Advances in Radiation Oncology (2022) 7, 100990

advances in radiation oncology

www.advancesradonc.org

Scientific Article

Readiness for Radiation Treatment Continuity: Survey on Contingency Plans Against Cyberattacks

ByongYong Yi, PhD,* Amit Sawant, PhD, Shifeng Chen, PhD, Sung-Woo Lee, PhD, and Baoshe Zhang, PhD

Department of Radiation Oncology, University of Maryland School of Medicine, Baltimore, Maryland

Received January 18, 2022; accepted April 30, 2022

Abstract

Purpose: Cyberattacks on health care systems have been on the rise over the past 5 years. Formulation and implementation of a robust postattack business continuity plan and/or contingency plan (CP) is essential for minimal disruption to patient care. The level of awareness and planning within the radiation oncology community for cyberattacks is not clear. This study was undertaken to survey and assess cyberattack CP awareness and preparedness.

Methods and Materials: A survey instrument comprising 5 questions on awareness and preparedness of cyberattack CPs was e-mailed to 150 radiation oncology departments. Recipients included 105 institutions with residency programs in therapeutic medical physics, as listed by the Commission on Accreditation of Medical Physics Education Program (usually either school-based or large institutional settings), and 45 additional smaller settings within the United States, representing community practices.

Results: Forty-three responses were deemed evaluable for analysis. Forty-two percent (18 respondents) of respondents responded that they are well-aware of the concept of a cyberattack CP. A large discrepancy in awareness exists between larger hospitals (LH) that have 5 or more treatment machines and smaller hospitals (SH) that have 4 or fewer, 54% versus 24 % ($P < .05$). Fifty-eight percent of respondents considered it "essential" to have such a plan in place, and 28% considered it "desirable" to do so but not practical. Nine percent regarded a cyberattack CP as unnecessary. No significant differences in responses were noted among different types or sizes of institutions on this issue. Sixty-two percent of LH responded that they were either preparing or evaluating a CP, compared with only 29% of SH ($P = .03$). However, no respondents explicitly replied that they already had a CP in place in their practices.

Conclusions: The importance of cyberattack preparedness and implementation does not seem to be well-recognized in radiation oncology. Both the awareness and the preparedness of SH are substantially less than those of LH. Specific and ongoing education efforts in parallel with development of appropriate programs are needed to counter the increasingly pervasive and complex threat of cyberattacks.

Introduction

Increasing frequency and severity of cyberattacks is a major security concern in the health care industry as well as in other industries and government agencies.[1] Cyberattacks on high−profile companies and government agencies regularly result in significant data breaches and

Sources of support: This work had no specific funding.

Disclosures: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data sharing statement: Research data will be shared upon request to the corresponding author.

*Corresponding author: ByongYong Yi, PhD; E-mail: byi@umm.edu

https://doi.org/10.1016/j.adro.2022.100990

service continuity disruptions.[2] The 2020 Healthcare Information and Management Systems Society cybersecurity survey revealed that 70% of responding hospitals had experienced a "significant security incident" within the past 12 months, including phishing and ransomware attacks, that resulted in disruption of information technology operations (28%) and business functions (25%), as well as data breaches (21%) and financial loss (20%).[3] Joyce et al[4] summarized cybersecurity threats in 2021 and demonstrated that health care providers are increasingly the focus of major cyberattacks. Reports also demonstrated that cyberattacks, including ransomware and malware, can happen at any time to a radiation oncology department or facility.[5-8]

As a data-intensive practice, radiation oncology is one of the most vulnerable to cyberattacks among the medical practices. In most radiation oncology departments, the radiation oncology information system (ROIS) includes all radiation therapy and electronic medical record (EMR) data. When the ROIS ceases to function, clinical operations may be effectively paralyzed — the facility may be unable to perform any patient−related imaging, planning, or treatments. Cancer radiation therapy treatments are timing-dependent, and substantial delays could put patient welfare at risk. Most modern radiation treatments are delivered by computer-controlled systems. If delivery information saved in the data server is inaccessible due to data deletion, locking, or corruption, intended treatments cannot be guaranteed. The EMR, which includes radiation therapy treatment information, is critical because underdosing to the tumor would significantly increase local recurrence risk and overdosing to normal tissue would increase toxicities.[1]

