Cyberattack RT & framework/ROSEIS

Petra Reijnders-Thijssen
Manager kwaliteit & veiligheid : Maastro
Voorzitter ROSQC/ESTRO
Mede-cursusleider : risk course ESTRO

Kosten cyberattack

Global Benchmarks for 2025

According to multiple industry reports, the **average cost of a cyberattack in 2025** varies significantly depending on the type of organization and region:

- **Global Average**: Approximately **$4.4 million per breach**, a slight decrease from 2024 due to improved detection and AI-powered defenses. [infinum.com]
- **United States**: The average breach cost is **$9.48 million**, the highest globally. [bluefire-redteam.com]
- **Healthcare Sector**: Continues to be the most expensive, with average breach costs around **$10.93 million** in 2023 and **$9.8 million** in 2024.
- **Small Businesses**: Median cost is **$46,000**, but over half of victims report losses exceeding **$100,000**. [smartfinancial.com]

The **total global cost of cybercrime** is projected to reach **$10.5 trillion in 2025**, making it one of the largest economic threats worldwide. [deepstrike.io], [infinum.com]

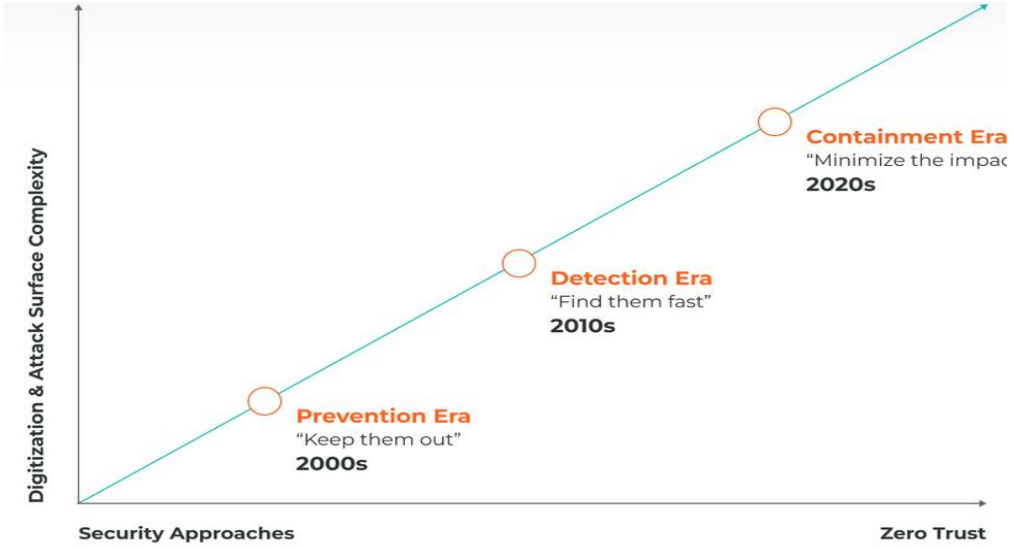
https://www.illumio.com/products/what-is-zero-trust-segmentation

Breach containment. The new paradigm.

It seems everything has to be connected to the internet these days. Convenient to many, but a significant challenge for CISOs, security, and IT teams. IT environments are moving from on-premises to a hybrid, cloud-first, hyper-connected landscape. Digital transformation is dramatically expanding the attack surface, and attacks like ransomware are more pervasive than ever. In the past two years alone, 76% of organizations were attacked by ransomware, and ransomware attacks occur every 11 seconds. All these factors are increasing risk.

76%
of organizations
In the past 2 years, 76% of organizations were attacked by ransomware

11
seconds
Ransomware attacks occur every 11 seconds



Indeling presentatie

1. Trends aanvallen
2. Incidenten
3. Impact radiotherapie
4. Wat kan ons helpen!

Risico is kans maal effect

Trends aanvallen

Algemene trends in cyberaanvallen op de zorgsector

De zorgsector, inclusief radiotherapiecentra, is een steeds vaker doelwit van cyberaanvallen vanwege:

1. De waardevolle patiëntgegevens die ze beheren.
2. De afhankelijkheid van digitale systemen voor behandelingen.
3. Vaak beperkte IT-budgetten en verouderde systemen

https://cybermap.kaspersky.com/country/NL (real-time cyberaanvallen wereldwijd)

Hoewel specifieke aanvallen op radiotherapiecentra zelden publiekelijk worden gedocumenteerd, zijn er wel meldingen van bredere aanvallen op ziekenhuizen en medische instellingen waarbij ook radiotherapiesystemen zijn getroffen. Bijvoorbeeld:

Ransomware-aanvallen die hele ziekenhuisnetwerken platleggen, waardoor ook radiotherapiesessies worden uitgesteld of geannuleerd.

WannaCry (2017) trof onder andere het Britse NHS, wat leidde tot uitval van medische apparatuur, inclusief beeldvormings- en behandelsystemen.

Scripps Health (VS, 2021): Een ransomware-aanval legde het hele IT-systeem plat, inclusief toegang tot radiotherapiegegevens en planning. Patiënten moesten worden verplaatst of behandelingen uitgesteld.

