TLP:AMBER

CYBER THREAT RADAR

Dutch Healthcare Sector

COMPUTER EMERGENCY
RESPONSE TEAM
VOOR DE ZORG
CERT

10 October 2022 - Copenhagen
7th e-Health Security Conference

https://www.linkedin.com/in/wimhafkamp/

Wim Hafkamp

- Managing Director Z-CERT
- Dep. Director National Cyber Security Center
- Group CISO Rabobank
- Founder and Chair Financial ISAC NL
- Chair Advisory Board Cybersecurity Research Community NL
- Member of Permanent Stakeholder Group ENISA

300 member organizations

2017
4 employees

2022
27 employees

ROOTS AND ORIGINS OF Z-CERT

Sponsors

Ministerie van Volksgezondheid, Welzijn en Sport

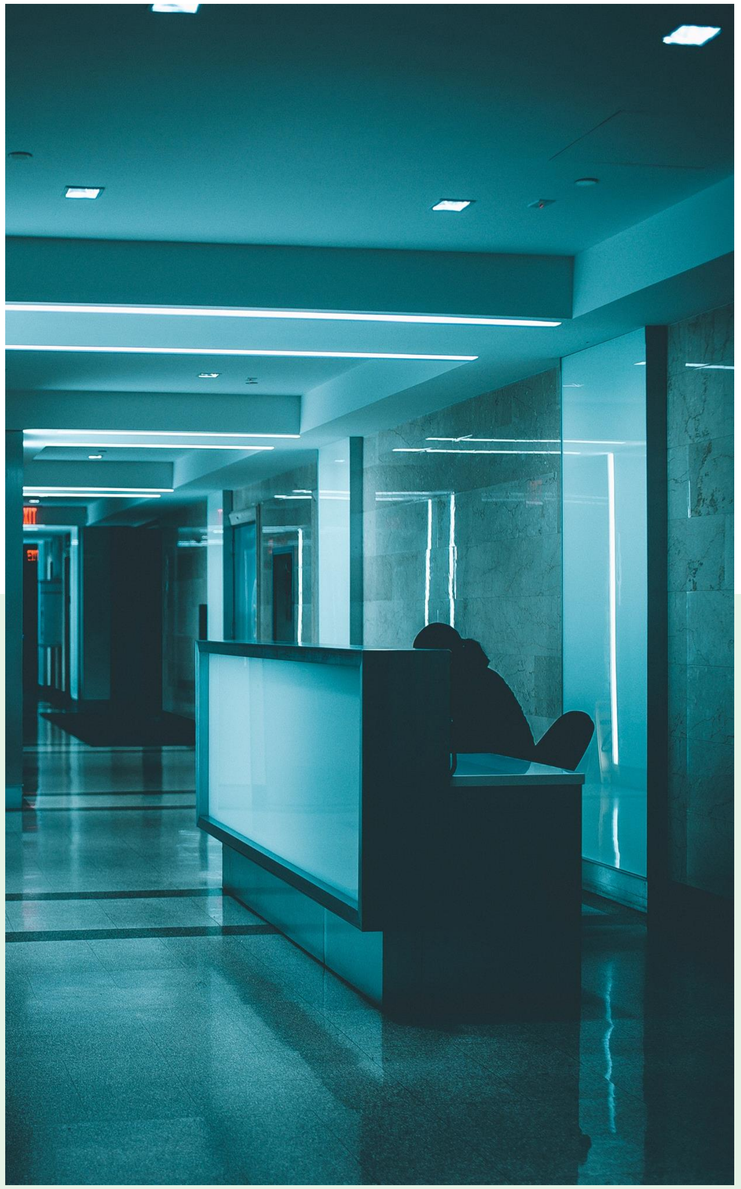
NFU NEDERLANDSE FEDERATIE VAN UNIVERSITAIR MEDISCHE CENTRA

Nederlandse Vereniging van Ziekenhuizen

de Nederlandse ggz

Foundation (Nonprofit)

- Membership fees
- Public funding



(Medical) Advisories

IOCs

Best Practises (NEN7510)