It is therefore imperative that members of the radiation oncology community, just as in any other industry, have business continuity (contingency) plans in place so that patient treatments can be continued without significant interruptions in the event of a cyberattack. Current solutions for providing data redundancy for ROIS are designed with hardware and software failure in mind and do not provide an effective business continuity plan for the clinic, as a lot of time and effort is required to restore patient data from the institutional backup system and then to check data integrity. For example, even with patient data redundancy from enterprise backup systems, recent cyberattacks on radiation oncology practices have caused disruptive service interruptions (ranging between weeks and months).[4,6-9]

The American Association of Physicists in Medicine Task Group Report 201 stated, "Business continuity and disaster recovery plans should be formulated with a thorough knowledge of these server configurations."[10] The U. S. Department of Health and Human Services has also urged health care providers to have a contingency plan (CP) in place to restore daily operations as quickly as possible after compromise from a cyberattack.[11] However, the extent of such preparedness in radiation oncology across the United States is not clear. The current study was undertaken to assess cyberattack CP awareness and preparedness across radiation oncology departments within the United States. Note that our scope is limited to what a clinic should do after an attack has occurred and institutional and departmental network services are unavailable. The prevention of cyberattacks, which most commonly falls under the purview of hospital information services, is outside the scope of this study.

Methods and Materials

An institutional review board−approved survey instrument comprising 5 questions and 2 subquestions (Table 1) was devised and sent out to physicists in 150 radiation oncology departments and practices. Recipients included 105 institutions with physics residency programs (therapy) as listed by the Commission on Accreditation of Medical Physics Education Program (usually either school-based or large institutional settings) and 45 additional smaller settings in the United States to represent community practices. A senior physicist from each selected institution or practice received an e-mail with an attached survey instrument file and a subsequent reminder by e-mail or phone after 1 week. It was requested that the e-mail be sent to the appropriate personnel unless the e-mail recipient was knowledgeable enough to respond to the questions. One more week was allowed after this reminder before the survey was closed.

Only 1 data set from each institution was used for analysis. When more than 1 response was received from an institution, only the first received was included in analysis. Collected data were tested their validity and were filtered for duplication as stated below, then anonymized. Responses with answers missing on item 2 on awareness and necessity for CPs were excluded from analysis. Missing answers on items other than these 2 questions were excluded from response calculations on the specific related items. Missing answers on questions about institution (eg, organization type or number of treatment machines) were considered as unknown. Descriptive statistics were used to calculate the percentage of awareness of and readiness for a CP. χ^2 tests were performed to analyze awareness and readiness differences among sizes of institutions. P values $< .05$ were considered statistically significant.

Results

We received 43 responses (Table 2) constituting a 29% response rate after discarding 1 duplicate response from an institution. Table 2 shows the characteristics of the respondents' institutions from the evaluable responses.

Table 1 Questions used in this study

Questions
1-1 About your institution: Organization type: A. Private or a community practice. B. Medical (physician's) group. C. University/medical school hospital. D. Other (Specify:)
1-2 About your institution: Organization type: Number of treatment machines in your institution. A. 1 LINAC (or 1 proton gantry). B. 2 LINACS (or 2 proton gantries). C. 3-4 LINACS (or 3-4 proton gantries). D. >5 LINACS (or >5 proton gantries)
2. Have you heard about a contingency plan or a business continuation plan against a cyberattack? 1) I am familiar with plans to prevent cyberattacks but have not heard of a contingency plan, 2) I have heard the term, but do not know what it is exactly, 3) I am very familiar with the concept of a CP. 4) Other (Specify:)
3. In your opinion, how necessary is it for a radiation oncology department to have a contingency plan against a cyberattack? 1) Not necessary; It is more important to focus on preventing cyberattacks, 2) Desirable to have, but it is not practical considering current resources and expertise at our institution, 3) A CP is essential, 4) Other (Specify:
4. What is the status of CP at your department? 1) We do not have a CP and are unlikely to consider this a priority in the near future, 2) We are formulating and/or evaluating in-house solutions, 3) Waiting for a commercially available solution, 4) We have identified a CP solution and are testing, 5) We have implemented a CP solution in our clinic (please specify if in-house or commercial)
5. What is the plan you already either have or wish to have for a contingency plan? Choose ALL that apply. 1) Pay ransom if applicable, 2) To send patients to nearby practices, 3) Wait until the R&V system (such as, ARIA, Mosaic) is fully recovered and patient data are fully verified, 4) Only treat emergency patients manually with simple techniques (such as AP/PA fields) before the R&V system (such as ARIA, Mosaic) is fully recovered and patient data are fully verified, 5) Only resume non-IMRT/VMAT/SRS patient treatments without IGRT capability with manual treatments and paper charts, 6) Resume all of the patient treatments without IGRT capability, 7) Resume patient treatments with the same IGRT accuracy shortly (eg, within 48 hours) through DICOM file mode of treatment machine console but with paper charts, 8) Resume patient treatments with the same IGRT accuracy shortly (eg, within 48 hours) through a backup/secondary R&V system, 9) No need to have such plans since we have an established anticyber-attack program, 10) Other (Specify:)
A CP in radiation oncology is defined as follows: Once the normal radiation therapy patient treatment workflow and systems (such as Varian ARIA/Elekta Mosaic R&V systems) are unavailable due to a network-level or ransomware cyberattack, a CP is a separate treatment workflow that can resume radiation therapy patient treatments with the same accuracy (such as IGRT) without delay. Note: Because the CP focuses on continuation of ongoing patient treatments, new patient enrollment and related activities (such as simulation, planning) are not covered herein.

