Mitigation and Management of Cyberattacks

From a Radiotherapy Perspective

An ESTRO ROSQ Committee project

Kantonsspital
St.Gallen

Agenda

- What is a cyber-attack?
- Actual threat situation
- How cyber-attacks work
- How is patient treatment affected?
- Preparedness and Business Continuity Management
- Summary and Outlook

What is a cyber-attack?

- "A cyberattack is any intentional effort to steal, expose, alter, disable, or destroy data, applications, or other assets through unauthorized access to a network, computer system or digital device." (IBM)
- Usually, the attacker seeks some type of benefit from disrupting the victim's systems
- Types of most common cyber-attacks
  - Malware (spyware, **ransomware**, viruses, worms, Trojan horses)
  - Phishing
  - Denial-of-service attack
  - Zero-day exploit
  - SQL injection
  - Man-in-the-Middle attacks

Actual threat situation

- Worldwide
  - In 2023: a cyberattack took place every 39 seconds, which translates into over 2,200 cases per day[1]
  - global cost of cybercrime $8.4 trillion in 2022[2]
- Healthcare:
  - In 2023 over 725 major data breaches (500+ records) in the US[3]
  - in 2023 average cost of $11 million per data breach[4]

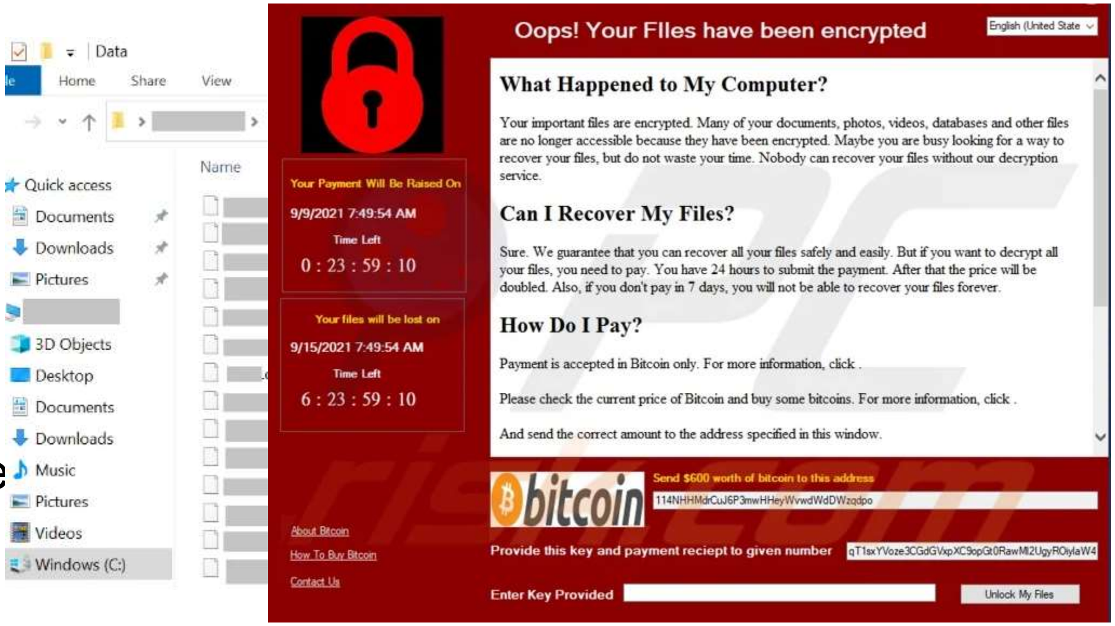
[1] https://www.watchguard.com/wgrd-news/blog/there-was-cyberattack-every-39-seconds-2023#:~:text=According%20to%20a%20study%20by,incident%20occurred%20every%2044%20seconds.

[2] https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/

[3] https://www.hipaajournal.com/security-breaches-in-healthcare/#:~:text=Report%3A%20Security%20Breaches%20in%20Healthcare&text=An%20unwanted%20record%20was%20set,breaches%20set%20the%20previous%20year.

[4] https://www.weforum.org/agenda/2024/02/healthcare-pays-the-highest-price-of-any-sector-for-cyberattacks-that-why-cyber-resilience-is-key/ -

How cyber-attacks work



Oops! Your FIles have been encrypted

Your Payment Will Be Raised On

9/9/2021 7:49:54 AM

Time Left

0 : 23 : 59 : 10

Your files will be lost on

9/15/2021 7:49:54 AM

Time Left

6 : 23 : 59 : 10

What Happened to My Computer?

Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But if you want to decrypt all your files, you need to pay. You have 24 hours to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you will not be able to recover your files forever.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click .

Please check the current price of Bitcoin and buy some bitcoins. For more information, click .

And send the correct amount to the address specified in this window.

Send $600 worth of bitcoin to this address

114NHHMdrCuJ6P3mwHHeyWvwdWdDWzqdpo

About Bitcoin

How To Buy Bitcoin

Contact Us

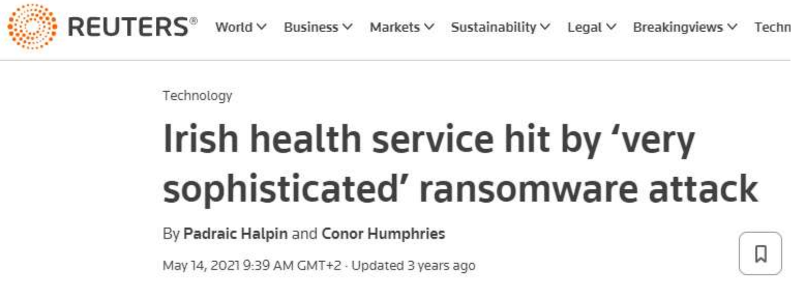
Provide this key and payment reciept to given number qT1sxYVoze3CGdGVxpXC9opGt0RawMI2UgyROiylaW4

Enter Key Provided

Unlock My Files

- Exemplified by a ransomware attack
- Ransomware:
  - encryption of data, so it cannot be
  - Data loss or Data breach
- Process:
  - A phishing-mail is received and the link or infected attachment opened
  - Attackers have now access to the system and install the malware
  - Malware (encryption Trojan) spreads over the network to gather information
  - Systems are infected by the ransomware
  - Encryptions of systems (DBs, Data) starts: no more access to the data
  - Message appears asking for ransom (e.g. bitcons)
  - As no access to data → no treatment, no information on patients

How cyber-attacks work – example 1


REUTERS® World Business Markets Sustainability Legal Breakingviews Techn

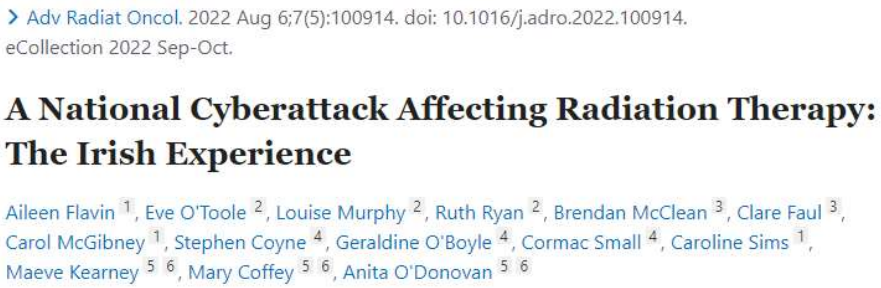
Technology

Irish health service hit by 'very sophisticated' ransomware attack

By Padraic Halpin and Conor Humphries

May 14, 2021 9:39 AM GMT+2 · Updated 3 years ago

https://www.reuters.com/technology/irish-health-service-hit-by-ransomware-attack-vaccine-rollout-unaffected-2021-05-14/