E-mail / Cyware (CSAP)

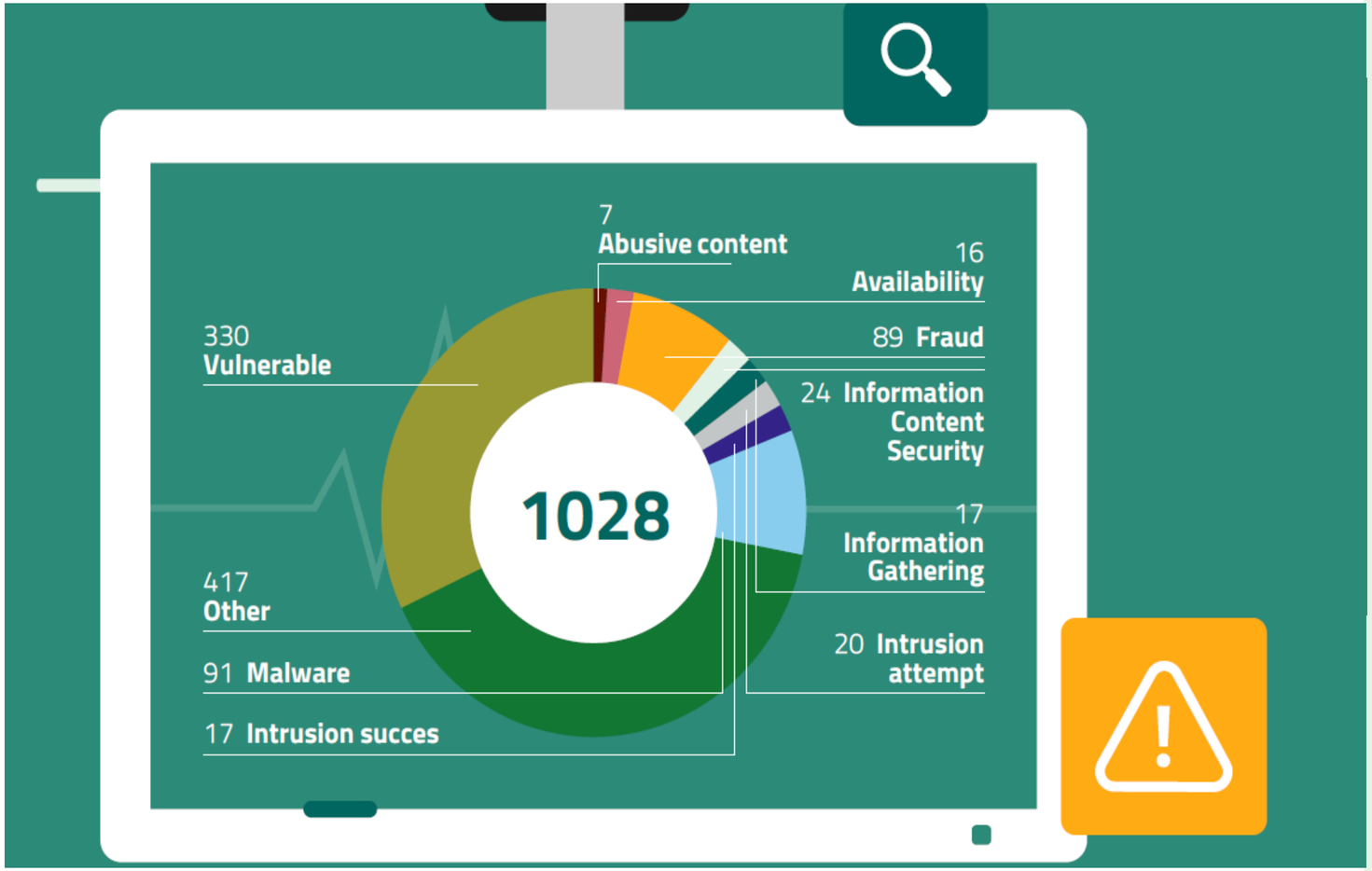
ZDN (MISP)

