Advances in Radiation Oncology (2022) 000, 100896

advances
in radiation oncology

www.advancesradonc.org

Evolving Threats in Cybersecurity and Radiation Oncology

# The Impact of a Cyberattack at a Radiation Oncology Department: Immediate Response and Future Preparedness

**Michael Oliver, PhD,[a,b,*] Andrew Pearce, MSc, MD,[c,d] Laurie Stillwaugh, MRT(T),[e] and Konrad Leszczynski, PhD[a,b]**

*[a]Department of Medical Physics, Health Sciences North, Sudbury, Ontario, Canada; [b]Department of Medical Sciences, Northern Ontario School of Medicine, Sudbury, Ontario, Canada; [c]Department of Radiation Oncology, Health Sciences North, Sudbury, Ontario, Canada; [d]Department of Clinical Sciences, Northern Ontario School of Medicine, Sudbury, Ontario, Canada; [e]Department of Radiation Therapy, Health Sciences North, Sudbury, Ontario, Canada*

Received November 1, 2021; accepted January 6, 2022

**Abstract**

Cyberattacks are increasing year after year and many organizations, including hospitals, are becoming targets. Radiation oncology is especially vulnerable because of the reliance on computer and network capabilities to transfer relevant patient information for safe and effective patient treatment. In early 2019, our institution was hit by a ransomware attack that brought down our oncology information system (OIS). Although we were not fully prepared for such an attack, a total of 69 treatment fractions occurred without our OIS thanks to the quick development of a contingency plan and the ability to restore the patients' records. The OIS was recovered by the manufacturer 4 days after the attack. We also have developed a contingency plan and outline important considerations for institutions trying to prepare for unexpected downtime such as a cyberattack.

## Introduction

A recent U.S. government report on cybersecurity noted a 300% increase in attacks from 2016 compared with 2015.[1] Some reasons for the drastic increase in cyberattacks are that the value for an electronic health record is worth 10 to 100 times that of a credit card[2] and that the ransom is paid 32% of the time, with an average ransom price of USD $170,404 for a midsize organization.[3] A survey by Sophos indicated that in 2020, 34% of health care organizations were hit by a ransomware attack, and in 54% of all cyberattacks the cybercriminals succeeded in encrypting the data.[3] These eye-opening statistics indicate that this is an underreported and pervasive problem in the health care industry for which radiation oncology is especially vulnerable because of its reliance on computer and network technology.

During the past few years, a number of high-profile cyberattacks on radiation oncology facilities have been reported in the literature and the media, including Vermont (October 2020),[4] the Elekta Cloud data breach affecting many U.S. customers (November 2020),[5] the Health Service Executive in Ireland (May 2021),[6] and the Waikato District Health Board (June 2021).[7] The root causes that led to the

Sources of support: This work had no specific funding.

Disclosures: none.

Research data are not available at this time.