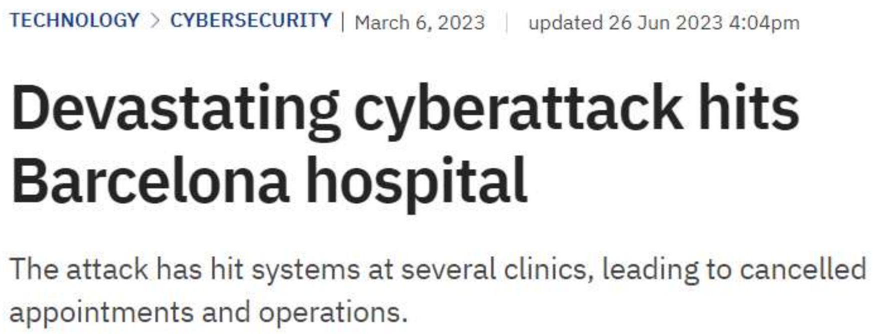

Adv Radiat Oncol. 2022 Aug 6;7(5):100914. doi: 10.1016/j.adro.2022.100914. eCollection 2022 Sep-Oct.

A National Cyberattack Affecting Radiation Therapy: The Irish Experience

Aileen Flavin [1], Eve O'Toole [2], Louise Murphy [2], Ruth Ryan [2], Brendan McClean [3], Clare Faul [3], Carol McGibney [1], Stephen Coyne [4], Geraldine O'Boyle [4], Cormac Small [4], Caroline Sims [1], Maeve Kearney [5] [6], Mary Coffey [5] [6], Anita O'Donovan [5] [6]

- Refused to pay ransom ($ 20M)
- All IT systems taken down (preventively)
- All linacs and TPS terminals shut down
- No internet connection (email, phone)
- No access to patient information, contact details, medical record
- Build up isolated network
  - Operational linacs on day 4, 6, 11 and 14
  - Replanning
  - Gap compensation
- Decryption tool received; full restoration took more than 4 month

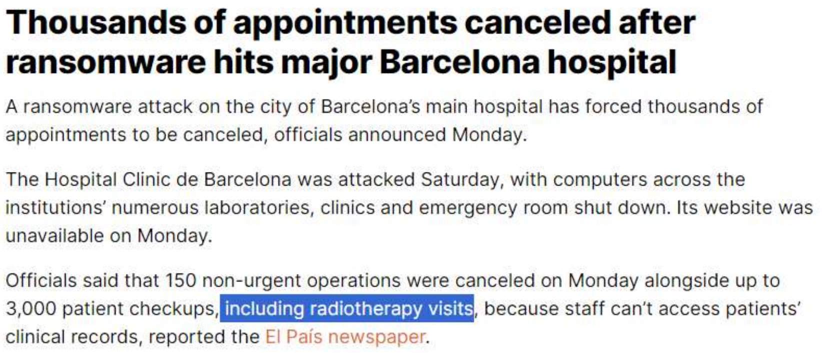
How cyber-attacks work – example 2



TECHNOLOGY > CYBERSECURITY | March 6, 2023 | updated 26 Jun 2023 4:04pm

Devastating cyberattack hits Barcelona hospital

The attack has hit systems at several clinics, leading to cancelled appointments and operations.



Thousands of appointments canceled after ransomware hits major Barcelona hospital

A ransomware attack on the city of Barcelona's main hospital has forced thousands of appointments to be canceled, officials announced Monday.

The Hospital Clinic de Barcelona was attacked Saturday, with computers across the institutions' numerous laboratories, clinics and emergency room shut down. Its website was unavailable on Monday.

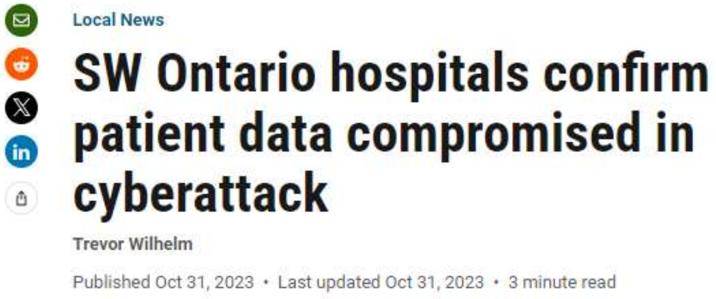
Officials said that 150 non-urgent operations were canceled on Monday alongside up to 3,000 patient checkups, including radiotherapy visits, because staff can't access patients' clinical records, reported the El País newspaper.

https://techmonitor.ai/technology/cybersecurity/barcelona-hospital-cyberattack
https://therecord.media/barcelona-hospital-ransomware-spain

- Refused to pay the ransom!
- All virtual servers down
- Access to ROIS not possible, not even Linacs (vendor support weak)
- All patient sent to enamouring hospitals
  - Status for treatment unclear, full replanning
- After 12 days: systems fully restored; work back to normal

Information provided by Jordi Saez, MP at Hospital Clínic de Barcelona

How cyber-attacks work – example 3

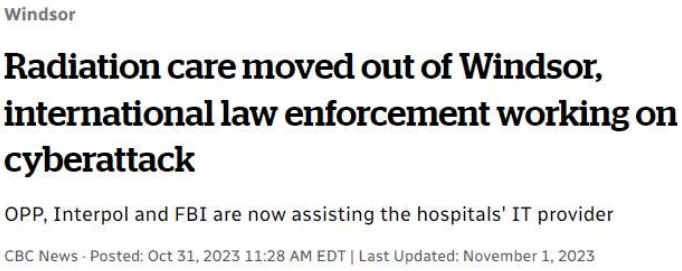


Local News

SW Ontario hospitals confirm patient data compromised in cyberattack

Trevor Wilhelm

Published Oct 31, 2023 • Last updated Oct 31, 2023 • 3 minute read



Windsor

Radiation care moved out of Windsor, international law enforcement working on cyberattack