Factsheets / Webinars

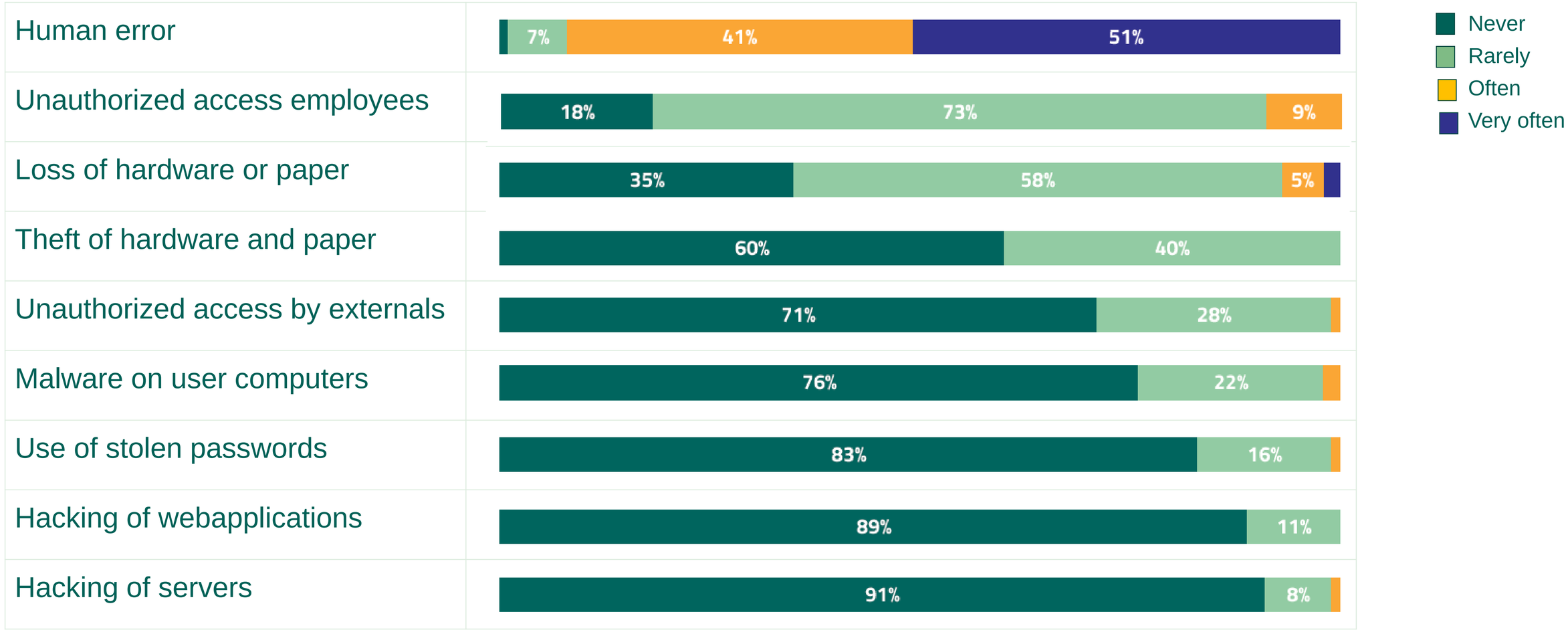
INFORMATION SHARING

“Improve and build up cyberresilience in the Dutch Healthcare sector”