*Corresponding author: Michael Oliver, PhD.; E-mail: moliver@hsnsudbury.ca

https://doi.org/10.1016/j.adro.2022.100896

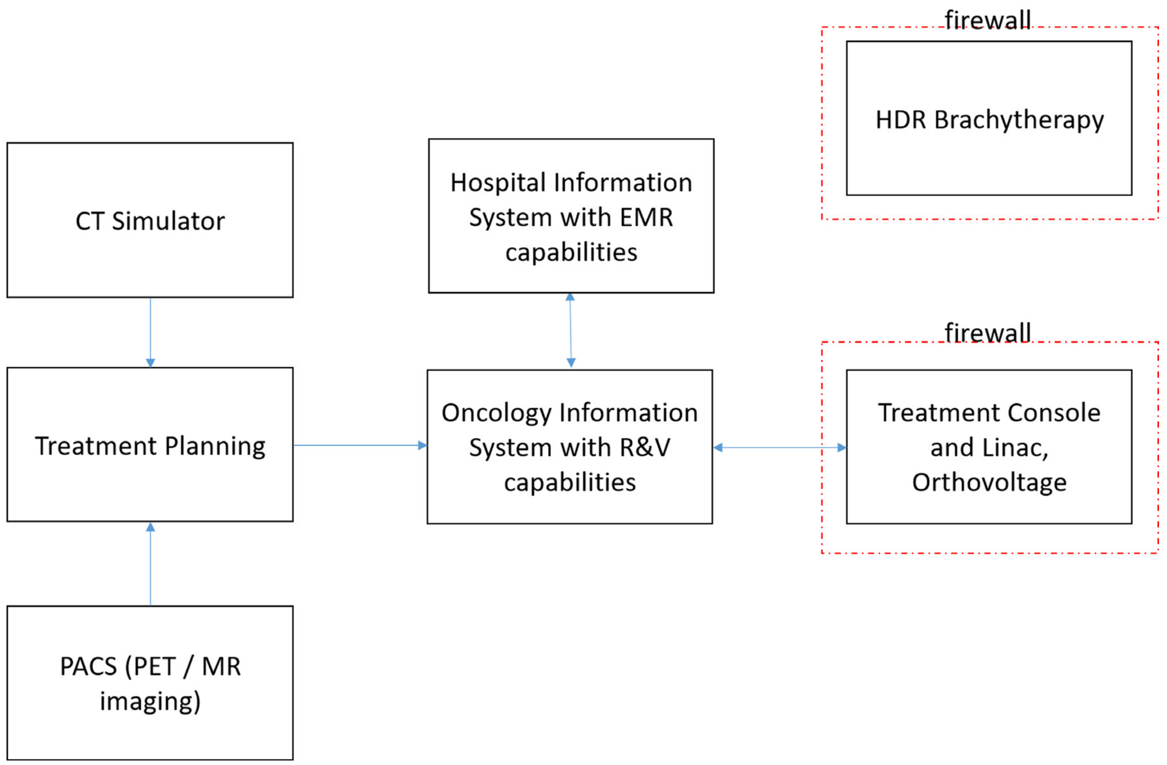
firewall
HDR Brachytherapy
CT Simulator
Hospital Information System with EMR capabilities
firewall
Treatment Planning
Oncology Information System with R&V capabilities
Treatment Console and Linac, Orthovoltage
PACS (PET / MR imaging)

**Fig. 1** Simple schematic demonstrating essential radiation oncology infrastructure and required network communication.

cyberattacks might be different, but the end effect is a delay in radiation oncology patients receiving timely treatments due to a crippling of the network infrastructure and data storage needed to safely treat patients.

Figure 1 shows the interconnectedness of different radiation oncology resources at our department circa January 2019, with network connectivity being depicted by blue arrows. In a fully functioning radiation oncology department all of the interconnected systems would be required for day-to-day operations; however, in a cyberattack scenario there is the capability to treat patients safely when 1 or more of the systems is unavailable. Zhang et al[8] described a solution that allows for treatment of patients if the oncology information system (OIS) is down because of a cyberattack by retrieving daily treatment records on a secure data server. The secure data server is safe during a cyberattack as it has restrictive network security settings and short-burst opening of network opening times.[8] Nelson et al[9] described how to treat patients when the MOSAIQ OIS (Elekta AB, Stockholm, Sweden) is down with Varian Truebeam and Clinac (Varian Medical Systems, Inc, Palo Alto, CA) machines, by capturing and organizing the Digital Imaging and Communications in Medicine−Radiation Therapy (DICOM-RT) plan files sent by the OIS and then creating a report of patients being treated on each linear accelerator (LINAC). This allows the DICOM-RT plan files to be available in an organized fashion and ready to be used on the Varian console using file mode, which is explained in detail in Varian documentation.[9-11]

The remainder of the article will describe the experience of our center treating patients without the capability of our OIS, as was done at Health Sciences North (HSN) in 2019, along with our preparedness plan for future downtime of our MOSAIQ OIS.

## Summary of the Cyberattack Incident at Health Sciences North

HSN is an academic health sciences center in Sudbury, Ontario, Canada with a radiation oncology service that treats over 2000 patients per year between the main site in Sudbury and a satellite facility approximately 300 km west in Sault Ste. Marie, Ontario, Canada. The radiation oncology department is equipped with a Philips Pinnacle treatment planning system (TPS) (Philips Medical Systems, Fitchburg, WI), an Elekta MOSAIQ OIS installed on-site, 5 linear accelerators (2 Varian Clinac iX, 1 Varian TrueBeam, 2 Elekta Infinity), and 1 Gulmay orthovoltage unit (Gulmay Medical Limited, Surrey, United Kingdom). In addition, the physical location of the electronic medical record and OIS servers in HSN at Sudbury are in a dedicated server area and not in a cloud configuration. The clinic in Sault Ste. Marie has a single standalone Varian