OPP, Interpol and FBI are now assisting the hospitals' IT provider

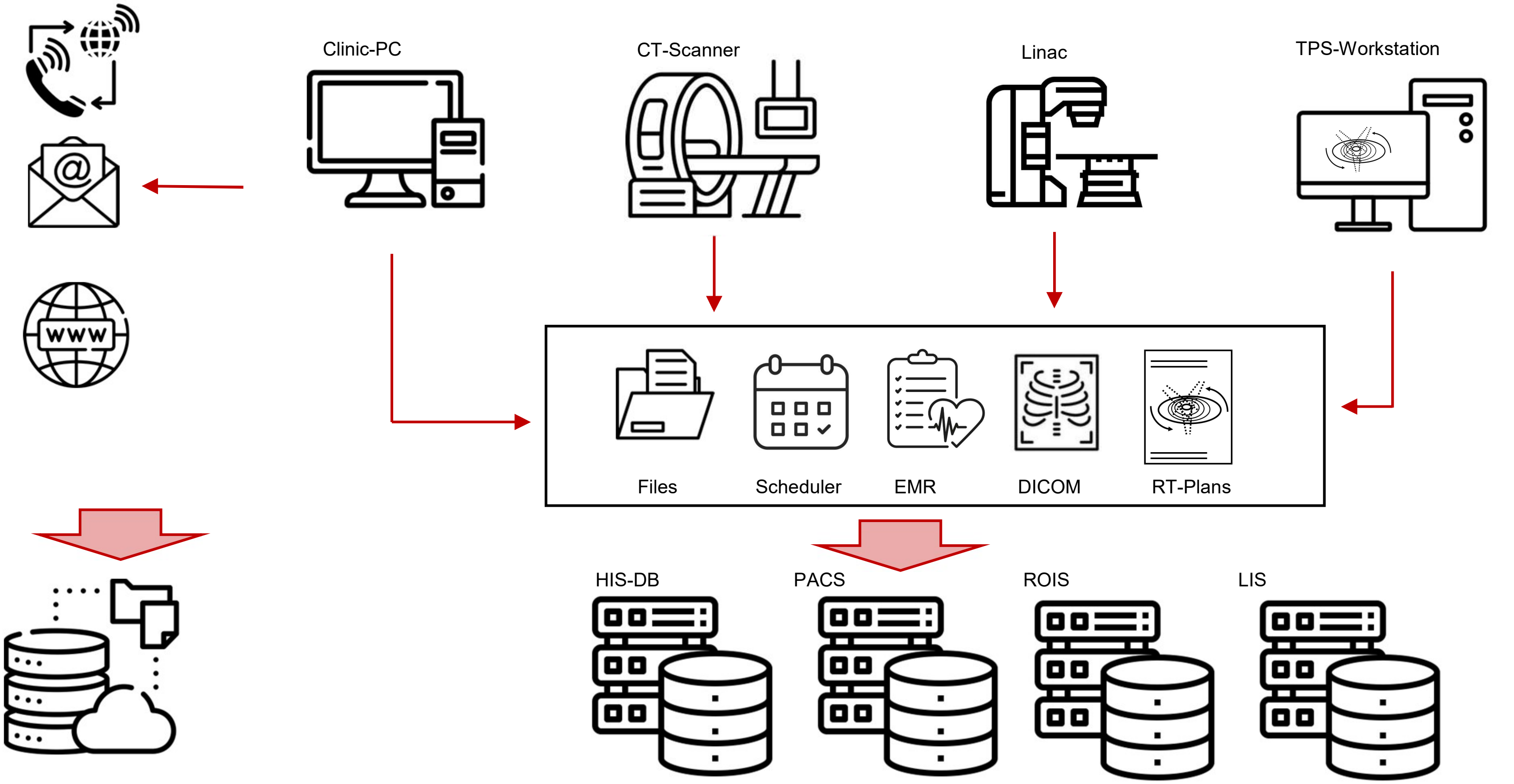
CBC News · Posted: Oct 31, 2023 11:28 AM EDT | Last Updated: November 1, 2023

https://windsorstar.com/news/local-news/southwestern-ontario-hospitals-confirm-patient-data-compromised-in-cyberattack
https://www.cbc.ca/news/canada/windsor/windsor-regional-hospital-radiation-cyberattack-1.7020989

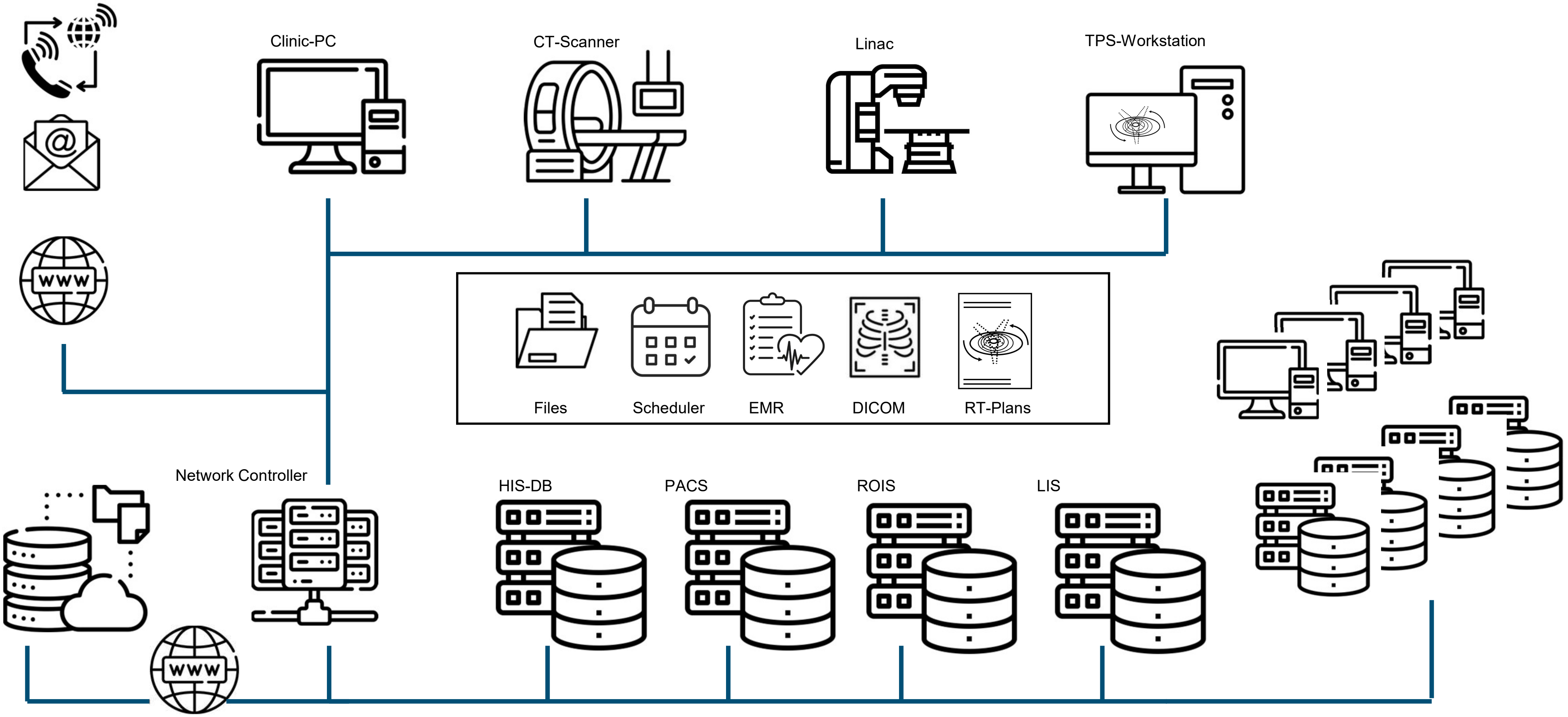
- Refused to pay the ransom of $ 8M
- Disruption of internet, Wi-Fi, email, phones
- Impact on radio-therapy:
  - No planning, delivery, documentation …
- Patients referred throughout the province (2 – 4 h travel!)
- After 6 weeks:
  - planning and treatment possible; no email and internet

