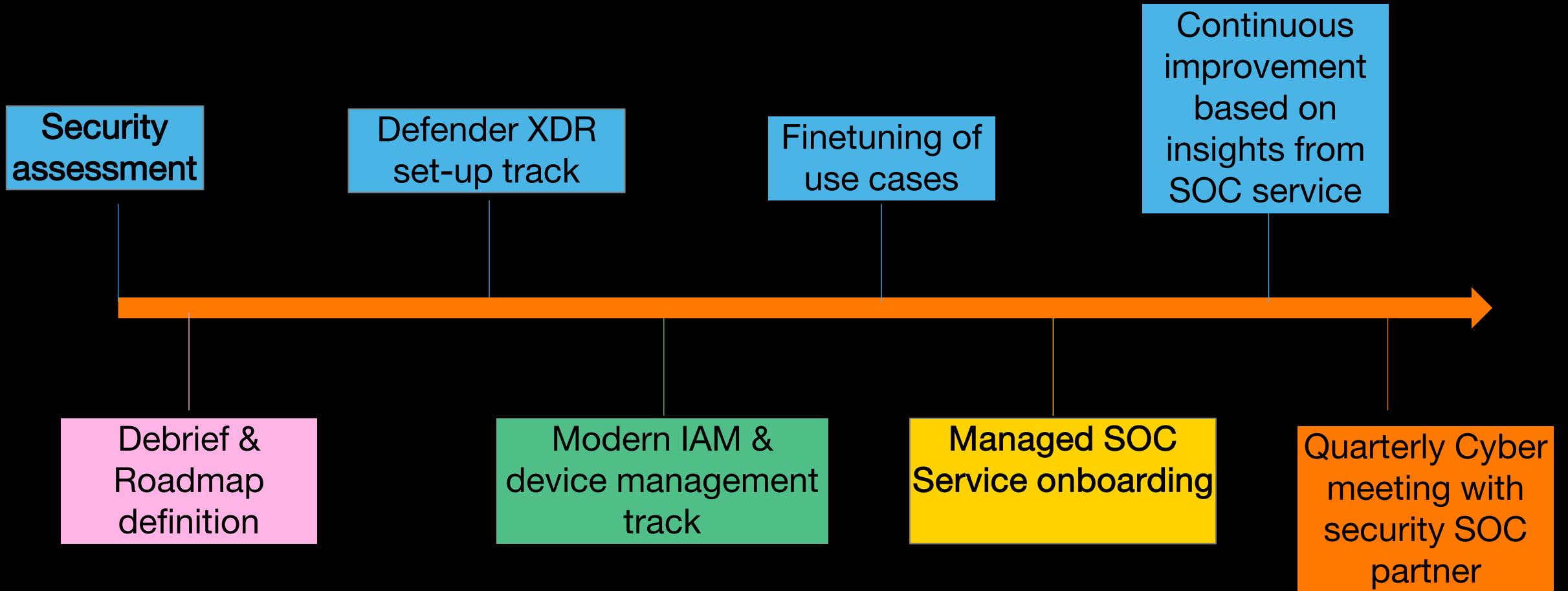




# Zero Trust set-up H.H. Mol

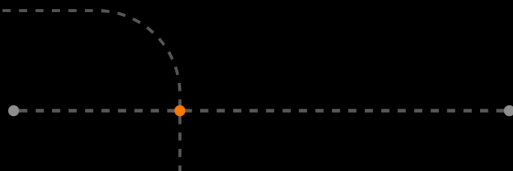


# Timeline H.H. Mol



# Why SOC as-a-service?

- **Unburdening: cybersecurity follow-up is complex: specialized knowledge & resources required**
- **Follow-up is necessary**
  - **Proactive**
    - Insights from SOC form the basis for evolutionary improvement actions, both through technological evolution and from SecOps.
    - Monthly SOC report + Quarterly meeting in which open vulnerabilities and recommendations are listed and discussed
  - **Reactive**
    - Suspicious incidents are not always resolved 'automatically' by the technology; manual follow-up and intervention are necessary. Being agile is very important in cybersecurity.
- **SOC is often a prerequisite for (affordable) cybersecurity insurance**