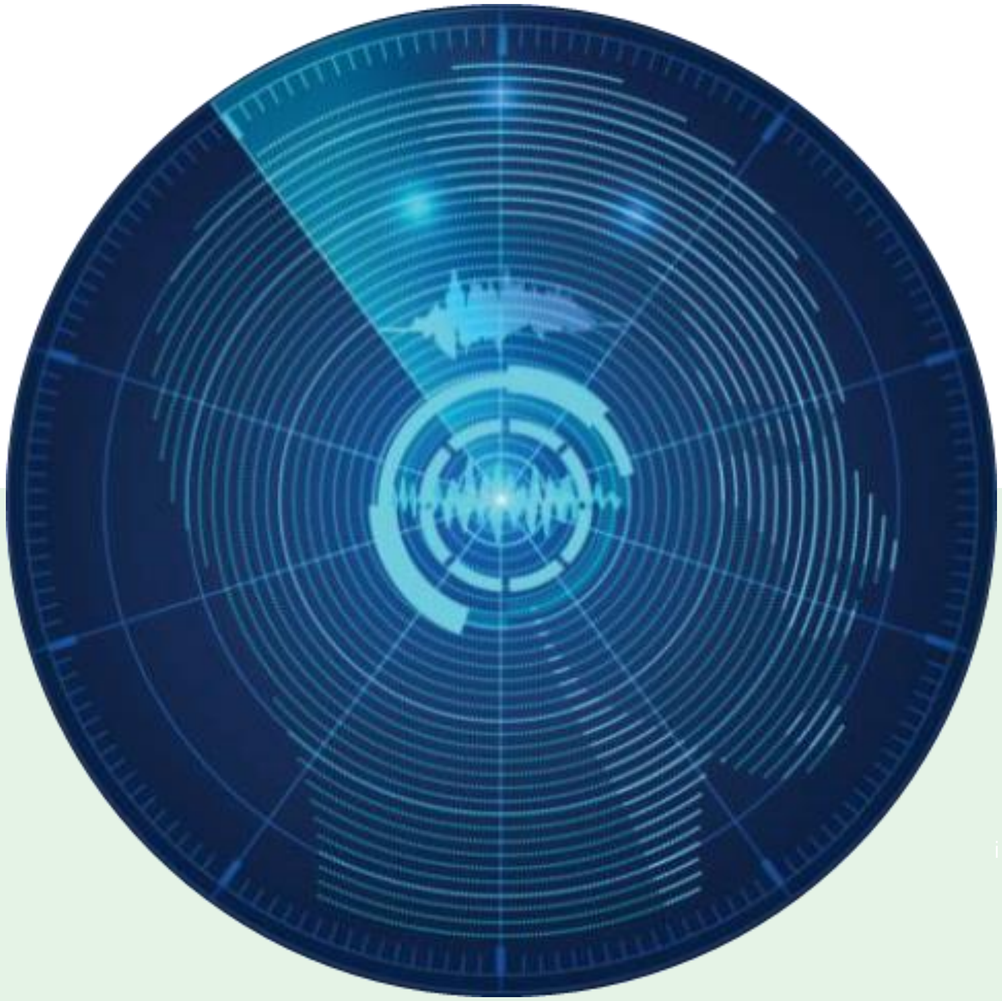
Incidents reported to Z-CERT including operational advisories towards members