Incidenten

In **Europa** was tussen 2021 en 2023 **53% van alle cyberaanvallen gericht op de gezondheidszorg**

Aanvallen:

2021: Ireland

2024: Spanje

2024: Duitsland

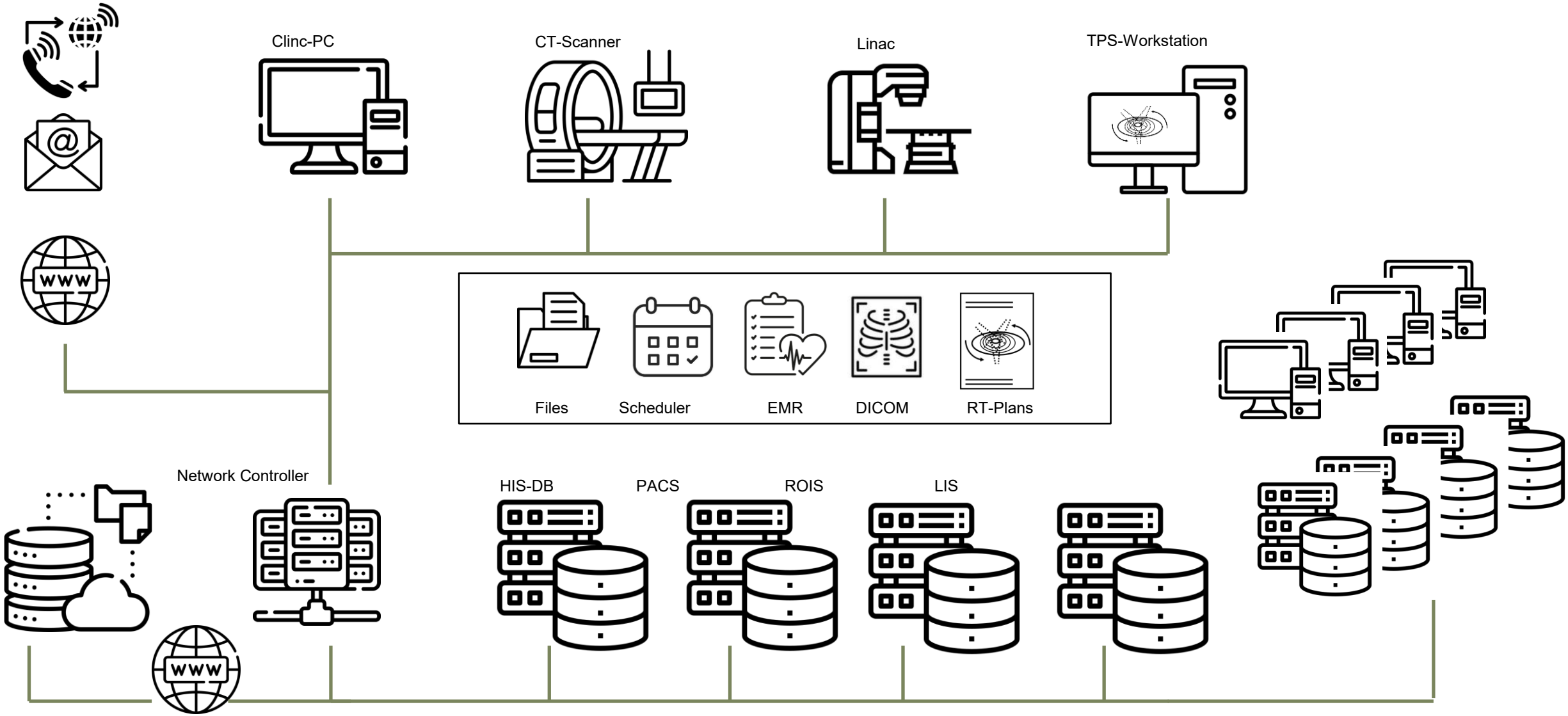
2025: overal

Personal View of a National Cyberattack

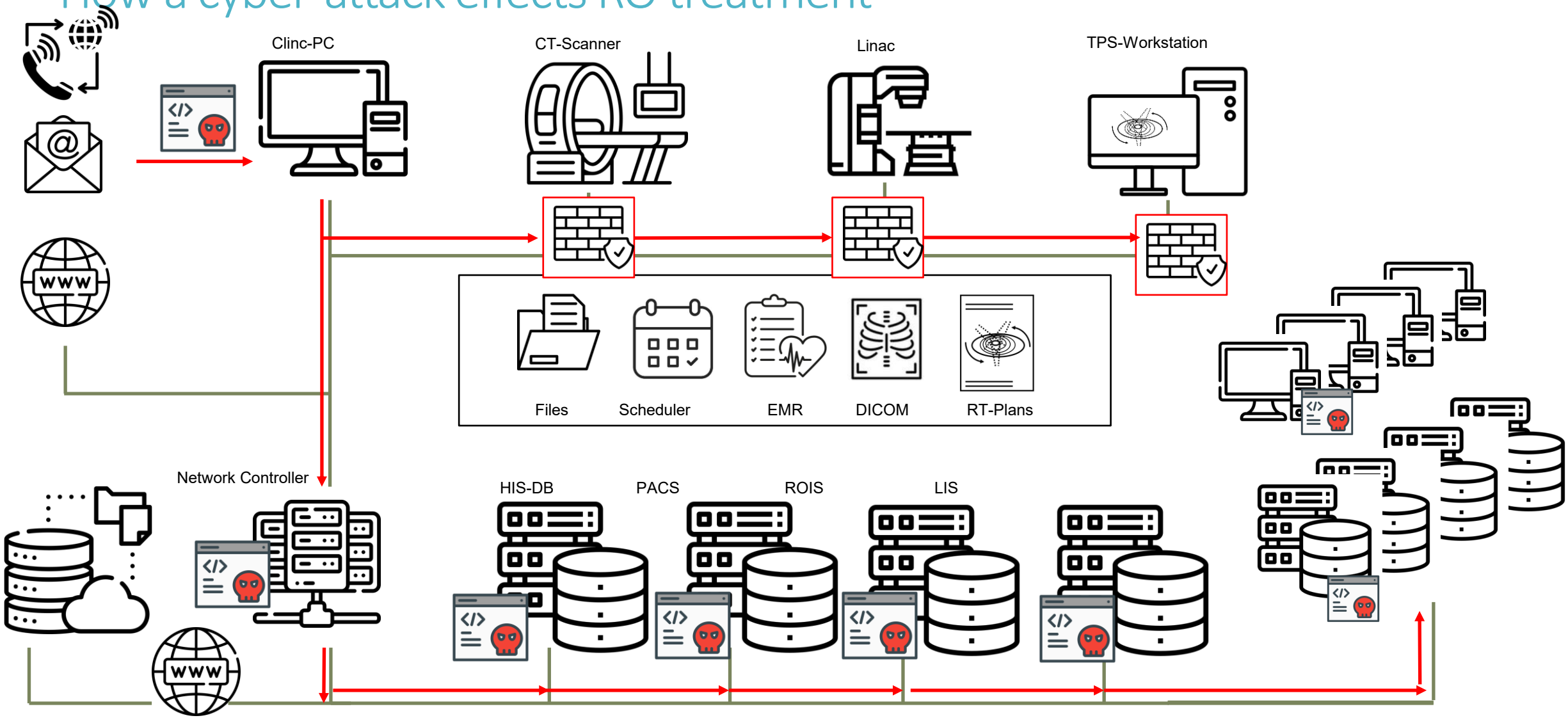
Friday 14 May 2021, is a day I will never forget. I walked to work with a colleague, having heard on the national news that there had been a cyberattack on the Health Service Executive (HSE), i.e., the Irish health system. We had just come out of another COVID lockdown, the sun was shining, and certainly we had no desire to discuss another looming disaster. We briefly mentioned it, I suppose thinking it would be sorted by the time we got to work, or that it probably wouldn't affect our services. Anyway, we were very wrong. In the case of my hospital, only 16 days later were we able to deliver radiotherapy to a patient. That period and subsequent dealing with the aftermath meant that those summer months were an absolute nightmare.