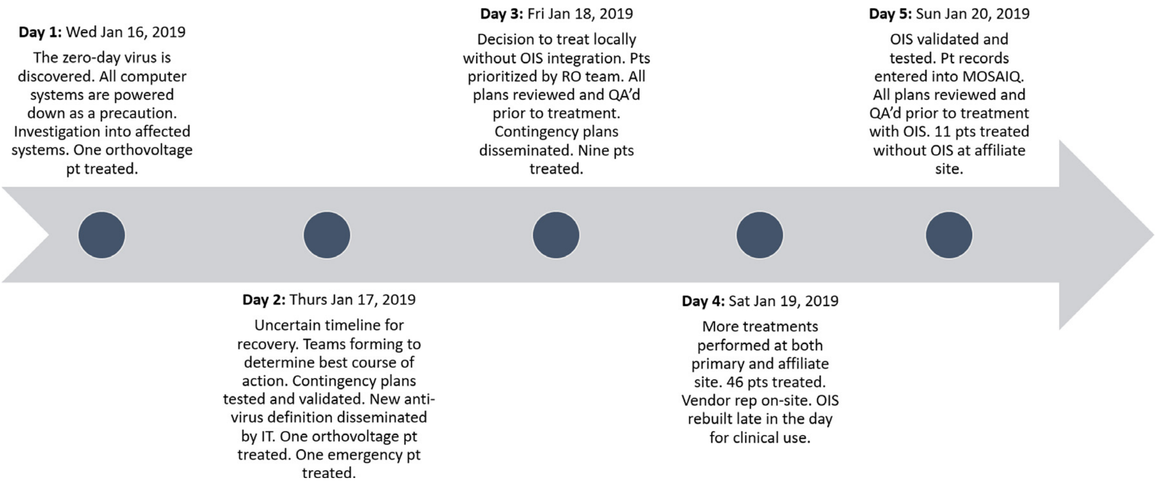
Day 1: Wed Jan 16, 2019
The zero-day virus is discovered. All computer systems are powered down as a precaution. Investigation into affected systems. One orthovoltage pt treated.
Day 2: Thurs Jan 17, 2019
Uncertain timeline for recovery. Teams forming to determine best course of action. Contingency plans tested and validated. New anti-virus definition disseminated by IT. One orthovoltage pt treated. One emergency pt treated.
Day 3: Fri Jan 18, 2019
Decision to treat locally without OIS integration. Pts prioritized by RO team. All plans reviewed and QA'd prior to treatment. Contingency plans disseminated. Nine pts treated.
Day 4: Sat Jan 19, 2019
More treatments performed at both primary and affiliate site. 46 pts treated. Vendor rep on-site. OIS rebuilt late in the day for clinical use.
Day 5: Sun Jan 20, 2019
OIS validated and tested. Pt records entered into MOSAIQ. All plans reviewed and QA'd prior to treatment with OIS. 11 pts treated without OIS at affiliate site.

**Fig. 2** Timeline of cyberattack at HSN including a brief description of key events on each day.

Clinac iX and is connected to the HSN OIS and TPS via dedicated wide area network connectivity and is serviced with a permanent medical physics and radiation treatment staff but rotating coverage by the HSN radiation oncologists.

A brief timeline of the cyberattack and subsequent response is included in Figure 2 highlighting the timeframe from attack to treatment without OIS and then subsequent rebuild of OIS.

On day 1 (January 16, 2019), a zero-day virus infected the computer networks at HSN and brought some clinical operations to a halt, including radiation oncology. All unnecessary computer systems were powered off until deemed safe to be brought back online by information technology (IT). Out of an abundance of caution, the dedicated network connectivity to the affiliate site was also blocked. On the day of the cyberattack, 1 orthovoltage patient was treated without OIS owing to the simple nature of treatment. In addition, computed tomography (CT) simulations continued after a paper documentation process. The IT department received an update to the antivirus definitions and all LINAC consoles were tested for signs of being infected by the virus and were deemed to be unaffected. On day 2 (January 17, 2019), it was deemed that many computer network drives were infected along with our OIS and hospital information system. In parallel, the medical physics group also investigated the possibility of treating patients without the OIS for our various LINAC types: Varian Clinac iX, Varian Truebeam, and Elekta Infinity. Daily team huddles with physicians, staff, and leadership increased as electronic means of communication were not possible. Multiple in-person debriefings per day occurred with leadership, the IT department, and incident command. Work began with understanding what information was available, what was missing, and how we could obtain it. Subteams were created to assign specific tasks within the radiation department such as creating a paper chart, collating all the required information from a variety of sources (ie, Pinnacle plan, printed care plans, and reports), performing quality assurance checks, creating schedules, and communicating with patients.

