



Cybersecurity: How Ready Are We?

Kham Nguyen, MBA, CMD, RT(T), Cody Wages, CMD
MD Anderson Cancer Center

Background

Cyber threats are an increasing global concern with massive business and clinical risk potential. A recent IBM Security’s Cost of Data breach reports the healthcare sector to have the highest breach-related financial impact for 12 consecutive years, with an average attack costing \$10.1 million¹. Healthcare sectors (and radiation oncology) are high-value targets for bad actors. In fact, in 2020 The U.S Department of Health and Human Services (HHS) Office of the Assistant Secretary for Preparedness, the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Safety Agency (CISA), issued an advisory, stating:

“CISA, FBI and HHS have credible information of an increased and imminent cybercrime threat to U.S. hospitals and health care providers”²

In addition to increasing severity, cyber threats are growing in complexity and variety of tactics. . A 2021 article in Security Magazine identified these five areas of concern:

- Social engineering attacks (non-technical)
- Exposure of known and unknown internet-facing vulnerabilities
- Exploitation of system administration tools.
- Ineffective monitoring of critical IT systems.
- Human-operated ransomware risks.

A strong defense relies on a robust layered approach. Our two-pronged approach involves proactive and rapid response countermeasures.

At our institutional level, board-reaching measures were established to protect against common threats, such as phishing or exploitation of administrator tools.

At the local, Radiation Oncology level, we focused on measures to ensure continuity of care in the event of a cyberattack as interruptions and/or delays in a patient’s radiation treatment course for a prolonged time is a serious risk to patient safety.

Radiation Oncology practices are uniquely vulnerable to prolonged downtime due to our complex delivery systems and reliance on technology. Modern machines are not designed to treat without a pre-created treatment plan, putting many patients at risk for radiation treatment disruption for an unknown period if a cyberattack occurs.

As part of our business continuity planning, efforts were put into place to identify technology needs and then design a procedure to maintain radiation treatment continuity during a prolonged downtime. The administrative team defined the scope of the project to encompass these main goals:

Goals

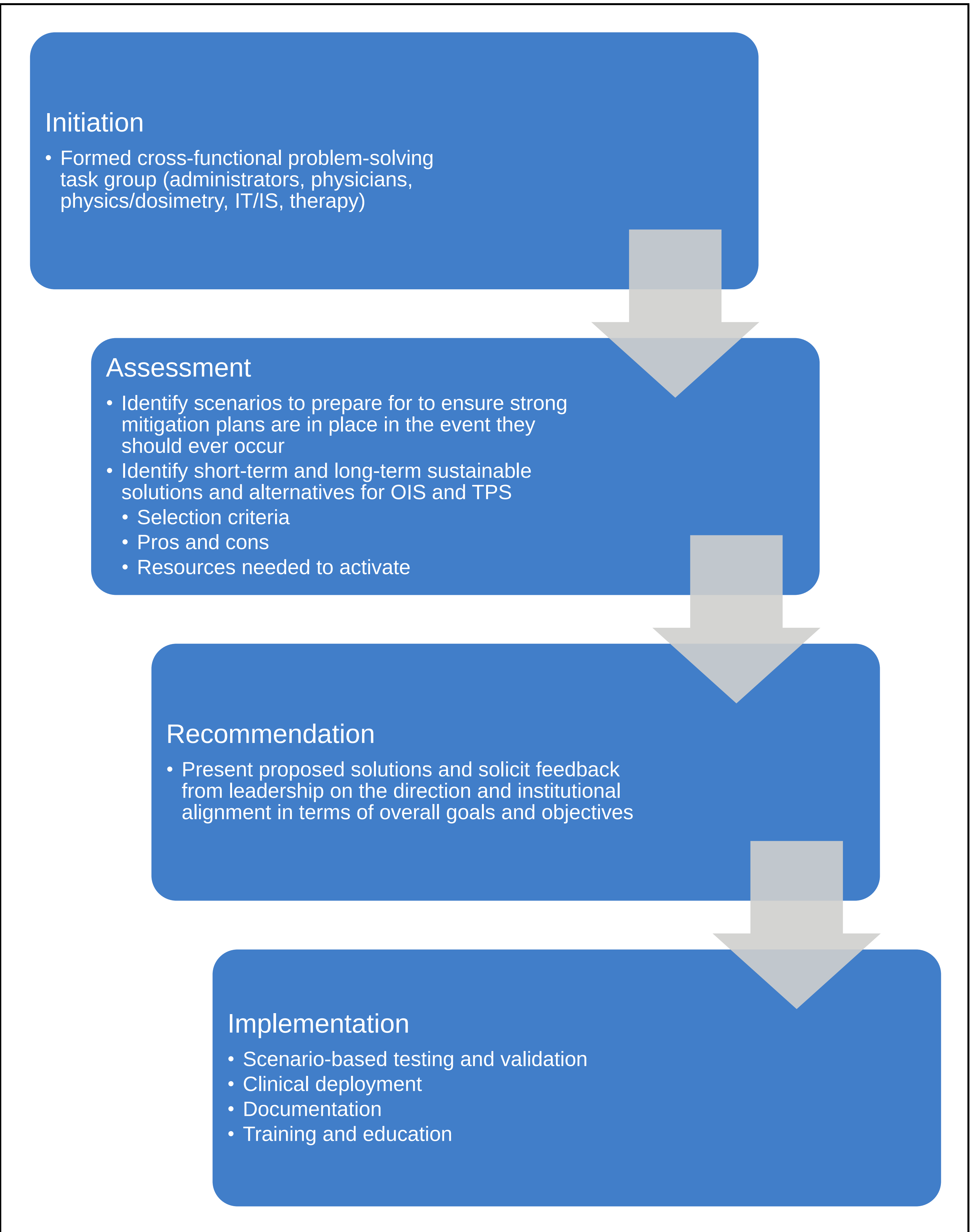
- Define how to maintain patient communication and radiation treatment for prolonged downtime
- Define technical requirements to provide uninterrupted treatment delivery
- Develop a safe and robust emergency response process for all areas that deliver radiation treatment
- Document and generate a testing strategy and then a training and clinical implementation plan