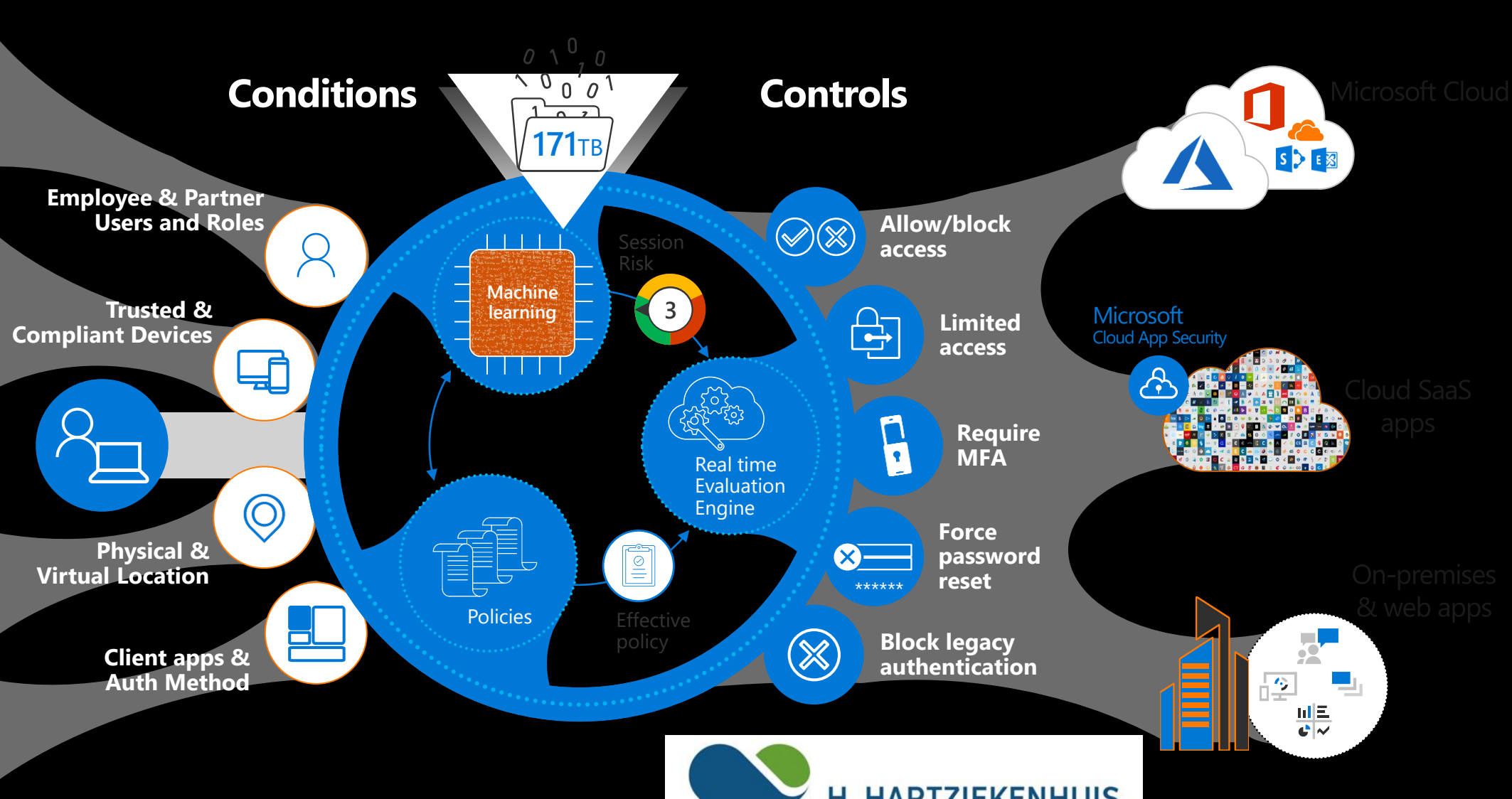
# Azure AD Conditional Access + Identity Protection

- Azure AD
- ADFS
- MSA
- Google ID

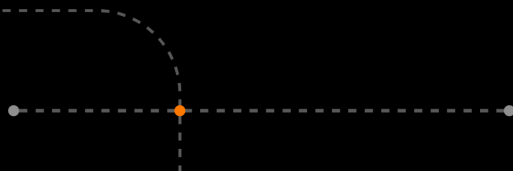
- Android
- iOS
- MacOS
- Windows
- Microsoft Defender for endpoints

- Geo-location
- Corporate Network

- Browser apps
- Client apps



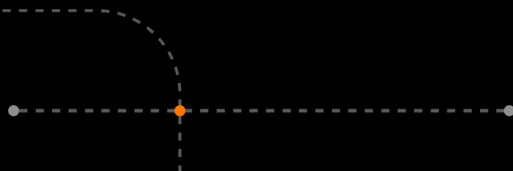
# General conclusion



# General conclusion



*Elk nadeel  
HEB ZIJN  
voordeel  
- Johan Cruyff*



# General conclusion

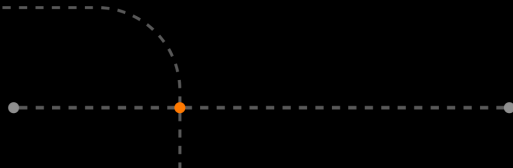


*Elk nadeel  
HEB ZIJN  
voordeel  
- Johan Cruijff*

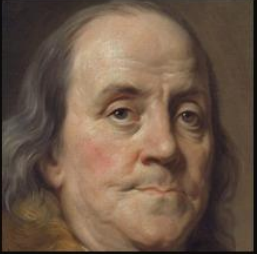
Als wij de bal hebben kunnen  
hun niet scoren.