Almost half of the responders (18; 42%) were aware of the concept of a business continuation plan, whereas 25 (58%) indicated that they did not know what it is or they had never heard of the concept (Table 3). Individuals at larger hospitals (LH), defined as facilities with 5 or more treatment machines, were more aware of the concept than those at smaller hospitals (SH), defined as facilities with 4 or fewer treatment machines; 15 (60%) and 4 (24%), respectively (P = .03). The difference between organization types of institutions and practices such as academic versus community practice was not significant. Sixty-two percent of responders considered it to be essential to have a CP, whereas 35% (n = 16) considered this unnecessary or impractical. No statistical significances were found differentiating organization types or sizes of institutions.

Table 2 Characteristics of respondents' institutions

Characteristic	n	%
Total number of respondents	43	
Organization type		
Private or community practice	11	25.6
Medical (physicians') group	6	14.0
University or medical school	24	55.8
Other	2	4.7
Number of treatment machines		
1 LINAC or proton gantry	3	7.0
2 LINAC or proton gantries	6	14.0
3-4 LINAC or proton gantries	8	18.6
≥5 LINAC or proton gantries	26	60.5

Abbreviations: LINAC = linear accelerator.

Institutions were roughly equally divided on the state of preparedness for CP in the event of a cyberattack. Slightly more than half of the respondents (22; 51%) reported that they were currently doing nothing about a CP because they (1) had no plan for the near future (19; 44%); or (2) were waiting for a commercially available solution (3; 7%). On the other hand, 49% of responding institutions (n = 21, 16 LH and 5 SH) were either preparing or testing a CP solution. The LH group is more prepared than the SH group: 62% (n = 16) of total 26 LH are either preparing or evaluating a CP solution, compared with 29% (n = 5)

Table 3 Awareness and preparedness of CP

Awareness and preparedness	n (%)	%	Number of gantries		*P* value
			1-4 gantries	>5 gantries	
Awareness					
Know well	18	41.9	4	14	.049
No knowledge	25	58.1	13	12	
Never heard about contingency plan	(5)	(11.6)	(2)	(3)	
Heard the term, but do not know exactly	(20)	(46.5)	(11)	(9)	
Preparedness					
Not preparing	22	51.2	12	10	.027
Not considering to have a CP, soon	(19)	(44.2)	(9)	(10)	
Waiting for a commercial solution	(3)	(7.0)	(3)	(0)	
Preparing	21	48.8	5	16	
Preparing a solution	(16)	(37.2)	(4)	(12)	
Identified a solution and under testing	(5)	(11.6)	(1)	(4)	

Abbreviations: CP = contingency plan.

of total 17 SH (P = .03). No respondents reported being ready or currently running a CP.

Many institutions reported preferring to wait until the system recovery (44%) or to treat emergent patients manually without image guided radiation treatment (42%). Fifteen institutions (35%) considered either transferring patients to nearby hospitals or treating patients using digital imaging and communication in medicine (DICOM) mode with paper charts. Only 19% of the respondents indicated they would continue all treatments shortly after an attack with the CP, which is the business continuation plan. Six institutions (14%) were willing to pay ransom for restoration of data. Consistently, 9% of respondents did not believe a CP to be necessary (Table 4).

Table 4 Choices of items for CP

Choices	n	%
Pay ransom	6	14.0
Transfer patients to nearby institution	15	34.9
Wait until recovery	19	44.2
Tx emergent pt manually, no IGRT	18	41.9
Simple case, manual Tx, no IGRT	7	16.3
Tx all without IGRT	2	4.7
DICOM mode with paper chart	15	34.9
Resume all with CP	8	18.6
No need for such a plan	4	9.3

Discussion

Joyce et al[4] emphasized that cybersecurity threats continue to evolve and that a reliance on computer-driven technology makes radiation oncology practices especially vulnerable to cyberattacks. In many instances, transferring patients to other institutions is not an option when EMRs are compromised or networks are down practice-wide.[1] In an environment with escalating numbers and types of attacks, reliance on the multiple protection layers of cybersecurity strategy is not sufficient. Regardless of the antiattack plan, the chances for infection and disruption still remain.