Methods

Our overall charge was to identify potential solutions to safely provide continuity of radiation therapy services in the event of a catastrophic IT outage, for up to four weeks.

The scope of our solutions and implementation plans were prioritized based on two areas of focus:

- Patients under treatment
- New patients (unplanned)



Strategy

We developed a multi-point plan in alignment with the institution

Prevention

- Further strengthening the security of the clinical treatment environment across all locations, including regional sites
- Update equipment to Modern OS and/or add extra firewalls
- Enhance control/security on workstations
- Use of advanced systems for monitoring and protecting traffic between computers within our system

Rapid Response

- Preconfigured servers for each of our critical applications that are isolated from the network
- Robust backup system with multiple time points

Operational Preparation

- Emergency management
 - Integration into the existing incident command structure
- Internal and external communication plans
 - Patients and caregivers
 - Leadership updates and decision-making
 - Team huddles
 - Supporting services
- Patient triage
 - Development of a contingency list for patient triage and established clinical criteria
- Documentation
 - Downtime policies and procedures
 - Paper forms
- Training and Education
 - Perform tabletop exercises to proactively prepare for unplanned IT system downtimes
 - Assess team readiness
 - Identify opportunities to enhance ongoing training/education

Conclusion

Cyber threats are a rapidly growing concern that carries hefty financial and clinical consequences if your center was to experience prolonged downtime. Healthcare is specifically targeted with: increased frequency of attacks, rising complexity, and severity.

Proactive measures should be taken to bolster efforts to insulate infrastructure from a variety of threat types. Efforts should be taken to identify risks and plans developed to protect and then respond if your center is impacted to mitigate disruptions in radiation treatment delivery.

Development of these strategies requires a multi-disciplinary approach, an implementation plan, and then a long-term maintenance/education plan. A good defense is scalable, robust with minimal to no disruption to the clinical treatment workflow, and nimble enough to adjust as the threat tactics evolve.

References

1)Landi, Heather Fierce Healthcare, online July 27, 2022
<https://www.fiercehealthcare.com/health-tech/healthcare-data-breach-costs-reach-record-high-10m-attack-ibm-repor>
2) Cybersecurity and Infrastructure Security Agency. “Alert (AA20-302A) Ransomware Activity Targeting the Healthcare and Public Health Sector.” Accessed online February 1, 2021: <https://us-cert.cisa.gov/ncas/alerts/aa20-302a>.