- Johan Cruijff

Citates.NET



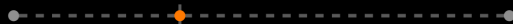
# Take home message



By failing to prepare, you are preparing to fail.

~ Benjamin Franklin

AZ QUOTES





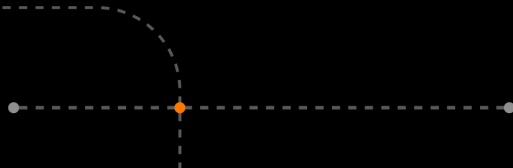
# Take home message



By failing to prepare, you are preparing to fail.

~ Benjamin Franklin

AZ QUOTES



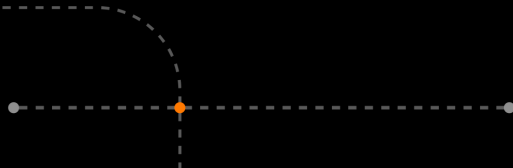
# Take home message



By failing to prepare, you are preparing to fail.

~ Benjamin Franklin

AZ QUOTES

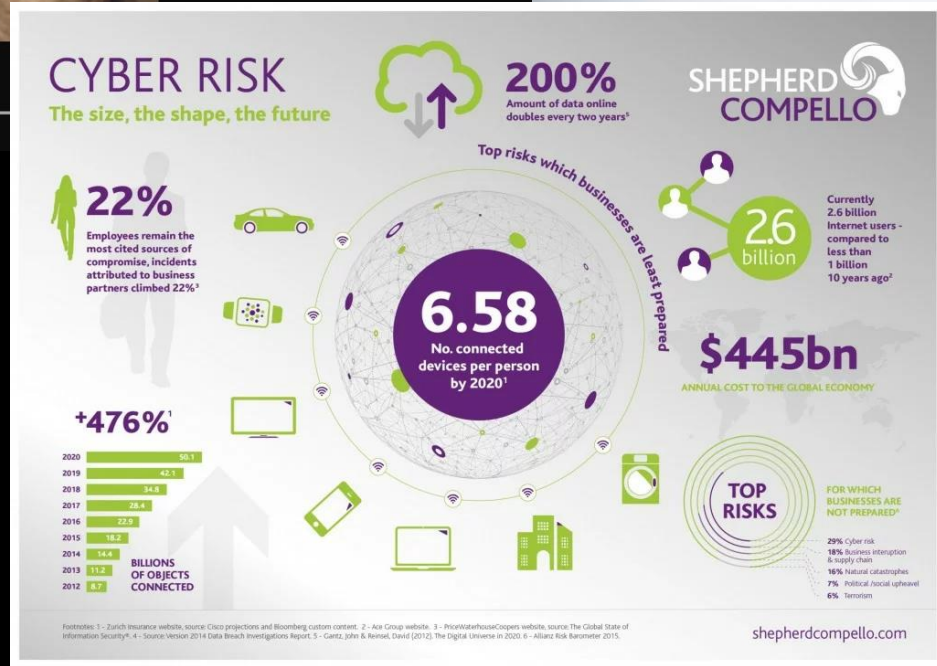


# Take home message



By failing to prepare, you are preparing to fail.