Information provided by Brian liszewski, RTT at Windsor Regional Cancer Centre

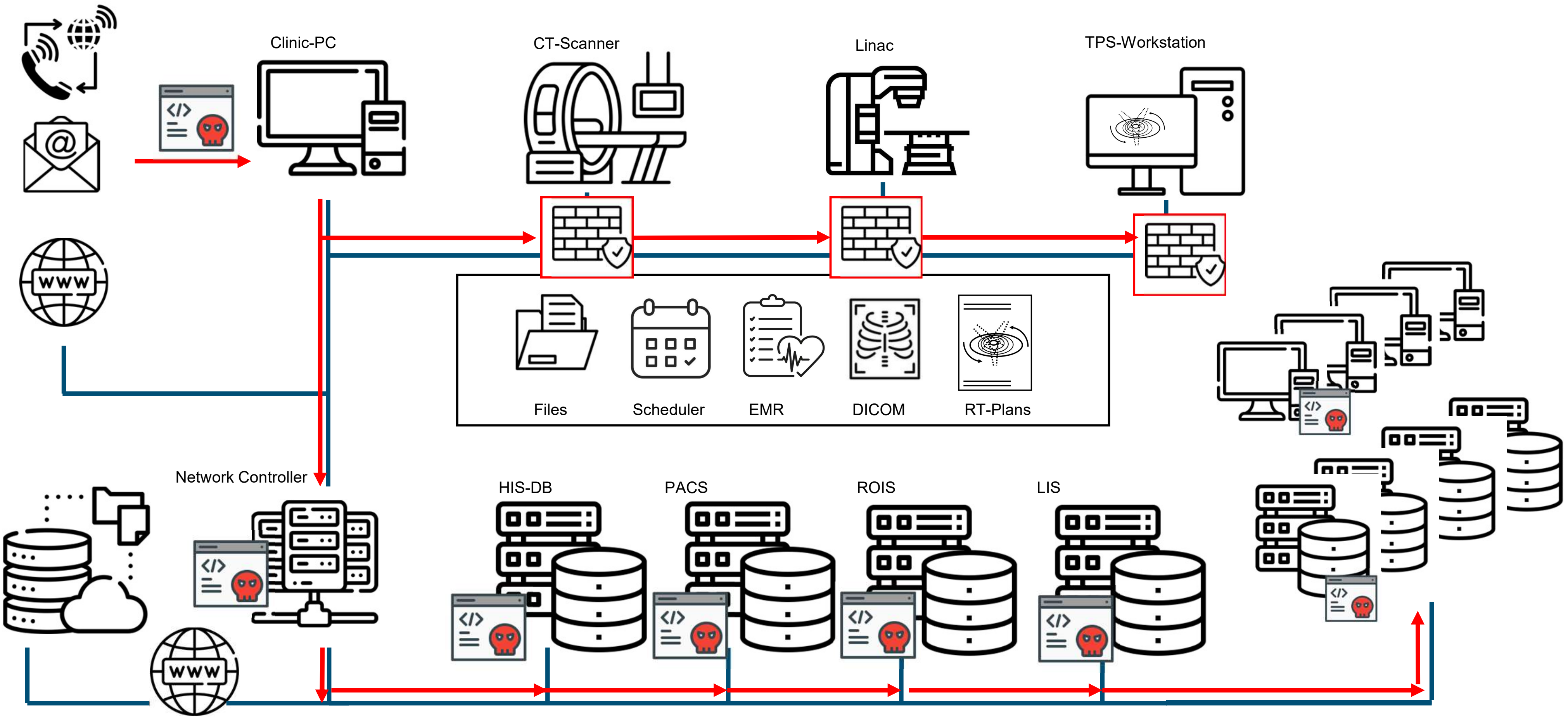
How a cyber-attack effects RO treatment



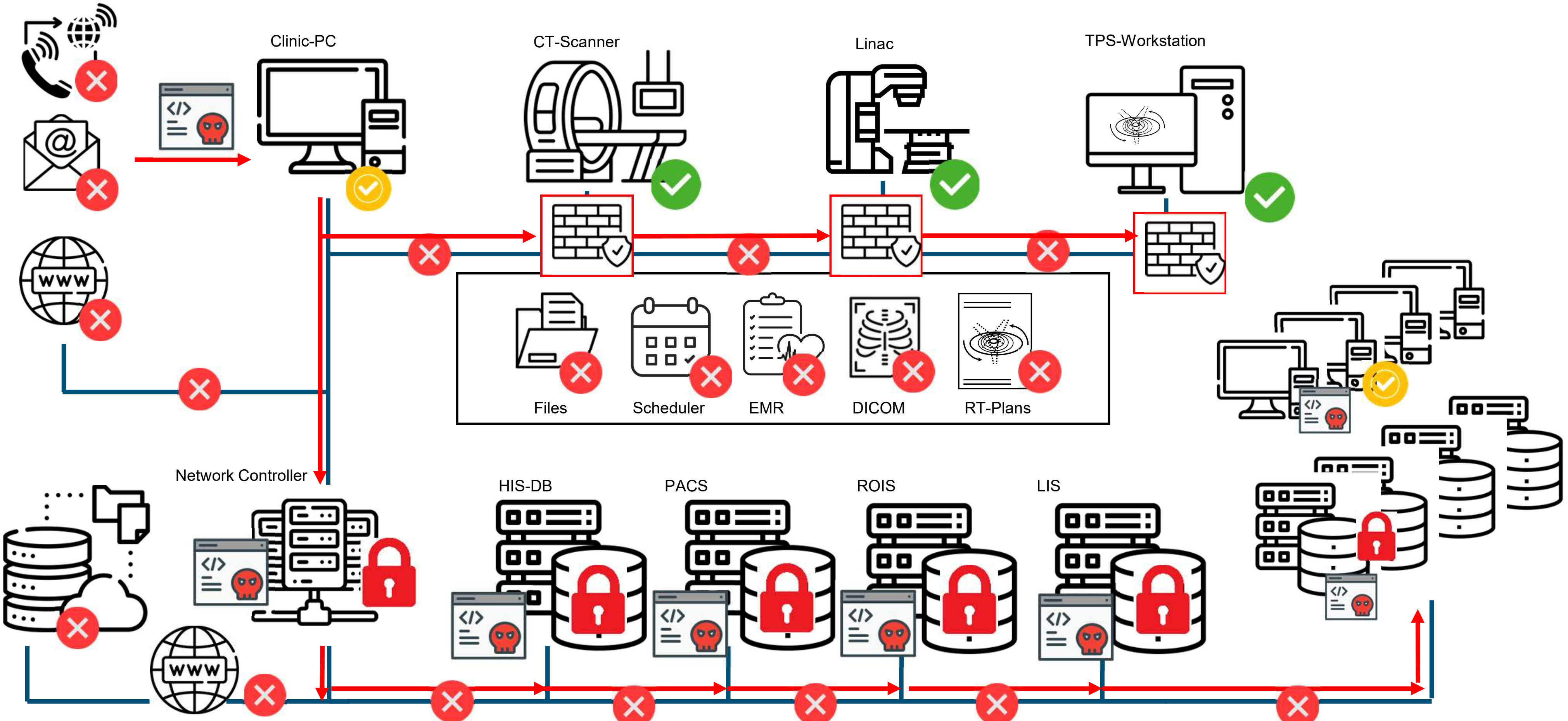
How a cyber-attack effects RO treatment



How a cyber-attack effects RO treatment



How a cyber-attack effects RO treatment



How a cyber-attack effects RO treatment

- Once a cyber-attack has happened:
  - No access to EMR!
  - No access to appointment scheduler!
  - No access to treatment plans!
  - No treatment possible!

→ What can we do?

→ How can treatment of patients be continued?

→ For how long can patients wait?

Solution 0 – Rebuild the whole infrastructure

- No Backups or hard copies available:
  - Try to find out which patients currently under treatment
  - Try to find out the treatment regime for each patient
  - Estimate applied dose to patients (on what basis?)
  - Need to rebuild all systems and DBs from scratch
  - Re-measure beam data

→ **Difficult and very time consuming!**

Solution 1 – Pay the ransom

- Easiest way!
- Back to normal very soon
- BUT:
  - Expensive
  - Legally questionable, who is accountable?
  - No guarantee the encryption key is handed out or works!
  - No guarantee the malware is fully removed!