Top 9 Data Breaches in 2021 *



* Source: Z-CERT member survey

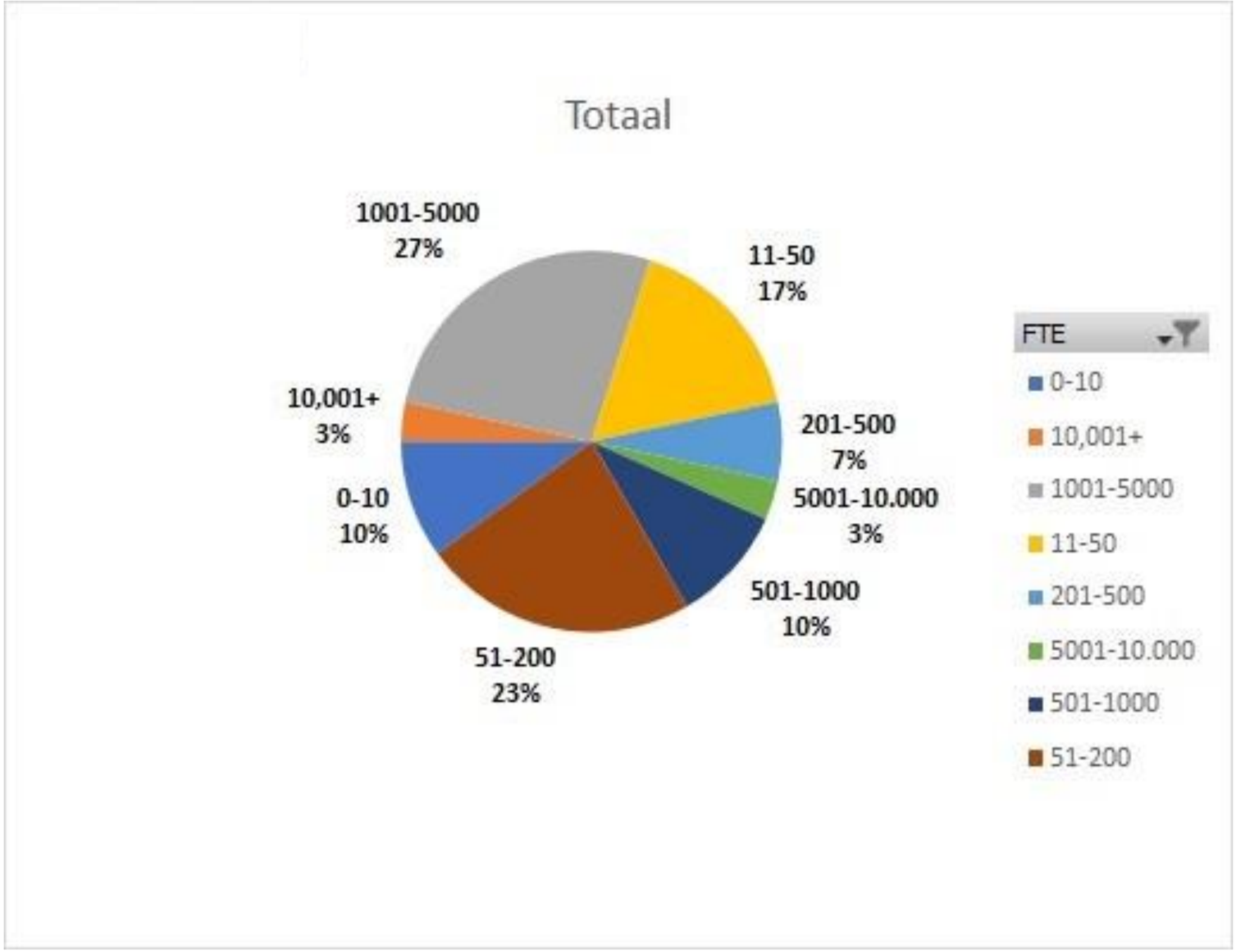


CYBER THREAT RADAR HEALTHCARE NL

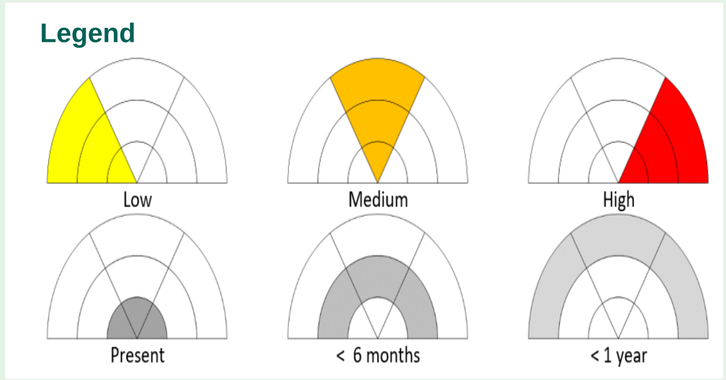
Top 10 Cyber Threats

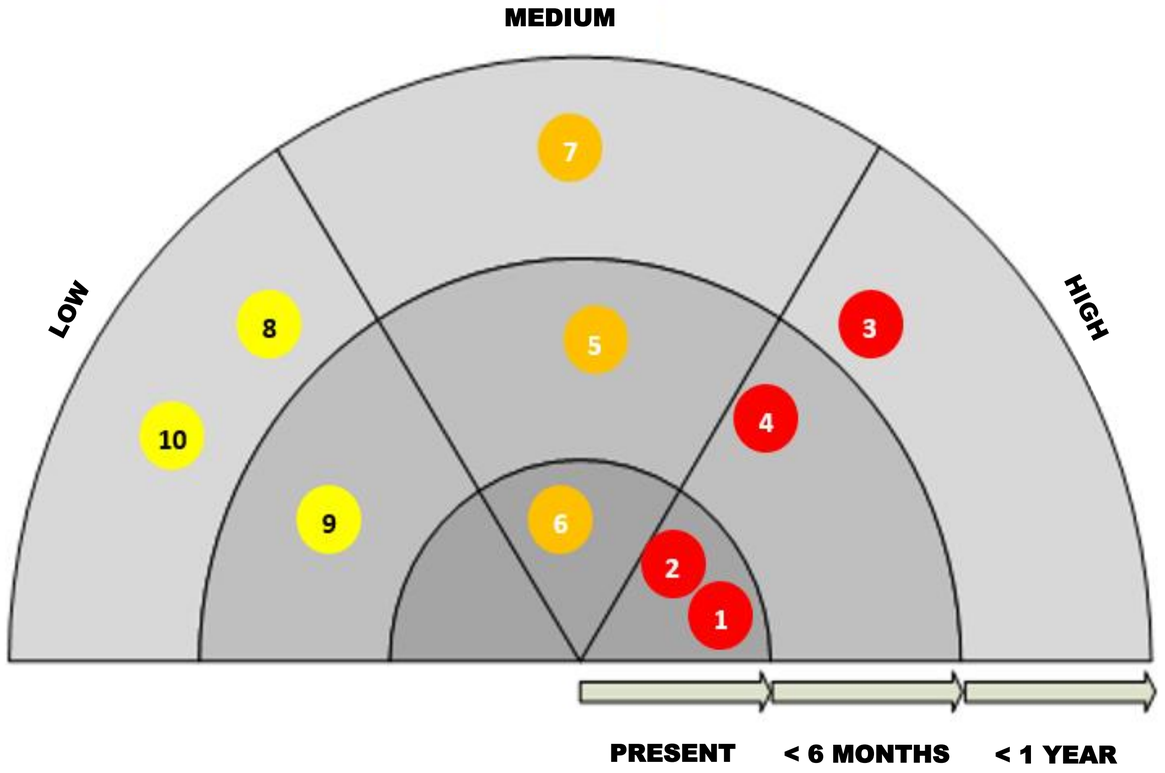
	Threat
1	Ransomware
2	Unavailability of Information Systems or Portals
3	Theft of medical patient records
4	Supply chain attacks
5	Attacks via vendors
6	Phishing
7	Attacks on connected medical devices
8	Insider threats
9	Malware via compromised websites
10	Malicious apps

Healthcare ransomware victims versus #FTE



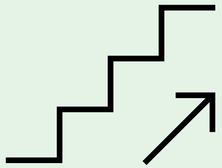
RADAR





1. Ransomware
2. Unavailability of information systems or portals
3. Theft of medical patient records
4. Supply chain attacks
5. Attacks via vendors
6. Phishing
7. Attacks on connected medical devices
8. Insider threats
9. Malware via compromised websites
10. Malicious apps

CYBERTHREAT ENABLERS



1	**Vendor market dominance**
2	Shadow IT
3	COVID 19 - IT network bypasses
4	Geopolitical situation (War in Ukraine)
5	Shift to home treatments
6	Cybersecurity mesh
7	Medical systems legacy

CYBERSECURITY DISABLERS

1	Cybersecurity knowledge of IT staff
2	Misconfigured API’s
3	Awareness @ board level
4	Tight cybersecurity labor market
5	Insufficient patch management
6	Awareness @ app developers
7	Cached admin credentials
8	Violation of least privileged policy
9	Disinformation / hoaxes

Stichting Z-CERT

www.z-cert.nl