Aileen Flavin
Radiation Oncologist
Medical Imaging & Radiation Therapy
School of Medicine, University College Cork
Ireland

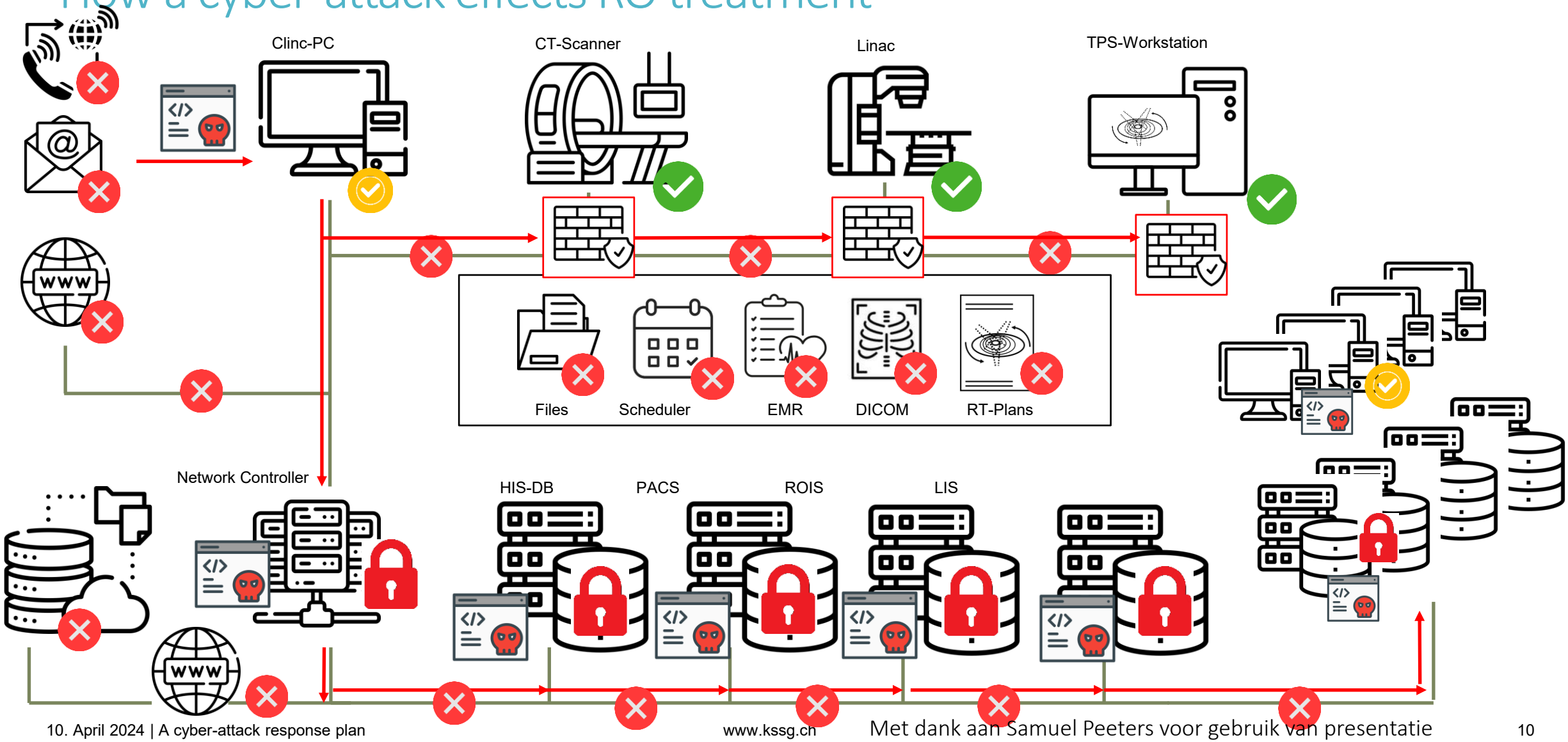
How a cyber-attack effects RO treatment



How a cyber-attack effects RO treatment



How a cyber-attack effects RO treatment



Consequences van een cyberattack

Gevolgen voor de patiënten:

Gevoelige patiëntinformatie kan openbaar worden gemaakt of blootgesteld aan het publiek.

Behandelingen van patiënten worden voor onbepaalde tijd onderbroken: Een paar weken? Een paar maanden?

Radiobiologisch effect?

Psychologisch effect voor de patiënt.

Gevolgen voor het personeel: geen toegang tot:

HIS/OIS: Patiëntdemografische gegevens – je kunt een patiënt niet bellen om hem of haar te informeren dat de behandeling moet worden uitgesteld of …

OIS/TPS: Gegevens over de behandeling van de patiënt.

OIS: Lijst van patiënten in behandeling – afsprakenlijst.