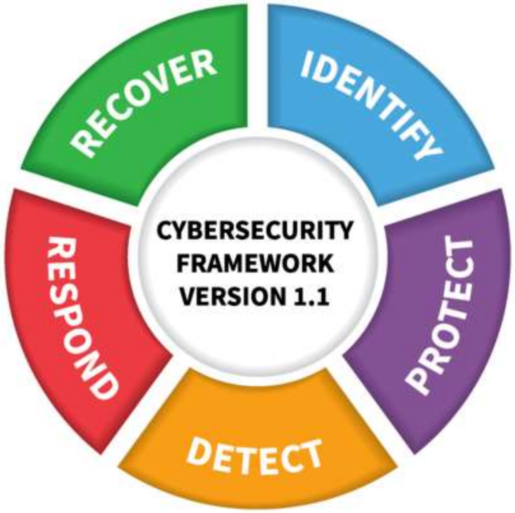
→ Definitively not recommended!

(Only) Solution 2 – Preparedness!

- Basics of preparedness:
  - Awareness
  - Incident response team (IRT)
  - Business Continuity Plan (BCP)
  - Functional backup solution
- Follow 6 Steps
  - 1. Preparation, 2. Prevention (Pre-Incident-Phase)
  - 3. Detection, 4. Respond, 5. Recover (Incident-Phase)
  - 6. Debriefing & Con. Improvement (Post-Incident-Phase)