## Immediate Response to Treat Patients Without OIS

On the third day of downtime (January 18, 2019), all stakeholders in the radiation treatment department decided that radiation therapy (RT) patients could be safely treated without OIS functionality. This decision to treat without an integrated OIS was done with the knowledge that the break in radiation oncology patient treatments was bordering on being unacceptably long because of accelerated repopulation, which can lead to a loss in local tumor control, especially for squamous cell head and neck, squamous cell cervix cancers, and non-small cell lung cancer.[12] Another solution that was considered was to transfer patients to a nearby cancer center; however, because of the long distances that patients and caregivers would need to travel and the impossibility of transferring all the required patient information, it was deemed necessary to perform treatments locally, without OIS integration.

The RT department worked to reconcile the current treatment status including number of fractions given, total number of fractions prescribed, dose per fraction, treating radiation oncologist, and patient contact information. The patient record was recreated by 2 independent groups using different information to parse the patient treatment record. The RT department used daily printouts of the booking clerk's list, which provided identification (ID) number, date of birth, and phone number, and the TPS locked plan provided the total fractionation for that patient as well as setup instructions, which were combined with radiation review master list printouts that provided the radiation oncologist the current state of their patients on treatment including total fractionation and number of fractions given. A master list was constructed with this information, and the RT department consulted with all radiation oncologists regarding whether there were any planned holds, stops, or restarts assigned to any patient treatments. In parallel, the medical physics department used machine LINAC log files to create an independent list of patient names, IDs, total fractionations, and number of fractions given, which we were able to create for all of our LINAC types. This was done by reading specific LINAC log files (Varian Clinac - Dynalogs, Varian Truebeam - Trajectory log files, and Elekta Ebin/Elog log files) from a network drive that was fortunately not affected by the virus and writing simple scripts to extract relevant information into a spreadsheet for further analysis. The master list from RT and medical physics lists were compared against each other to validate that all patients on treatment were captured with their current fractionation status.

The RT staff contacted patients and created a treatment schedule. Extra treatment time was given for every patient to ensure all safety checks could be performed adequately. Further to this, the RT manager coordinated staff and ensured that adequate staff were in place to treat patients safely. This included adding a treatment planner as a third therapist on the treatment unit to assist with any troubleshooting and to act as an additional “checker.” Shifts were also reassigned to ensure staff had at minimum 1 day “rest” during the 5 days of down-time.

The medical physics group had concluded that treatment on both Varian Clinac iX and Varian Truebeam was possible using file mode, where DICOM-RT files are loaded directly from the treatment console.[10,11] When the Clinac 4DITC console receives DICOM-RT plan files from the OIS, they are stored on the local console in an incoming-outgoing directory, which allowed us to find DICOM-RT plans for all of our patients already on treatment on the Clinac machines. For our clinical configuration, these files are different from the DICOM-RT plan files from the TPS, which are not able to be treated on the Clinac console because they do not contain a treatment time, a tolerance table, imaging fields, and required extended interface data. In addition, it was determined that treatment on Elekta LINACs in service mode is technically possible with full manual couch position adjustment cone beam CT (CBCT)−based image guided radiation therapy (IGRT). The medical physics department determined that there were 4 unique safe ways to treat patients:

1. Orthovoltage with manual monitor unit calculation for patients on treatment.
2. Manual sim and treat with kV imaging and clinical mark-up for new start emergency patients with radiation oncologist present to determine field placements with only rectangular fields allowed for Clinac, Truebeam, and Inifinity LINACs.
3. Treatment using file mode with kV IGRT with manual couch motion for patients already on treatment for Clinac and Truebeam LINACs.
4. Treatment using file mode in service mode with kV CBCT IGRT with manual couch motion for patients on treatment for Elekta LINACs.