Ziekenhuisnetwerk en IT-infrastructuur (pc's, internet, opslag, PACS, …)

Impact radiotherapie

Waarom radiotherapie kwetsbaar is

Radiotherapie maakt gebruik van:

1. Geavanceerde software voor dosisplanning.
2. Netwerkverbonden apparatuur (zoals lineaire versnellers).
3. Patiëntgegevens die vaak centraal worden opgeslagen.

Deze afhankelijkheid van digitale systemen maakt radiotherapie bijzonder gevoelig voor IT-storingen en cyberaanvallen.

Wat kan ons helpen!

1 Preventie

Risicobeheer en -beoordeling: Voer regelmatige audits uit van IT-systemen en medische apparatuur.

Opleiding van personeel: Train artsen, technici en administratief personeel in cyberhygiëne (zoals phishingherkenning en wachtwoordbeheer).

Segmentatie van netwerken: Scheid radiotherapiesystemen van algemene ziekenhuisnetwerken om besmetting te beperken.

🕵️ 2. Opsporing

Monitoringtools: Implementeer geavanceerde detectiesystemen voor verdachte activiteiten.

Vroegtijdige waarschuwing: Sluit aan bij EU-initiatieven voor realtime dreigingsinformatie (beschikbaar vanaf 2026).

🛠️ 3. Reactie en Herstel

Incidentresponsplan: Ontwikkel en test draaiboeken voor cyberincidenten, specifiek voor radiotherapie.

Back-ups: Zorg voor dagelijkse back-ups van patiëntendossiers en behandelplannen, offline opgeslagen.

Samenwerking met nationale cyberdiensten: Maak gebruik van EU-cyberbeveiligingsreserves en lokale hulpdiensten.

🚫 4. Afschrikking

Beveiligingsbeleid en naleving: Zorg dat alle systemen voldoen aan NIS2-richtlijnen en GDPR.

Gebruik van cyberdiplomatie: Werk samen met overheden om aanvallen te melden en te vervolgen.

Working together

Samenwerking met BeSTRO:

BeSTRO is de wetenschappelijke organisatie voor radiotherapie in België. Lidmaatschap staat open voor radiotherapeuten, radiotherapeuten in opleiding, radiatiefysici, radiobiologen, biomedici en radiotherapeutisch laboranten.

Werkgroep Cybersecurity:

We werken samen met Belgische ziekenhuizen om:

Elkaar te ondersteunen bij het opzetten van preventieplannen en mogelijke oplossingen.

Informatie te verzamelen over bestaande lineaire versnellers (linacs), behandelaccessoires, TPS, OIS, enz.

Werkgroep DPO (Data Protection Officer):

Bescherming van patiëntgegevens: opslag en uitwisseling van patiëntdata.

Werken aan naleving van GDPR, Cloud Act, enz.

ESTRO – ROSQC commissie (Radiation Oncology Safety and Quality):

Schrijfgroep voor richtlijnen bij cyberaanvallen (Samuel Peters – Petra Reijnders-Thijssen, …)

Met dank aan Samuel Peeters voor gebruik van presentatie

ROSQC

Description

The ROSQ Committee was established in 2016 to address issues of safety and quality from an ESTRO perspective. Safety and quality are integral to the achievement of the ESTRO Vision but, prior to this, the profession specific committees have addressed issues of safety and quality individually. The aim is to position ESTRO at the forefront of Safety, Quality and Risk Management in Europe. It was felt that a single focus for these issues was necessary to achieve cohesion and clarity of action. The ROSQC is multidisciplinary reflecting the importance of involvement in safety and quality for all professionals and has an international component to reflect the importance of collaboration with other professional societies addressing similar issues.

Strategy

Activities

Michael Baumgartl, Medical Physicist, University Hospital Zurich (CH)

Aileen Flavin, Radiation Oncologist, University College Cork (IE)

Velimir Karadža, RTT, University of Applied Health Sciences Zagreb (HR)

Maeve Kearney, RTT, Trinity College Dublin (IE)

Philippe Maingon, Radiation Oncologist, Hôpital Pitié-Salpêtrière, Sorbonne Université (FR)

Samuel Peters, Medical Physicist, Kantonsspital St.Gallen (CH)

Carl Rowbottom, Physicist, Clatterbridge Cancer Centre & University of Liverpool (UK)

Daniela-Lidia Sandu, Radiation Oncologist, University of Medicine and Pharmacy Timișoara (RO)

Affiliate Member: **Aude Vaandering**, RTT/Quality Manager, Cliniques Universitaires St-Luc Hospital (BE)

Young Committee Representative: **Daniel Portik**, Radiation Oncologist, Maastro (NL)

ROSEIS Working Group:

Chair: **Mary Coffey**, RTT, Trinity College Dublin (IE)

International Liaison Group:

Geoff Delaney, Radiation Oncologist, South-Western Sydney Local Health District (AU)

Brian Liszewski, RTT, University of Toronto (CA)