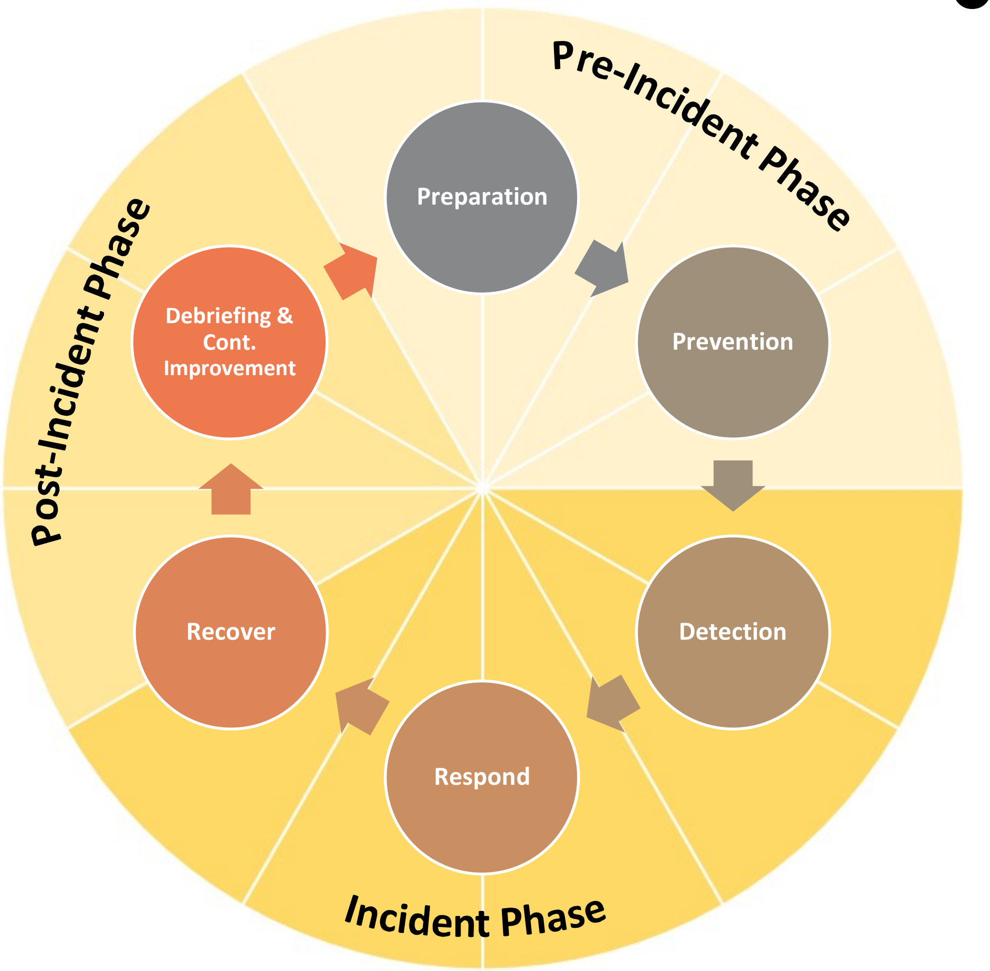
→ **All are needed!**

NIST-CSF

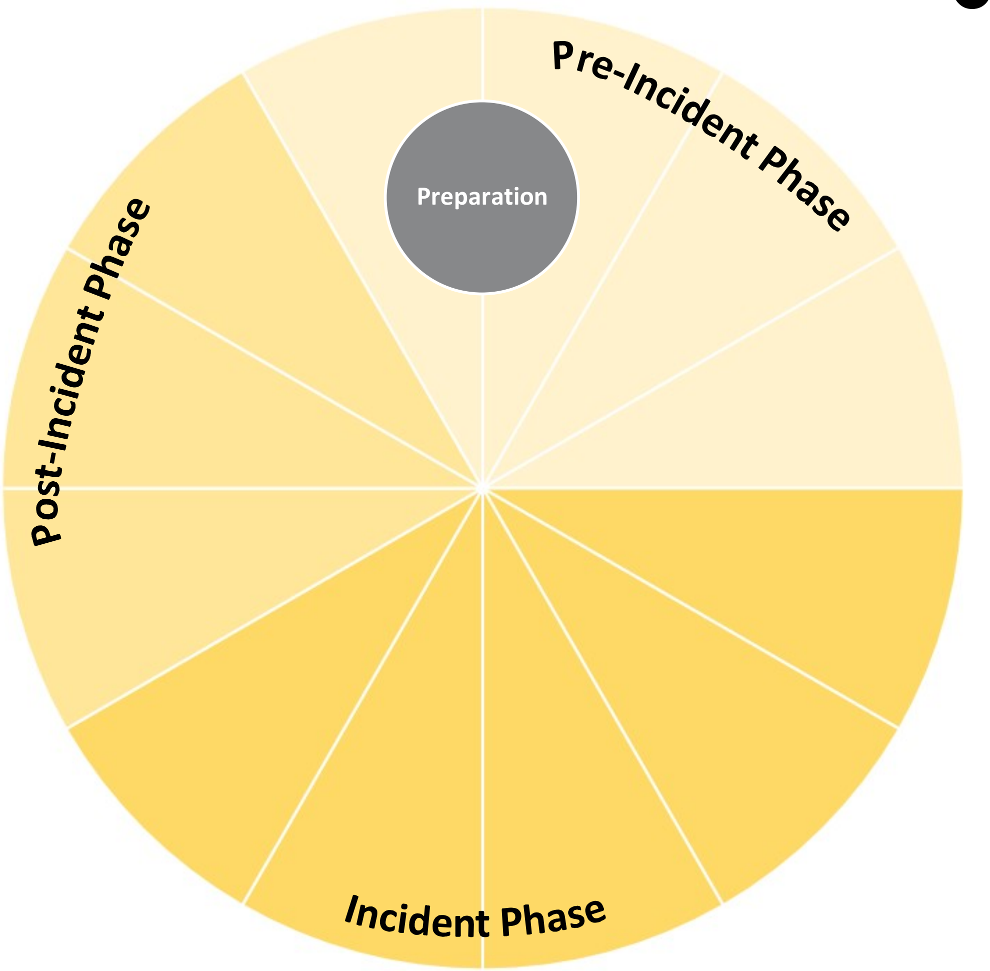


https://www.nist.gov/cyberframework

6 Steps

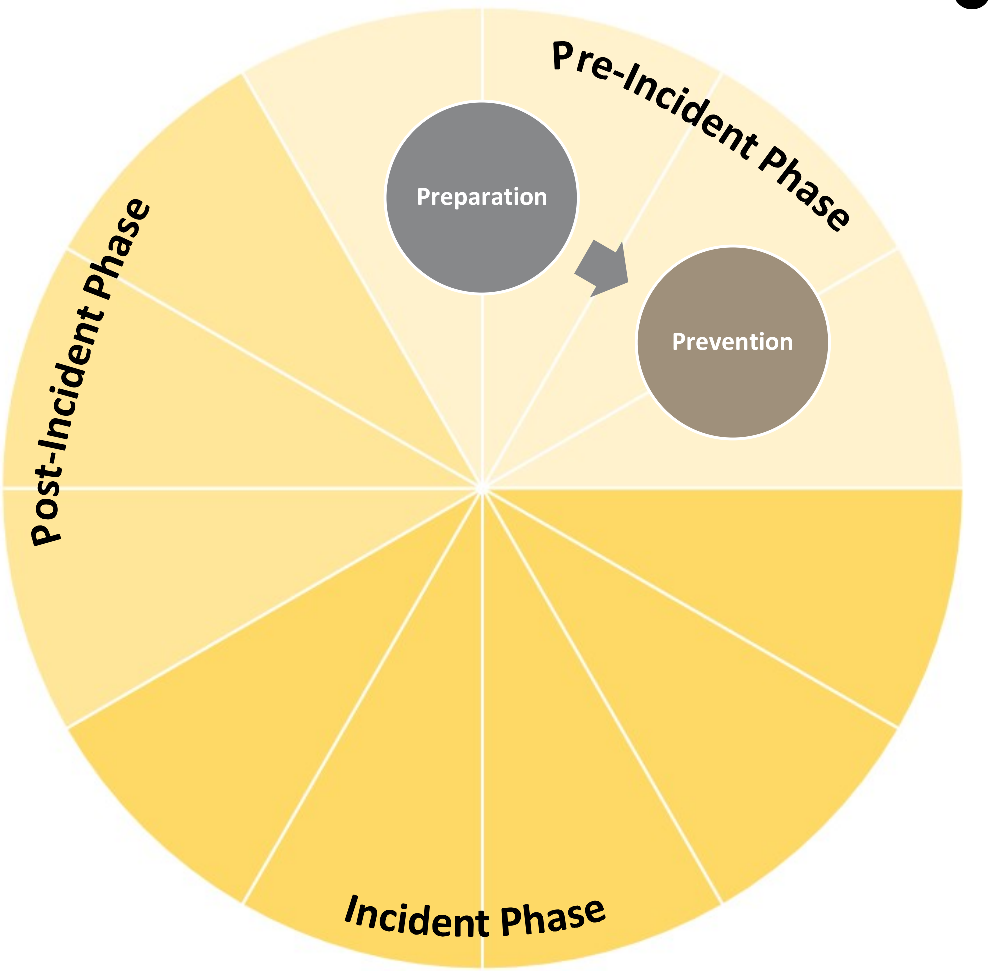

Pre-Incident Phase
Preparation
Prevention
Detection
Respond
Recover
Debriefing & Cont. Improvement
Incident Phase
Post-Incident Phase

6 Steps



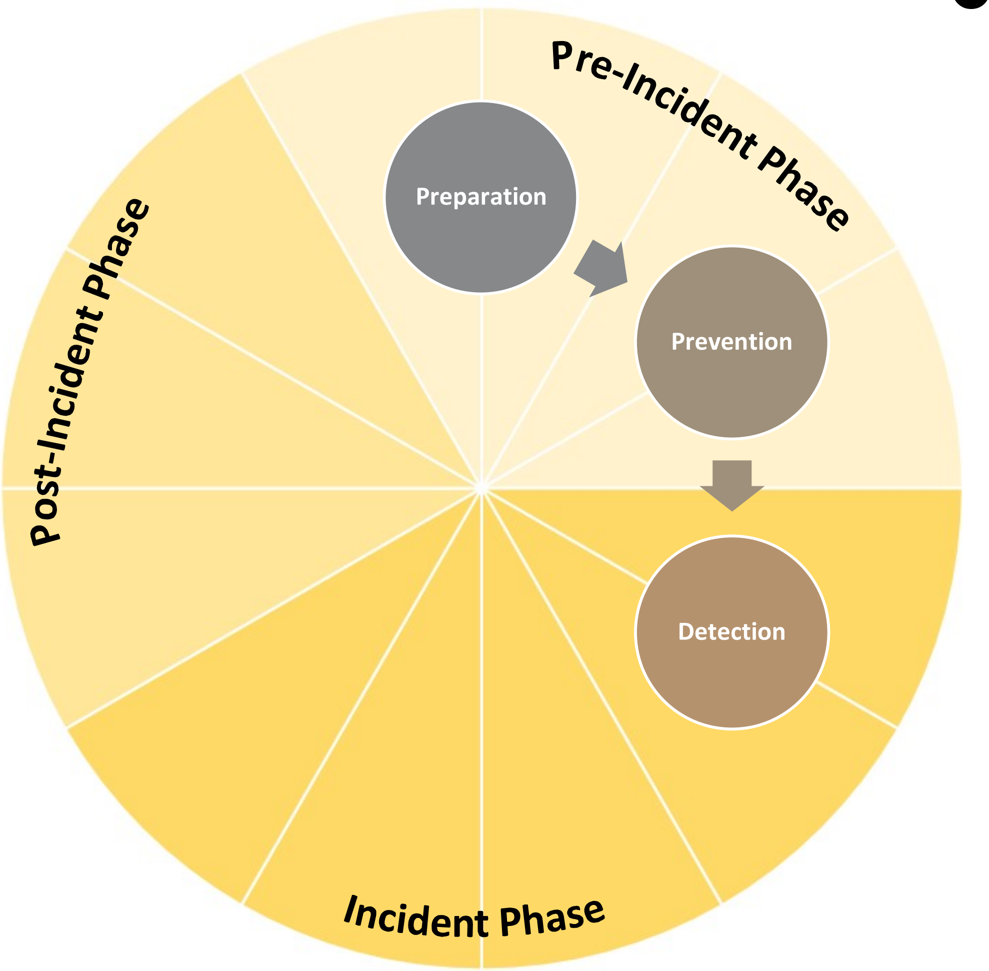
- Identification of **systems, tools, processes and stakeholders** to be affected by a cyber-attack
- Define a **business continuity plan (BCP)** and ensure it is in place and known for the organisation
- Define personnel with specific roles and responsibilities including **incident response team**

