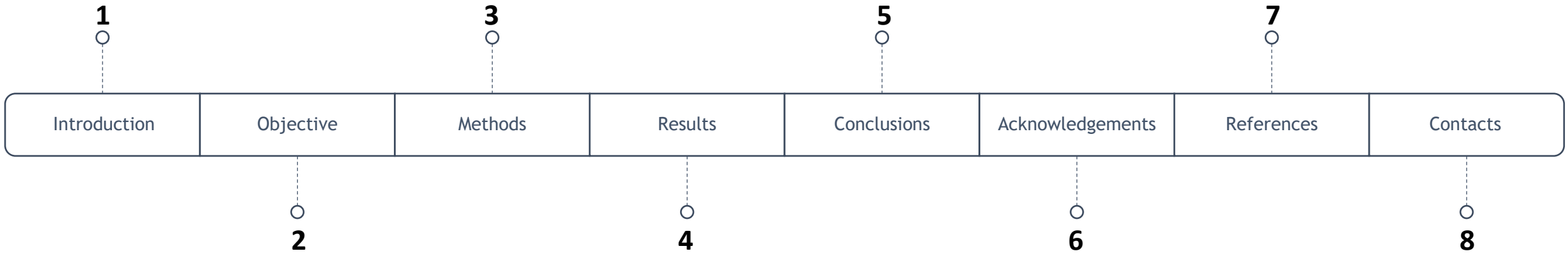
How to prevent a cyberattack in radiotherapy? Measures to implement

Monteiro, I.[1]; Machado, Ana.[1]
[1]Mercurius Health

Summary


1
3
5
7
Introduction
Objective
Methods
Results
Conclusions
Acknowledgements
References
Contacts
2
4
6
8

1. Introduction

WHAT IS A CYBERATTACK?

Cyberattack is any attempt to gain unauthorized access to a computer, computing system or computer network with the intent to cause damage

1. Introduction

Cyberattacks are escalating every day

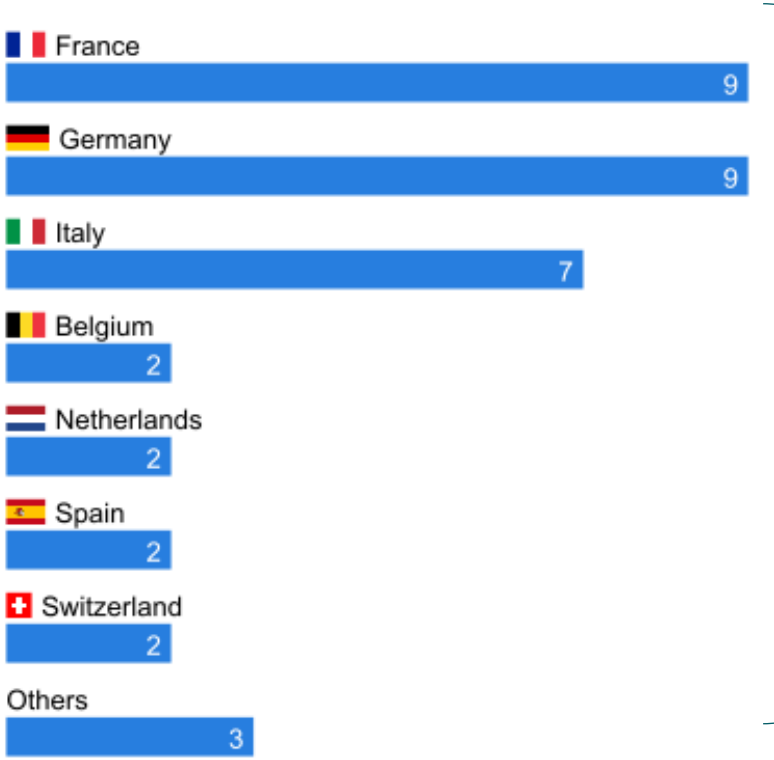
Healthcare providers, such as hospitals, maintain personal and private health information about patients

Hackers can steal information to:
- Benefit financially
- Damage the institution's reputation
- Ask for ransom money for restoration of data and systems integrity

So... healthcare providers are major targets of cyberattacks!

