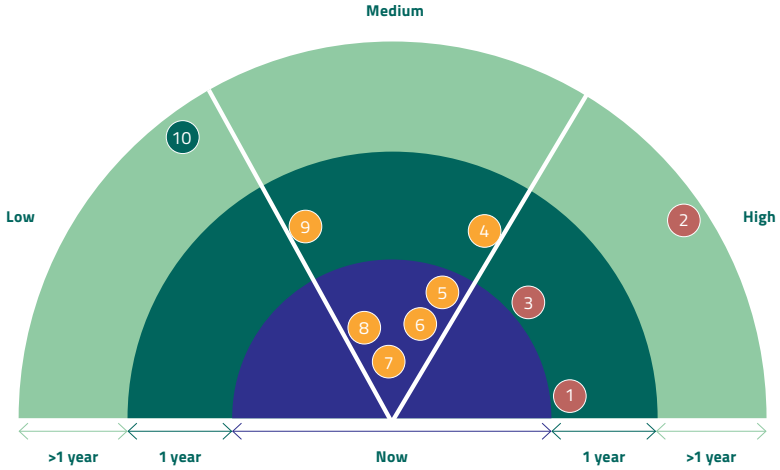
Cybersecurity report 2025



Threat Radar

The threat radar shows the timing, impact, and therefore the severity of the threat to the healthcare sector. The position of the various dots in the inner, middle, or outer ring indicates when something is expected to become a threat.

Threats – Trends and Developments

Threat	Level	Context
1. Ransomware and extortion involving data leaks		This threat remains consistently high. Single stage extortion, in which attackers threaten to publish stolen data, is gaining ground. In these cases, data encryption is omitted.
2. Espionage at research institutions		The Dutch healthcare sector is of interest to state sponsored actors due to its high quality scientific research, intellectual property, and large datasets of medical and personal data. In some cases, these actors use ransomware in addition to espionage, either as a distraction or for personal gain.
3. Ransomware at suppliers		A significant number of suppliers to European healthcare organisations have been affected. Ransomware has disrupted processes, and confidential data has been leaked. In the Netherlands, the incident involving Clinical Diagnostics was particularly notable.
4. DDoS attacks at suppliers		Various sectors supplying healthcare organisations were targeted, including telecom and service providers and information technology and service companies. As a result, several digital services were temporarily unavailable or only partially accessible.
5. Malware		In many cases, the impact of malware incidents is limited and infections are quickly resolved. Cybercriminals increasingly use infostealers to steal passwords or continue an attack. This year, it was notable that some (inexpensive) Android devices were delivered with malware pre-installed.
6. Credential Phishing		MFA is important but not foolproof. Not all MFA solutions withstand the latest phishing techniques, allowing malicious actors to gain access to mailboxes and other platforms linked to those login credentials. Several healthcare organisations were affected, often receiving phishing emails sent from a compromised supplier mailbox.
7. Insider threats		The frequency varies greatly depending on the type of insider threat. When incidents occurred, they often affected dozens of systems within an organisation. Unintentional data leaks are particularly common. Notable incidents this year involved former employees or contractors who stole data or threatened to do so.
8. DDoS		Geopolitical developments have not led to an increase in the number of incidents.
9. Financial fraud		The impact of financial fraud was greater than in 2024. However in 2025, it mainly involved forged invoices sent from compromised mailboxes of familiar colleagues or organisations.
10. Espionage at healthcare providers		Countries with offensive cyber programs are primarily interested in stealing scientific research or personal data belonging to targets of strategic interest. Therefore, healthcare institutions that do not possess such information are unlikely to be targeted.