Nelson et al[6] reported on their cyberattack experience on October 28, 2020. The attack shut down the ROIS, disabling treatments. Multiple layers of ROIS backups were rendered useless. Their strategy to continue operation was to prioritize treatment resumption by prioritizing patients into 3 groups. Patients in the highest priority group were sent to unaffected sites, with treatment resuming in 2 to 4 days. Treatments in the medium- and low-priority patient groups were resumed at the site after 6 to 7 and 12 to 13 days, respectively. Harrison et al[9] reported on a ransomware experience that disabled the record and verify system but left the hospital EMR operative and available. Using direct DICOM transfer combined with impromptu paper charts, the group was able to treat 50% of patients within 48 hours and 95% within 1 week. Both institutional reports emphasized the importance of having a recovery plan in place rather than having a better attack prevention plan. Three respondents emphasized that they cannot be protected from all attacks because the nature of attacks is unpredictable. More and more frequently, we hear news

about damage from the cyberattacks around us. Two of the respondents in our survey voluntarily disclosed that they had experienced attacks that took their treatments down for a period.

The U.S. Department of Health and Human Services notes that "Contingency plans aren't just a good idea; regulations for certain industries require contingency planning."[11] For example, the health insurance portability and accountability act security rule requires that health insurance portability and accountability act-covered entities and business associates establish and implement a contingency plan.[12]

The urgent challenge in our profession is development and distribution of a CP program that each institution can easily implement. Although 2 institutions shared their cyberattack experiences, their recovery efforts were not in place before the attacks, limiting the instructive utility of their experiences.[6,9] We have previously published a solution specific to our institution's systems, but this is not intended for scalable deployment, and it requires more development before widespread implementation.[1] Our experience suggests that even without a well-developed CP, a practical (and somewhat homespun) stop-gap solution is to write down the number of delivered fractions to each patient after each treatment and to save DICOM plan files to a new thumb drive every day. For small clinics, this could be a solution after a disastrous cyberattack that would allow patient transfer to unaffected treatment sites. This is neither a long-term nor an easily workable solution.

In general, a CP should provide an independent radiation therapy workflow strategy that can be implemented if a cyberattack disrupts routine patient treatment workflow or systems. Before preparing a CP, it is important to create a series of probable attack scenarios. Because the nature of attacks can vary widely, radiation oncology departments may need multiple levels of CPs. A CP can range from minimal, relying solely on the functionalities of treatment machines to treat emergency patients with simple techniques, to comprehensive, allowing resumption of the majority of treatments with customary accuracy (such as image guided radiation treatment). As a data-driven practice, the comprehensiveness of a radiation oncology CP will rely on the availability of essential clinical data and their formats, such as DICOM radiation therapy (eg, plan, structure, images) and EMR documents (eg, prescription directive, plan reports, diagnosis). At the same time, a CP must have the capacity to keep a record of treatment history for each treatment, regardless of the complexity level of the CP. Because a CP against cyberattacks consists of modules of backup and retrievals of data, parts of the CP can be shared for another CP against catastrophic events other than a cyberattack, such as a power or network outage and a ROIS database breakdown.

One limitation of this study is that LH clinics are overly represented in the sample. More than 60% of the respondents were from LH and this may not represent the distribution of LH and SH in the United States. Milligan et al[13] reported that there were 1615 radiation oncology practice sites in the United States in 2017, of which 3.5% were large practices, defined as an institution of 11 or more radiation oncologists' practices. The paper also reports 26% of Medicare claims are from large practices. The definition of "large practice" in this study is not the same as LH defined in the report, but the numbers reported in the report can be indicators to imagine how LH is overly represented in this study. Because of nonproportionality of the number of LH and SH, ie, LH clinic is overly represented than it is in the United States, between actual awareness and preparedness across the country may be less than the numbers in this report. Another limitation may be the demand characteristics bias,[14] where behavior or opinion may be changed because of their participation in the survey. For example, the awareness question asks if the responder has prior knowledge of CP, but the question itself already provides the information. Similar influence may happen on the question of necessity of CP. Only 42% of the respondents answered they are aware of CP, but 49% are either preparing or have a solution. This discrepancy may be from the social desirability bias. All these biases contribute to higher values of awareness, preparedness, and necessity for CP in the survey results. Notwithstanding the potential biases mentioned, which may have contributed to increased awareness and preparedness, those increased numbers are still lower than are desired.