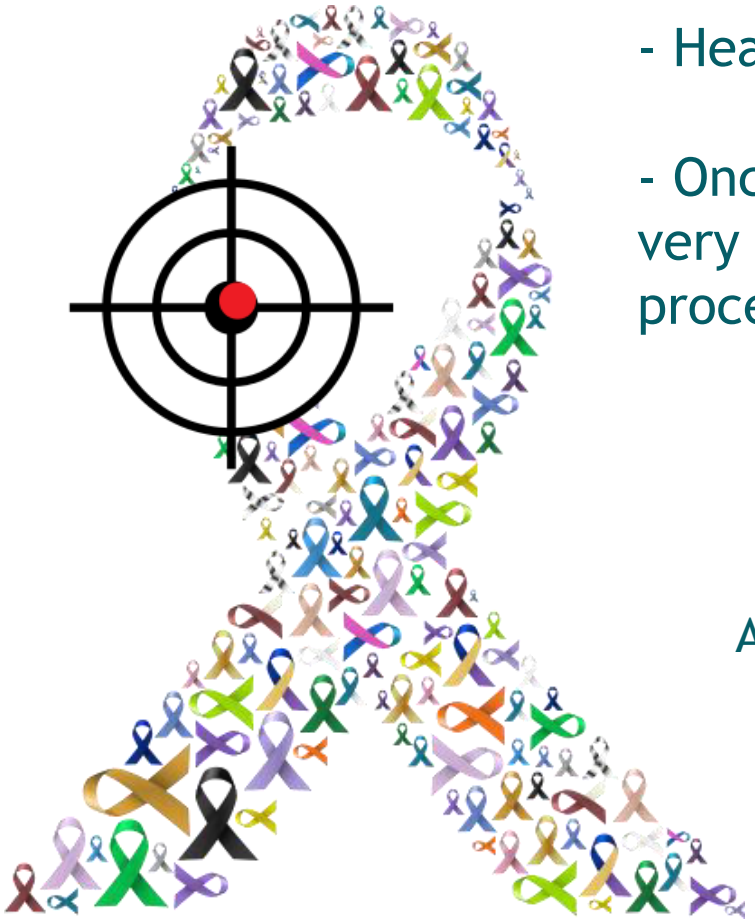
1. Introduction

Major cyberattacks on healthcare in Europe (2nd half of 2021)



Happened more in December

2. Objective



- Healthcare organizations are a prime target for cyberattacks

- Oncology services are among those that can suffer the most, as they are very susceptible to the consequences of such attacks on patient care procedures

↓

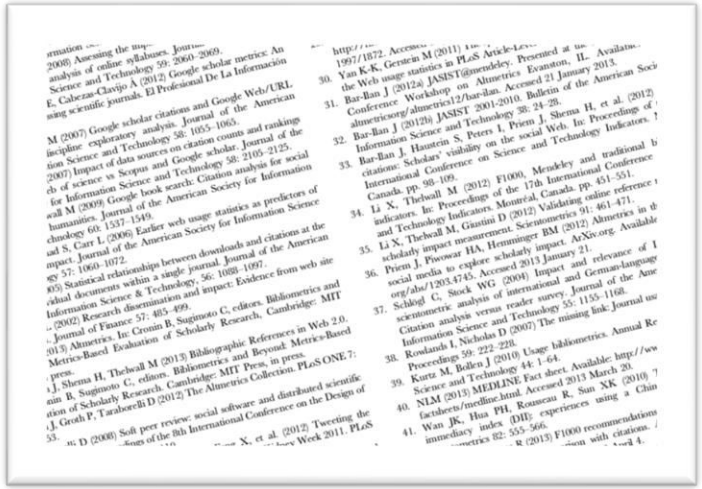
Preventing measures

Avoid losing important data, business disruption, financial expenses for restoring systems and files, and reputation damage

3. Methods

A **review of prospective literature** with the keywords:

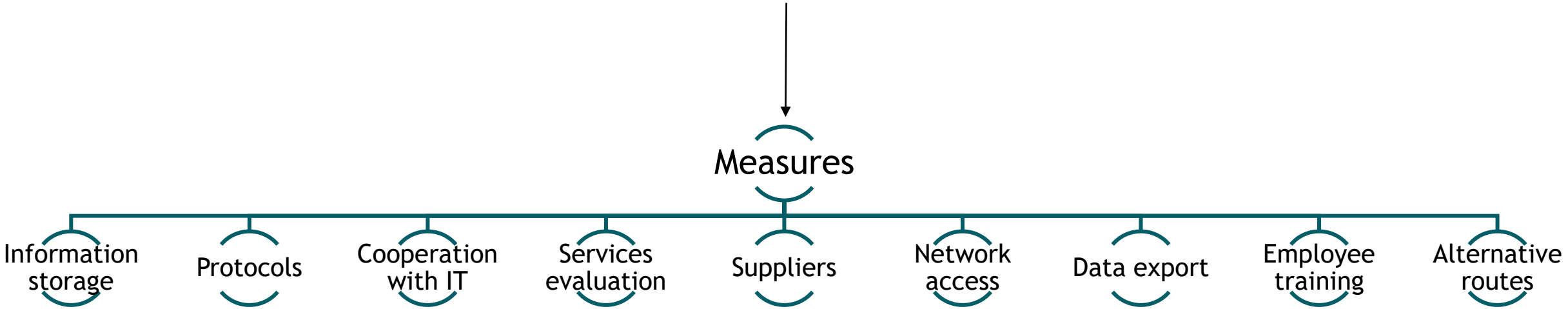
Radiotherapy	Cyberattack	Cybersecurity	Radiation Oncology



- Scientific articles
- Published since 2016
- Based on cyberattacks occurred in radiation oncology hospitals and which affected their practices

4. Results

A prevention plan requires a change in strategies, tactics, and culture around cybersecurity in radiotherapy



4. Results

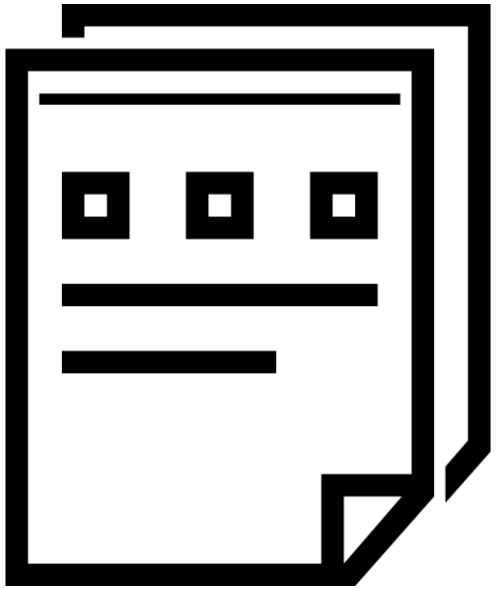
Information Storage

- Maintain paper records
- Consider offline storage/backups
- Have regular and not just one semi regular backup
- Create an intercommunication system between the service interface system (eg. Mosaiq) and a security server for data archiving
- Get Cloud storage services (prefer encrypted patient data)

4. Results

Protocols

- Establish and test both disaster and communication plans
- Develop incident response plans covering newly acquired products or systems
- Non-electronic protocols updated and readily available for activation



4. Results

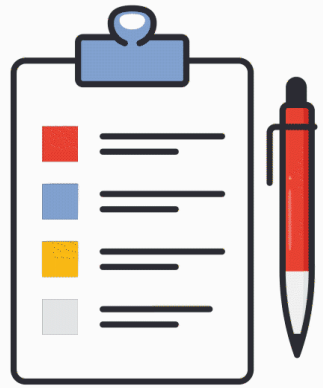
Cooperation with IT

- Involve the IT department in the stages of service procurement
- When it's a specific team, define roles, responsibilities, workflows and monitoring of the systems aligned with the basic hospital procedures