~ Benjamin Franklin

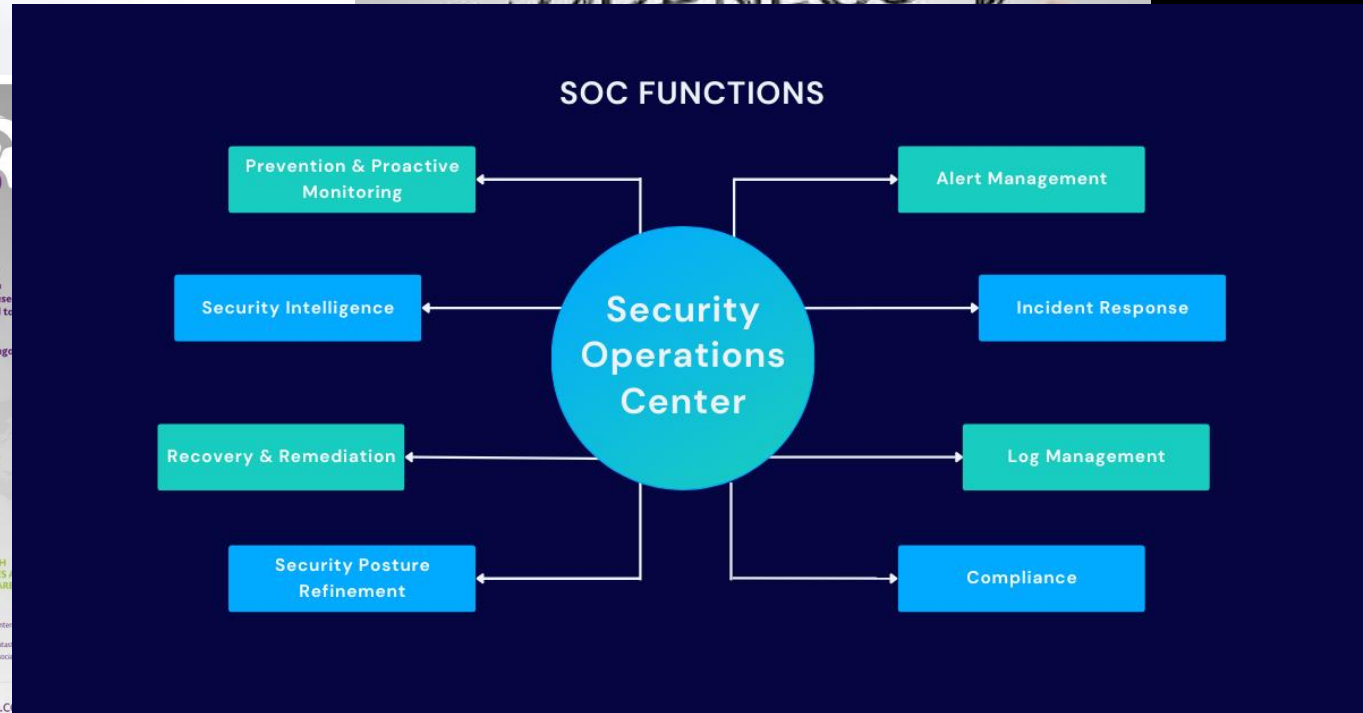
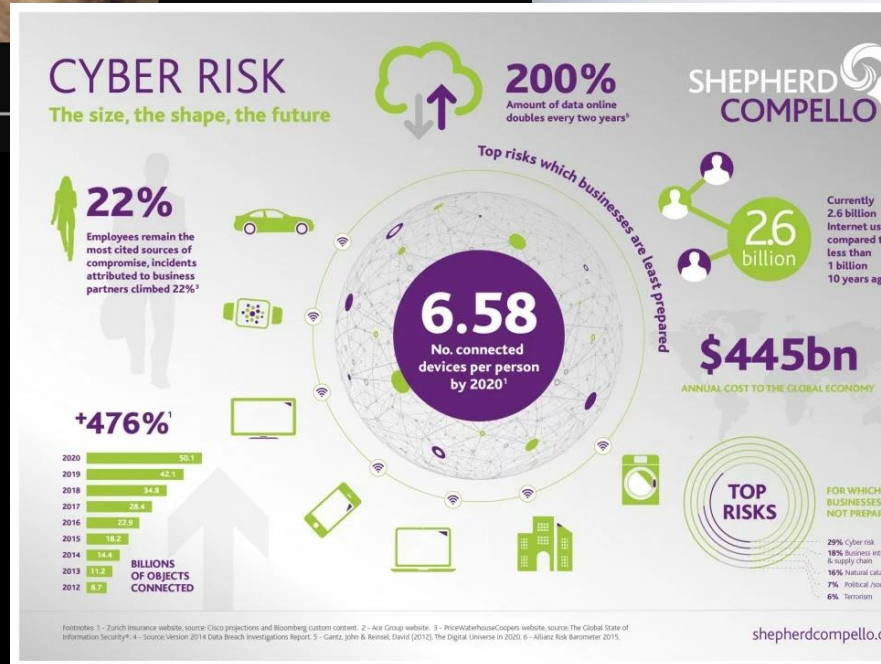


# Take home message

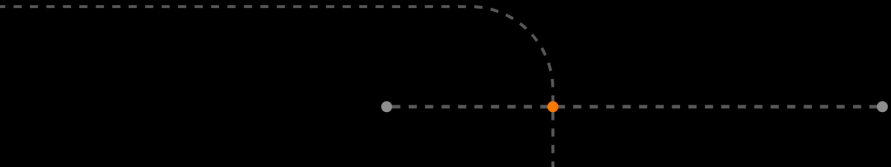


By failing to prepare, you are preparing to fail.

~ Benjamin Franklin



# Q&A



# Thank you