Despite the importance of CPs in clinical radiation oncology practice, both awareness and preparedness are low. Awareness of CPs may be even lower than the somewhat limited group sampled in this study. Publications and conference education sessions on this topic are quite rare.[1,15] A discipline-wide effort is needed to enhance education, such as organization of a task group and/or a series of sessions at American Association of Physicists in Medicine or American Society for Radiation Oncology meetings.

Conclusions

Awareness of CPs and preparedness for responses to cyberattacks in radiation oncology practices was surveyed. Recognition of the importance of CPs is relatively low in our opinion and preparation for cyberattacks lags further behind. Only a few institutions reported current efforts to prepare a cyberattack CP, and no institutions were operating such a plan. To fill the gap between the need and awareness and preparedness, systematic education efforts are needed. A parallel need is the development and distribution of practical CP programs that can be implemented across different types of practices.

Acknowledgments

The authors would like to thank Nancy Knight, PhD, for editorial contributions.

References

1. Zhang B, Chen S, Nichols E, D'Douza W, Prado K, Yi B. A practical cyberattack contingency plan for radiation oncology. *J Appl Clin Med Phys*. 2020;21:181–186.
2. Hill M, Swinhoe D. The 15 biggest data breaches of the 21st century. Available at: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html. Accessed October 26, 2021.
3. Healthcare Information and Management Systems Society. 2020 HIMSS cybersecurity survey. Available at: https://www.himss.org/resources/himss-healthcare-cybersecurity-survey. Accessed October 26, 2021.
4. Joyce C, Roman FL, Miller B, et al. Emerging cybersecurity threats in radiation oncology. *Adv Radiat Oncol*. 2021;6:100796.
5. Nichols EM, Rahman SU, Yi B. The impact of cybersecurity in radiation oncology: Logistics and challenges. *Appl Rad Oncol*. 2018;7:14–18.
6. Nelson CJ, Lester-Coll NH, Li PC, et al. Development of rapid response plan for radiation oncology in response to cyberattack. *Adv Radiat Oncol*. 2020;6:100613.
7. Alder S. Radiation treatments disrupted after cyberattack on software vendor. Available at: https://www.hipaajournal.com/healthcare-providers-postpone-radiation-treatments-cyberattack-elekta. Accessed October 26, 2021.
8. Cullen P. Cyberattack: HSE faces final bill of at least €100m. Available at: https://www.irishtimes.com/news/health/cyberattack-hse-faces-final-bill-of-at-least-100m-1.4577076. Accessed October 26, 2021.
9. Harrison AS, Sullivan P, Kubli A, et al. How to respond to a ransomware attack? One radiation oncology department's response to a cyber-attack on their record and verify system. *Pract Radiat Oncol*. 2021;12:170–174.
10. Siochi RA, Balter P, Bloch CD, et al. Report of task group 201 of the American Association of Physicists in Medicine: Quality management of external beam therapy data transfer. *Med Phys*. 2021;48:e86–e114.
11. U.S. Department of Health and Human Services. Office for Civil Rights. Plan A. . . B. . .contingency plan! Available at: https://www.hhs.gov/sites/default/files/march-2018-ocr-cyber-newsletter-contingency-planning.pdf. Accessed October 26, 2021.
12. U.S. Code of Federal Regulation 45 CFR § 164.308(a)(7). Available at: https://www.govinfo.gov/content/pkg/CFR-2007-title45-vol1/pdf/CFR-2007-title45-vol1-sec164-308.pdf. Accessed December 14, 2021.
13. Milligan M, Hansen M, Kim DW, Orav EJ, Figueroa JF, Lam MB. Practice consolidation among U.S. radiation oncologists over time. *Int J Radiat Oncol Biol Phys*. 2021;111:610–618.
14. Cattell RB, Digman JM. A theory of the structure of perturbations in observer ratings and questionnaire data in personality research. *Behav Sci*. 1964;9:341–358.
15. Winslow M, Curran B, Yi B, et al. Disaster preparedness: Are YOU ready? Therapy symposium, American Association of AAPM Spring Clinical Meeting 2020 (virtual). Available at: https://w3.aapm.org/meetings/2020SCM/programInfo/programSession.php?sid=8331. Accessed October 26, 2021.