6 Steps



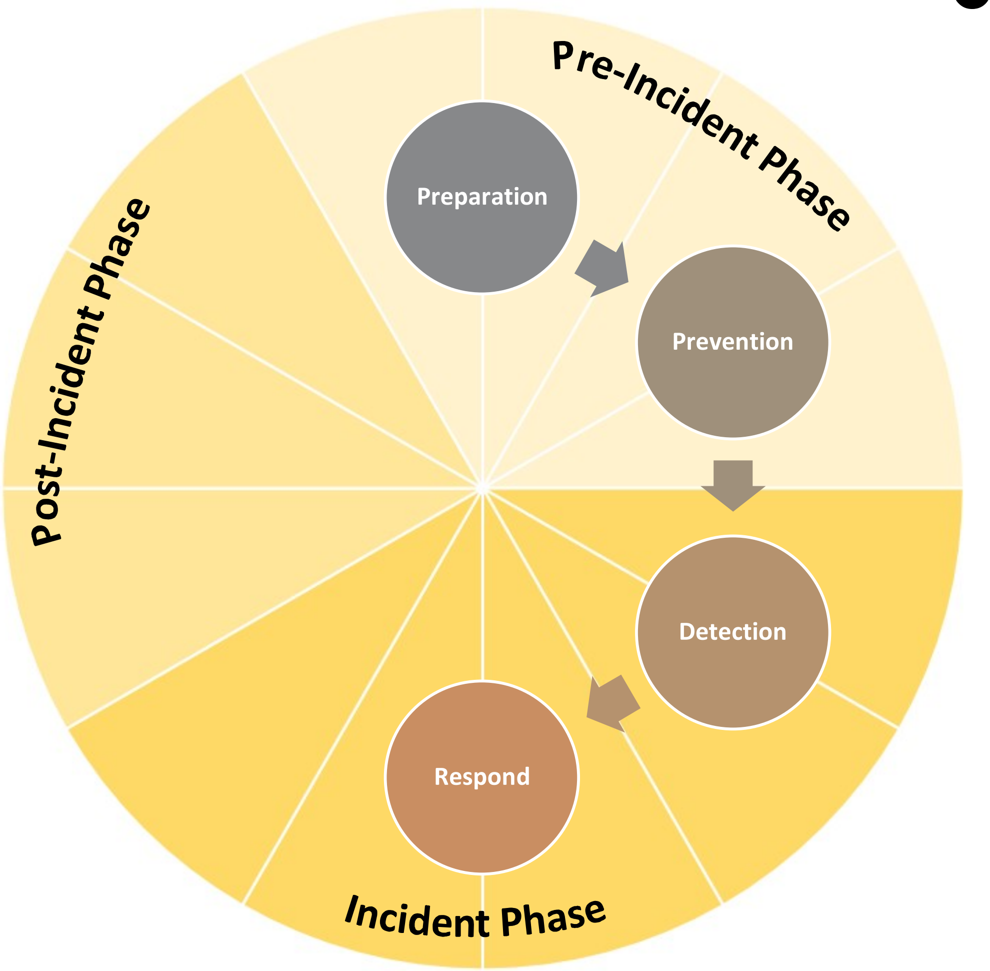
- Ensure **user awareness** and training in cyber security at all levels of the organisation
- **Technical measures**:
  - Conduct system patching
  - Ensure appropriate endpoint protection
  - Safeguard network architecture
  - stringent user management (incl. password policy, multi factor identification)
- **Protect data** (encryption, storage/archiving)
- Implement physical and remote **access restrictions**
- Hold **backups and hard copies**
- Conduct **regular testing** of reaction, response and recovery plans

6 Steps



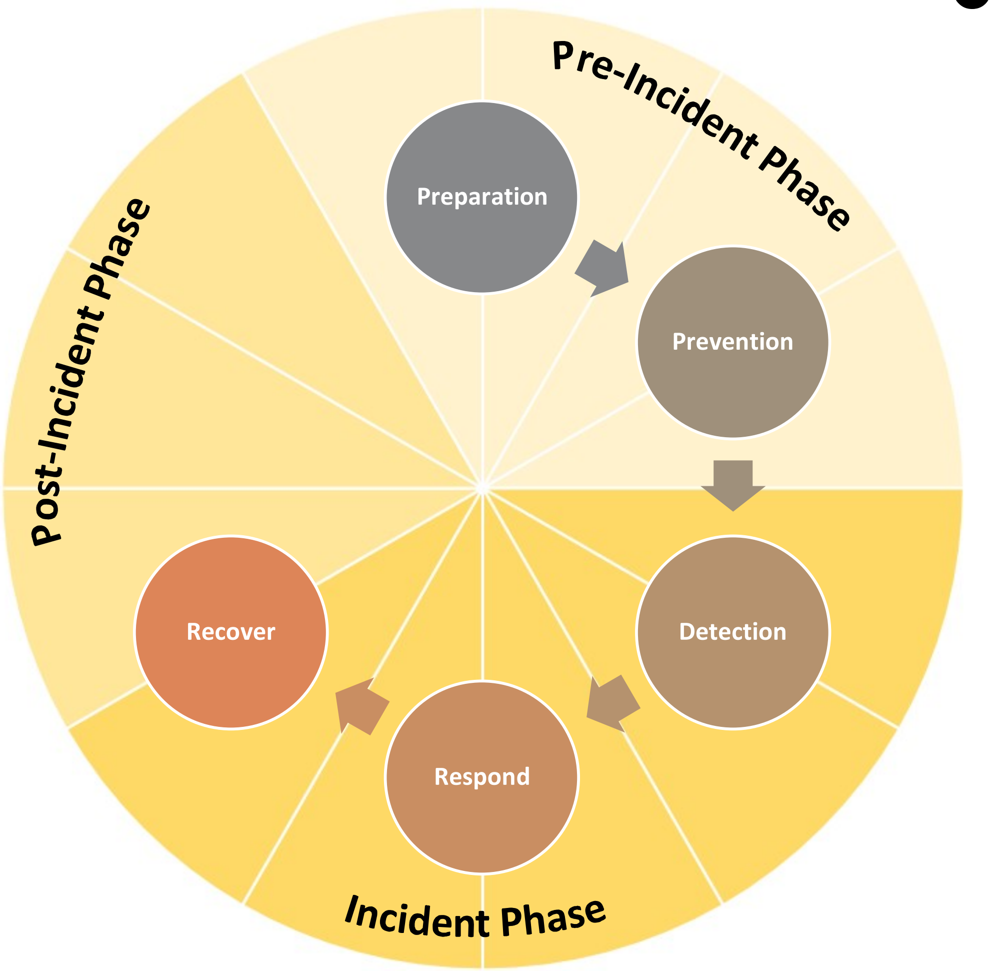
- Ensure **real time detection tools** (monitoring and logging, for malicious code and unauthorized access) are in place
- **Inform the incident response team** (communication process, automatic alerts) through the pre-defined crisis communication plan
- **Identify** the impact of the affected systems and data