Framework ROSQC

CYBERATTACK-groep ROSQC

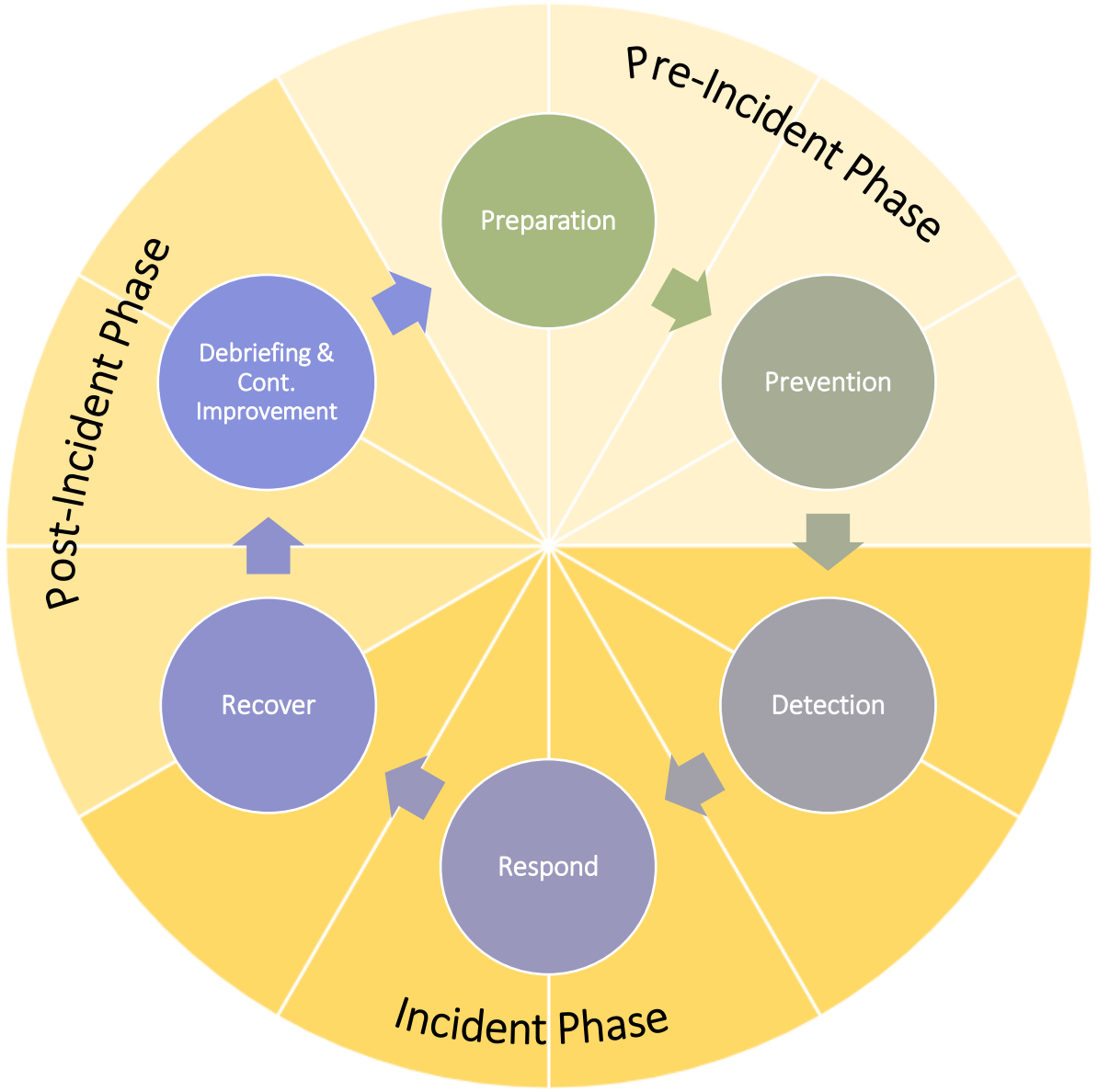
Het risico op cyberaanvallen neemt toe en kan grote problemen veroorzaken voor radiotherapieafdelingen. Ervaringen uit verschillende landen hebben ons inzicht vergroot in de risico's en de methoden die zijn gebruikt om de impact van dergelijke aanvallen te beperken en te beheren.

Het uiteindelijke doel van deze werkgroep is het ontwikkelen van specifieke richtlijnen voor radiotherapie om de impact op de behandeling van patiënten bij een cyberaanval tot een minimum te beperken. Er zijn al verschillende publicaties geïdentificeerd die beschikbaar zullen worden gesteld.

De Ierse overheid heeft een gedetailleerd document opgesteld over de cyberaanval die de volledige publieke gezondheidszorg platlegde en hoe deze werd aangepakt.

Taken:

1. Een literatuurstudie uitvoeren
2. Analyse van de bevindingen en de belangrijkste aandachtspunten
3. Vergelijking van de risico's die tot cyberaanvallen hebben geleid en de daaropvolgende acties
4. Ontwikkelen van een richtlijn voor preventie, herstel en mitigatie in het geval van een succesvolle aanval



- **Review** past events (lessons learned)
- **Check** whether plans in place have worked effectively or whether changes are required
- **Adapt and test** the detect, response and recovery plans in line with lessons learned
- Ensure **organisational learnings** from each phase of incident handling
- **Disseminate learning** to the wider organisation

Met dank aan Samuel Peeters voor gebruik van presentatie

Cyber-attack response plan - samenvatting

De dreiging is reëel – ransomware-aanvallen op ziekenhuizen nemen toe!
Wees voorbereid door een Incident Response Team en een Business Continuity Plan te hebben.
Evalueer de procedures regelmatig met alle betrokken partijen.
Werk samen met omliggende ziekenhuizen.

Praktische aspecten:
Zorg voor een geldige back-upoplossing (offline, op papier).
Zorg voor een geldige noodprocedure voor behandelingen.
Zorg voor een goed systeem voor overzicht van behandelingen en afspraken.

Radiation Oncology Safety Education and Information System (ROSEIS)

Wat is ROSEIS?

ROSEIS is een vrijwillige, webgebaseerde databank voor het melden en leren van incidenten en bijna-incidenten binnen de radiotherapie.

Doelstellingen en functies:

1. Kan gebruikt worden als een lokaal meld- en leersysteem binnen afdelingen, en helpt bij het voldoen aan wettelijke vereisten.
2. Bevordert breder leren door incidentinformatie anoniem te delen via het platform.
3. Radiotherapieteams kunnen incidenten en corrigerende maatregelen anoniem rapporteren.
4. Dient als een forum voor het uitwisselen van veiligheidsinformatie binnen de radiotherapiecommunity.

www.estro.org

Introducing ROSEIS: Advancing Safety and Quality in Radiation Oncology

At the ESTRO Congress 2025 in Vienna, the ESTRO ROSQ Committee (Radiation Oncology Safety and Quality) proudly launched the Radiation Oncology Safety Education and Information System, or ROSEIS.