4. Results

Services Evaluation

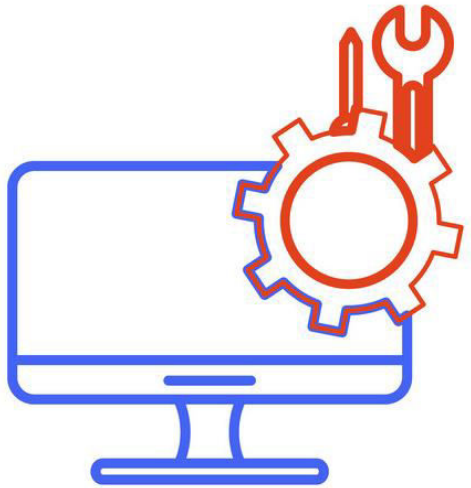
- Develop an update policy: operating system, software and anti-virus
- Be careful with the interoperability
- List the security requirements for each different component to avoid gaps
- Undertake audits to ckeck if all processes are defined and being performed correctly
- Get firewall protection and test regularly the locations and software



4. Results

Suppliers

- Ensure that vulnerabilities are considered before procuring new products or services and that they're monitored
- Determine a minimum set of security tests and risks assessments to be performed on acquired products or systems
- Define business continuity plans for if there is failure of a system
- Establish security baseline requirements



4. Results

Network access

- Have limited and controlled Wi-Fi access
- Implement network segmentation: isolate all devices connected to the network from the rest of the network
- Keep a medical device off of the network if it's needed to use an old version of the operating system known to have vulnerabilities
- Limit or not use USB devices
- Have computers time-out and lock screen

4. Results

Data Export

- Require encryption if data leaves the organisation
- Data can be copied to an external disk drive for storage in an alternative secure off site location

4. Results

- Employee training
  - Train staff that's working on site
  - Educate users

4. Results

Alternative communication routes

- Create alternative secure messaging and emergency call services for all hospital services
- Develop a wired backup network with basic internet connectivity

5. Conclusion

Healthcare is one of the lower industry spenders on IT

Patients data is one of the highest valued by hackers

Ideal environment for cyberattacks

Organizations providing oncology care should be alerted to the possibility of cyberattacks

Development of processes to reduce the impact of this activity on these essential services

6. Acknowledgements

7. References

- Coventry L, Branley D. Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. Maturitas. 2018;113:48–52.
- Cyberattacks on healthcare, Europe, 2nd half of 2021 [Internet]; 2022. Cyberattacks on healthcare, Europe, 2nd half of 2021; [cited 2022 Jul 20]; Available from: https://konbriefing.com/en-topics/cyber-attacks-2021-ind-healthcare-europe-h2.html
- European Union Agency for Cybersecurity. Procurement Guidelines for Cybersecurity in Hospitals [Internet]. 2020 Feb 01 [cited 2022 Jul 21]:8-51. Available from: https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020
- Ades Steven, et al. Cancer Care in the Wake of a Cyberattack: How to Prepare and What to Expect. JCO Oncology Practice [Internet]. 2022 Jan 01 [cited 2022 Jul 21];1:24-36. DOI 10.1200/OP.21.00116. Available from: https://ascopubs.org/doi/full/10.1200/OP.21.00116
- Carl Nelson J., et al. Development of Rapid Response Plan for Radiation Oncology in Response to Cyberattack. Advances in Radiation Oncology [Internet]. 2020 Nov 05 [cited 2022 Jun 22]:1-2. DOI 10.1016/j.adro.2020.11.001. Available from: https://www.advancesradonc.org/article/S2452-1094(20)30340-7
- Nichols EM, Rahman SU, Yi B. The impact of cybersecurity in radiation oncology: Logistics and challenges. *Appl Rad Oncol*. 2018;7(4):14-18
- Chow James C. L., et al. Internet-based computer technology on radiotherapy. Reports of Practical Oncology & Radiotherapy [Internet]. 2017 Nov 01 [cited 2022 Jun 30];22(6):455–462. DOI 10.1016/j.rpor.2017.08.005. Available from: https://www.sciencedirect.com/science/article/pii/S1507136716301602
- Zhang Baoshe, et al. A practical cyberattack contingency plan for radiation oncology. J Appl Clin Med Phys [Internet]. 2017 Nov 01 [cited 2022 Jul 7];22(6):181-186. DOI 10.1002/acm2.12886. Available from: https://pubmed.ncbi.nlm.nih.gov/32333513

8. Contacts

Ana Bárbara Machado
barbara.machado@mercuriushealth.com

Inês Monteiro
ines.monteiro@mercuriushealth.com

THANK YOU FOR YOUR ATTENTION!