6 Steps



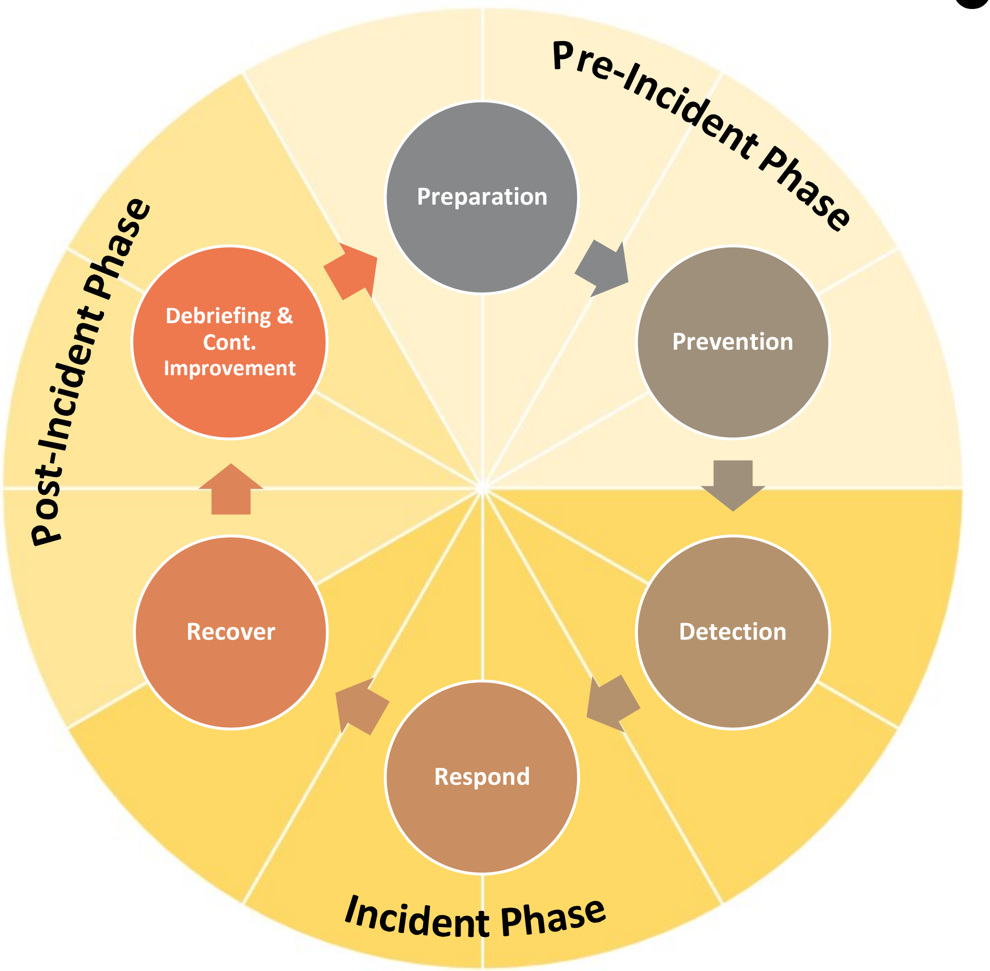
- Activate **business continuity plan** (BCP)
- **Isolate infected systems/data/network** ranges or segments immediately
- **Remediate the vulnerabilities** that have been exploited
- Implement **procedures regarding cyberattack** handling
  - **Inform** stakeholders according to communication plan
  - **continue treatment** on-site or redirect patients elsewhere
  - **documentation** of all activities

6 Steps



- Define when to **activate recovery plan**
- Determine which **recovery method** is to be used
- **Check recovered data** for completeness and correctness
- **Communicate** regularly (internal, external incl. public relations/press)
- **Define end** of the recovery and resume normal business activities

6 Steps



- **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

Cyber-attack response plan - summary

- Threat is real – ransom attack on hospitals are on the rise!
- Be prepared by having an **Incident Response Team** and a **Business Continuity Plan**
- Review the procedures regularly with all stakeholders
- Collaboration with neighboring hospitals
- Practical aspects:
  - Make sure you have a **valid backup solutions** (offline, paper-based, cloud)
  - Make sure you have a **valid contingency treatment procedure**
  - Make sure you have a good system for **treatment and appointments overview**
  - Make sure you have access to linacs/CTs/other devices **in an offline mode**

Outlook

- ESTRO ROSQ Committee
  - Project: “Cyberattack, preventative measures and emergency response”

    → Develop guidelines on prevention and mitigation in the event of a successful attack

Petra Reijnders, Anita O'Donovan, Mary Coffey, Philippe Maingon,
Brian Liszewski, Geoff Delaney, Amanda Cassie, Sophie Perryck, Aileen Flavin, Ali
Dabach, Eric Messens, Baoshe Zhang, Marcello Bellini, Peter Fischer, Gert Frenken

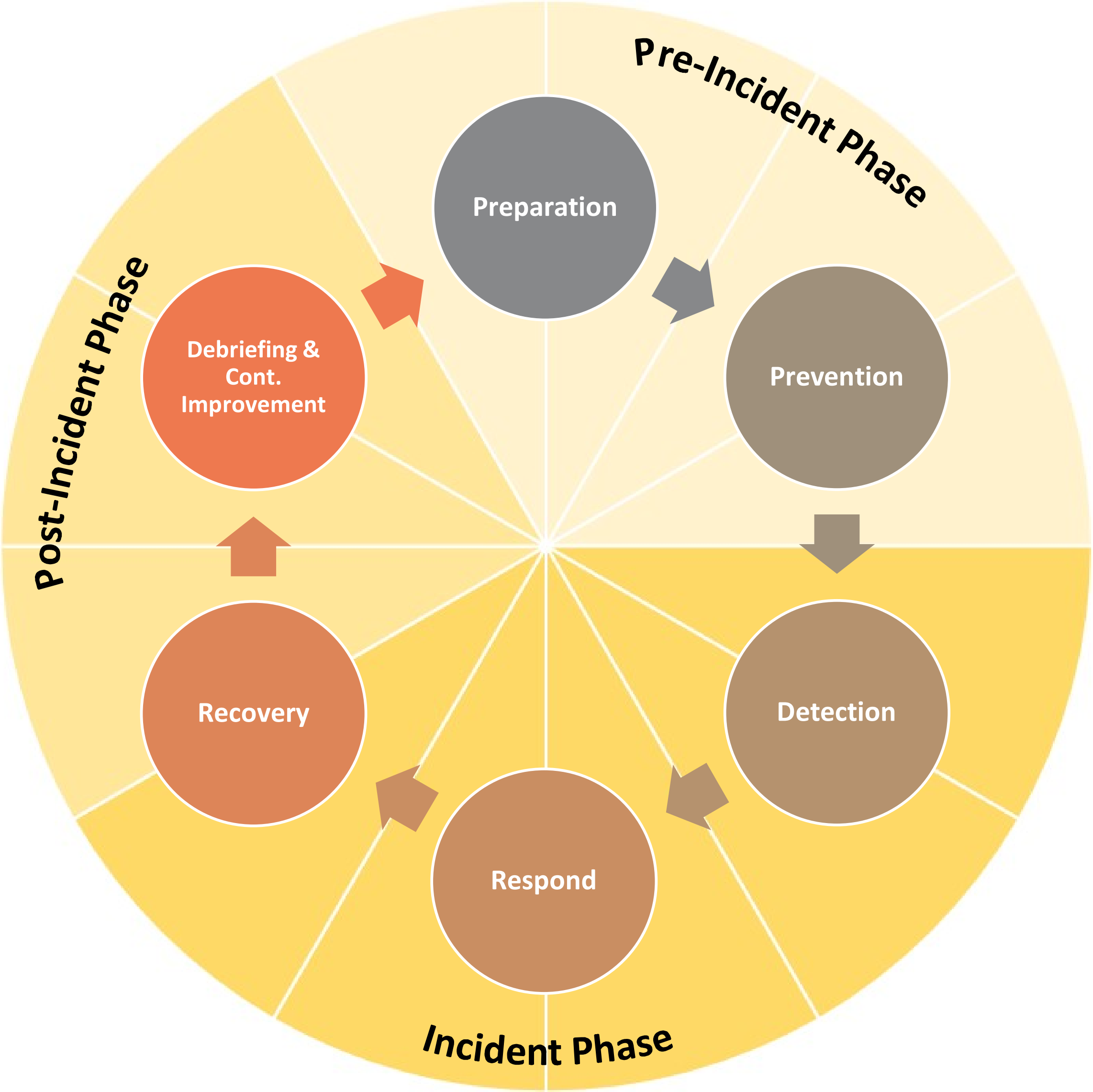
- AAPM task group No. 393
  - Radiation Oncology Contingency Plan Against Cyberattacks

«There are only two types of companies: Those that have been hacked and those that will be hacked.»

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

Thank you for your attention!

samuel.peters@kssg.ch - www.isroi.org


Pre-Incident Phase
Preparation
Prevention
Detection
Respond
Recovery
Debriefing & Cont. Improvement
Incident Phase
Post-Incident Phase