Radiotherapy incidents, although rare, can have serious consequences. Yet too often, valuable information remains isolated within individual departments, missing opportunities to learn and prevent injury to future patients. ROSEIS was developed to change that by creating a shared, proactive space for safety learning and quality improvement across the radiotherapy community.

Why was ROSEIS created?

ROSEIS was created to enable the sharing of information on incidents and near incidents in a safe environment to increase learning and improve the quality and safety of practice across European centres.

The EU Directive 2013/59/EURATOM mandates that radiotherapy centres implement a reporting and learning system for incidents, and the ESTRO ROSEIS enables centres without an existing reporting system to comply with this directive by providing a platform for reporting, reviewing, and anonymously sharing safety data across the radiotherapy community.

ESTRO

Corporate Members E-Library Hi P Sig

About ESTRO Membership School Workshops C

What's new?

The upgraded ROSEIS platform now supports reporting and tracking of:

- Software alerts
- Cyberthreats

These new features respond to evolving challenges in radiotherapy and ensure the platform remains a forward-looking safety tool.

Get involved

https://roseis.estro.org/

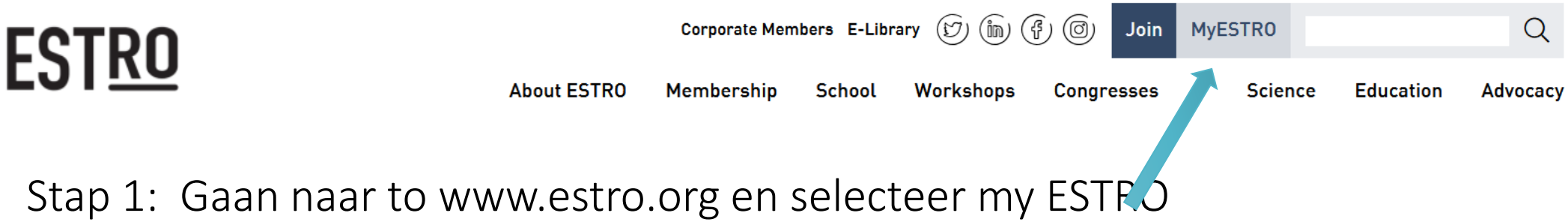
We invite all radiotherapy professionals to start using ROSEIS today — whether your centre is new to reporting or looking to contribute to the broader safety dialogue. Your reports, suggestions, and shared experiences are essential to building a safer community.

📽️ Watch the introduction video to discover how ROSEIS works and how your centre can benefit from using the platform.

📘 Read the user manual for step-by-step guidance on how to report, search, and navigate the system effectively.

By the ROSEIS Working Group of the ESTRO ROSQ Committee

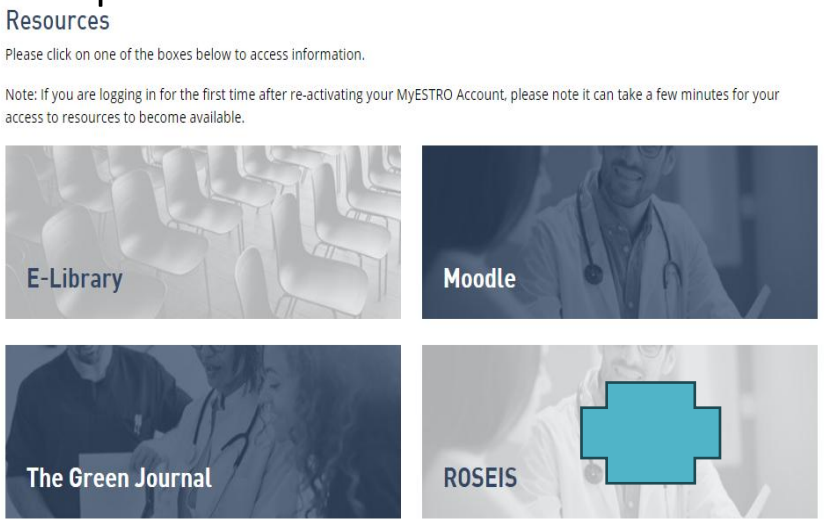
Radiation Oncology Safety Education and Information System (ROSEIS) Reporting an incident



Stap 1: Gaan naar to www.estro.org en selecteer my ESTRO

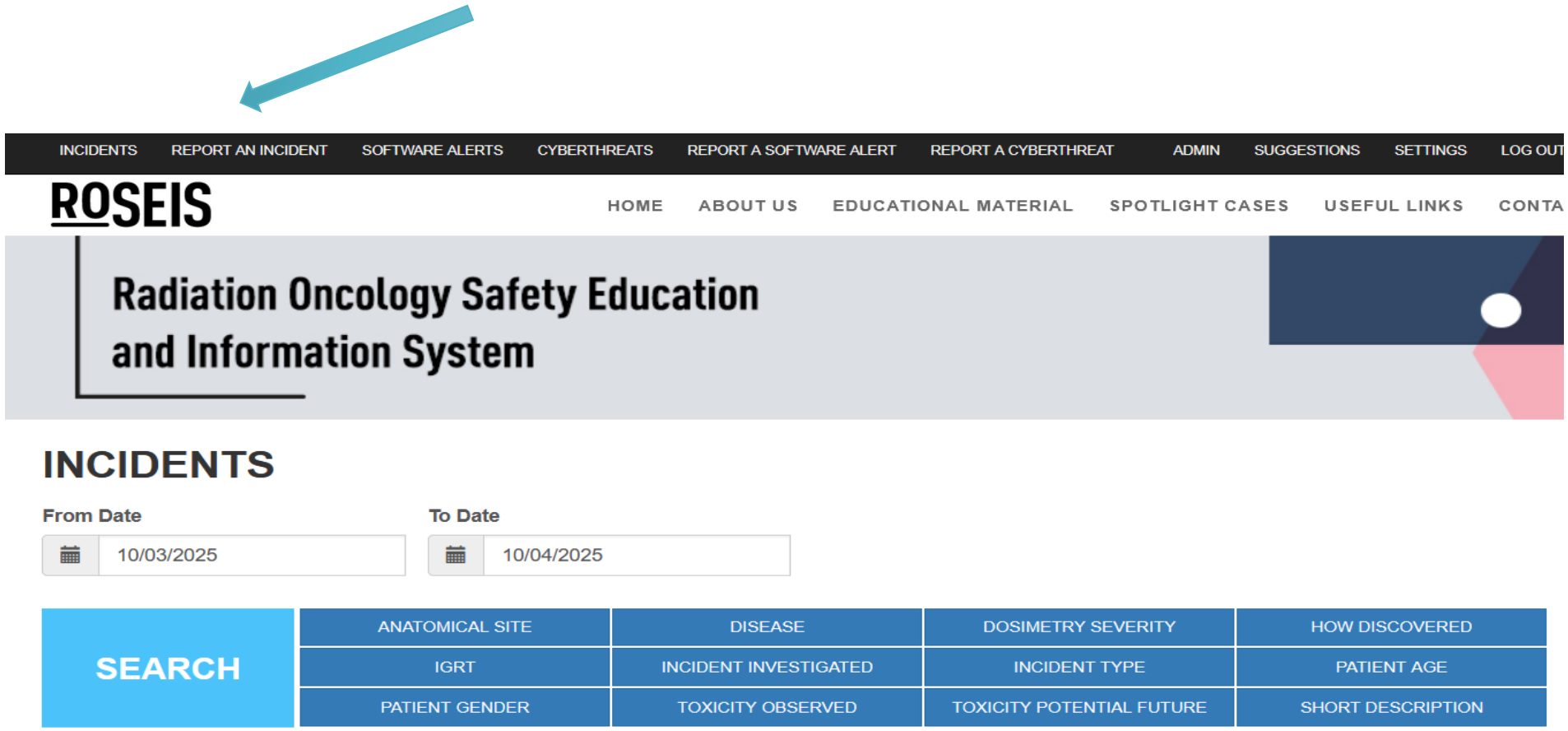
Stap 2: Click on Resources

Stap 3: Click on ROSEIS



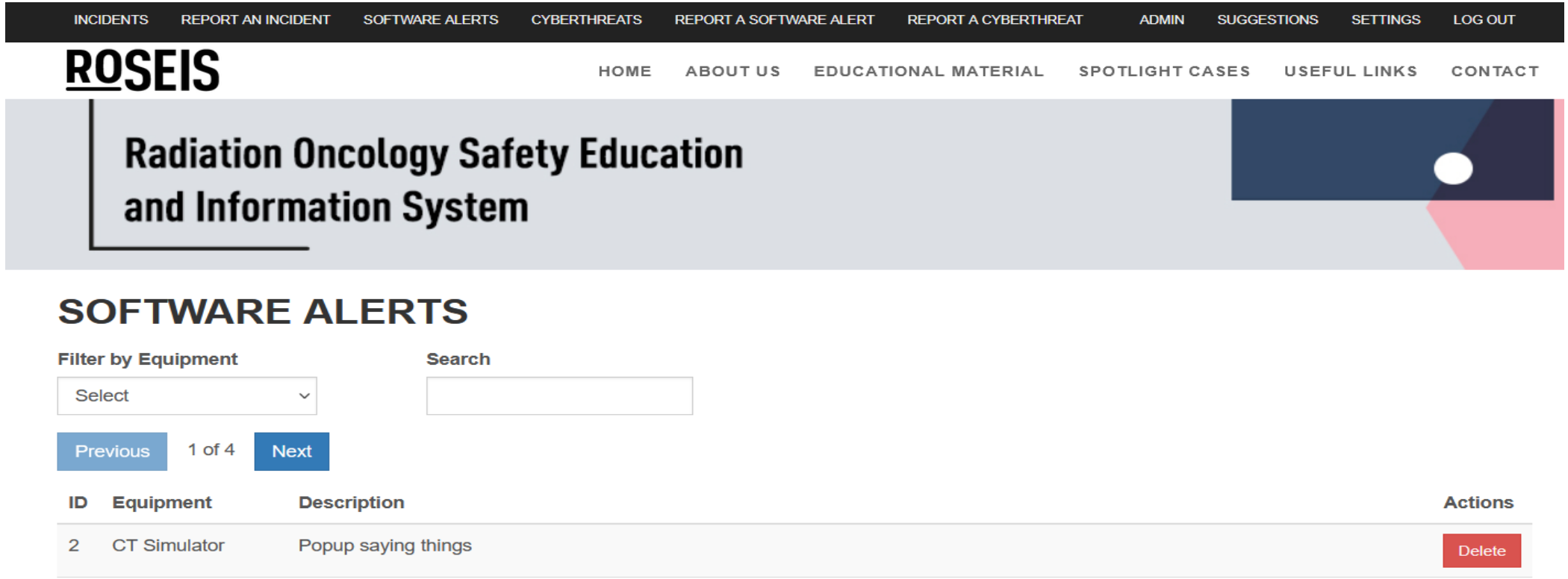
Radiation Oncology Safety Education and Information System (ROSEIS) Reporting an incident

Stap 4: Report an incident



Radiation Oncology Safety Education and Information System (ROSEIS) Additional resources

Reporting an ALERT

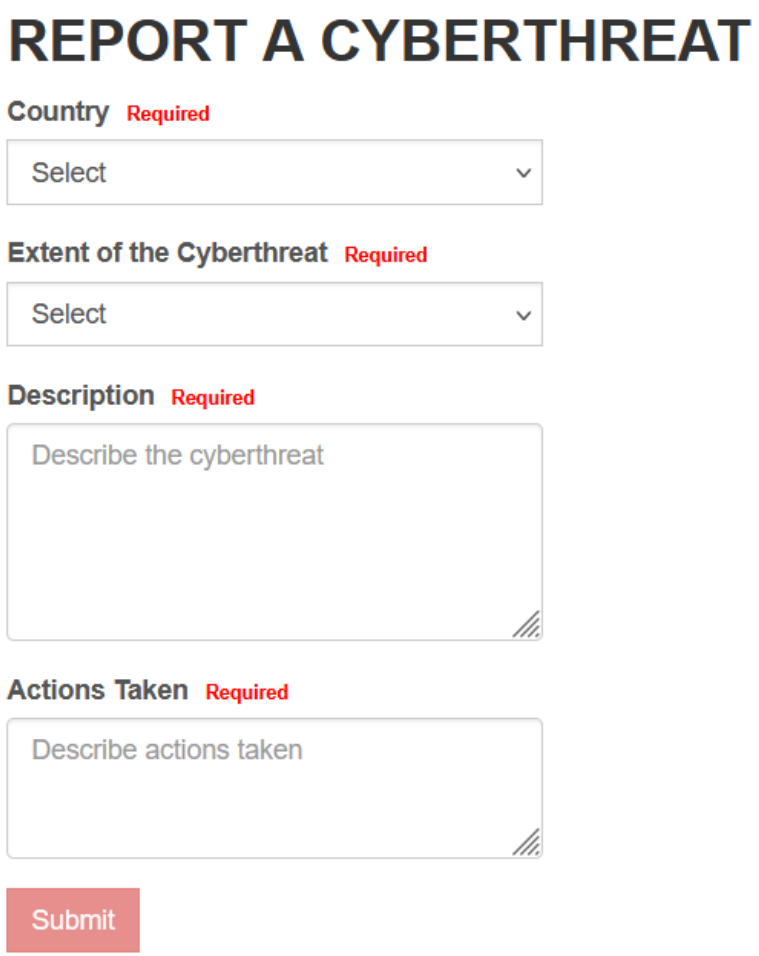


ALERTS "Waarschuwingen zijn vaak onbegrijpelijk en kunnen afleidend werken."

Radiation Oncology Safety Education and Information System (ROSEIS) Additional resources

Reporting a Cyberthreat

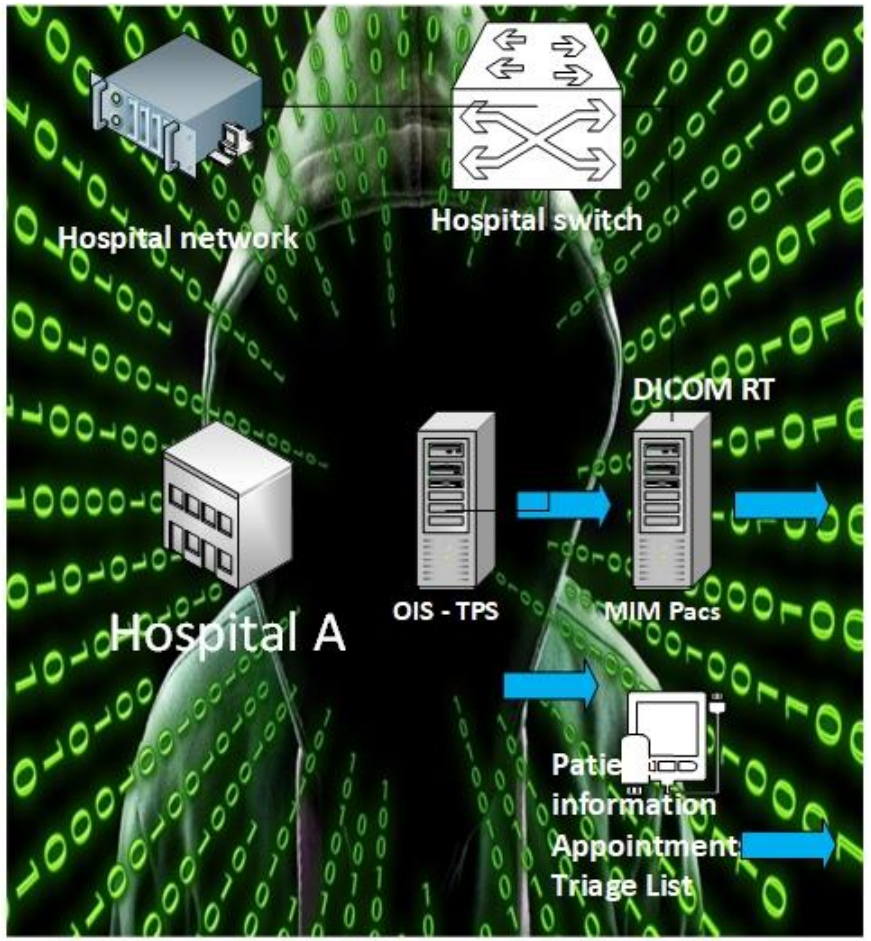
DOEL :
Leren van elkaar!!! En delen van informatie



Tips vanuit ervaringen :

Selecteer patienten cathegorien

Priority Level	Treatment Group	**Level 1 –** 80% capacity or above	**Level 2 –** Less than 80% capacity	**Level 3 –** Less than 50% capacity	**Level 4 –** Less than 25% capacity	**Level 5 –** Less than 10% capacity
1	Patients with an urgent need for radiotherapy (e.g. spinal cord compression)					
	Radical radiotherapy with curative intent for patients with more rapidly growing tumours i.e. head and neck or radical cervix patients either on treatment or about to start treatment					
	Patients already on treatment (Category 1)					
	Paediatrics patients					
2	Radical radiotherapy for all other patients					
	Adjuvant post-operative treatment for aggressive tumours (e.g. head and neck) or patients with known residual disease post-operative & SABR					
3	All other adjuvant treatments (e.g. breast) and radical radiotherapy for prostate cancer					
4	Palliative radiotherapy and SABR for oligometastases					
5	Radioactive iodine (RAI) for thyroid cancer patients and Radium 223 treatment					
6	Low grade malignant e.g. BCC or benign disease e.g. thyroid disease					



Belgische oplossing: via MIM software

Meer info in presentatie van Koen

Robert S. Mueller, III, former Director of the FBI

Met dank aan Samuel Peeters voor gebruik van presentatie