All patients treated in file mode that were deemed to be complex as having intensity modulated radiation therapy or volumetric modulated arc therapy went through our routine pretreatment patient-specific quality assurance process, which consisted of a measurement using an ArcCheck diode array (SunNuclear, Mebourne, FL) before treatment to ensure data integrity on the console. All treatment plan pretreatment patient-specific quality assurance measurements were evaluated using the inhouse standard of gamma (3%, 2 mm) >90%. The Pinnacle TPS workstation was tested for functionality and network connectivity and then placed at the LINAC consoles to provide setup information such as shifts from patient marks and to aid in 2-dimensional kV matching by providing rendering of 2-dimensional orthogonal digitally reconstructed radiographs, which the therapists used to visually assess patient kV images. For this reason it was critical to place the workstation beside the IGRT workstation.

The radiation oncology group prioritized patients into 3 priority groups that were ultrahigh priority, high priority, and medium priority with 6, 9, and 13 patients in each group, respectively, with head and neck, brain, gynecological, esophagus, and anus patients making up the ultrahigh and high priority groups. The remainder of the patients on treatment were to be treated after the higher priority patients received their fractions. The radiation oncology staff also reviewed and signed paper copies of all new prescriptions for patients on treatment as printouts from our TPS indicating what fraction they were on and giving RT staff an indication that treatment was requested by the treating physician. In addition, 1 emergency patient with a cord compression was treated at our satellite clinic with a clinical mark-up at the treatment unit, with the radiation oncologist present for field setup and treatment.

There were 69 treatment fractions given over 5 days using 1 of the 4 treatment procedures. The most common procedure involved continuing treatments of previously treated patients using Clinac file mode (57 treatments), followed by manual sim and treat for new starts (7 treatments), followed by orthovoltage patients already on treatment (4 treatments), and, finally, there was 1 patient

**Table 1 Major challenges, effects, and possible solutions**

| Major challenge | Effect | Solution |
|---|---|---|
| Uncertain timeline of OIS repair | Unacceptable delays in radiation therapy may affect local control, disease progression, and symptom control. | Determine acceptable timeframe for downtime before a contingency plan is enacted or patient is sent to another treatment center. |
| Unknown pertinent information for patients on treatment | Patients may miss treatment or receive excessive treatment, causing harm. | Establish plan to capture relevant patient information outside of OIS on a regular interval, including patient demographics, fractionation, status within treatment.<br>Explicit communication with each radiation oncologist was done to ensure that all patient hold orders were documented. |
| No contingency plan created | Unable to safely treat patients when needed; unnecessary stress on staff; potential for treatment errors | Develop a contingency plan for unexpected downtime relevant for your equipment and various downtime scenarios. |
| No detailed instructions for staff to treat without OIS | There is a much higher potential for errors when not following standardized procedures. | Establish a process for treating patients, prescribing treatment, recording treatment, and documenting treatment. |
| Unknown status of critical backups | Critical backups may not be available when needed. | Work with information technology department to establish the nature, frequency, and availability of backups from critical systems. |
| Status of OIS postrepair not known | OIS may not perform as expected postrepair. | Perform acceptance procedure of OIS with special attention paid to validity of historical records. |
| Records of patients treated outside of OIS not in OIS postrepair | Patients can receive too many treatments if records in OIS are not accurate. | Ensure that all patients treated outside OIS are manually recorded before returning to system for clinical use. |

*Abbreviation:* OIS = oncology information system.

treated using an Elekta LINAC, who was deemed ultrahigh priority by the radiation oncology team (1 treatment). No treatments were performed on the Varian TrueBeam LINAC because it is primarily a stereotactic machine and no TrueBeam patients were deemed ultrahigh or high priority, and the downtime procedure lacked advanced IGRT capabilities necessary for stereotactic treatments. Despite the difficulties with recreating patient treatment information without the OIS, there were no instances of fractionation errors by delivering extra treatment fractions due to having an incomplete patient treatment record. The manufacturer's support personnel were able to come on-site to restore the OIS from backups late in the day on January 19, resulting in a total of 4 days of downtime. Once OIS was validated and tested for functionality, all treatments delivered during the down-time were manually recorded to ensure an accurate and up-to-date treatment record before resuming treatments with OIS functionality on January 20 on all linear accelerators. This included a verification by a second therapist to ensure the accuracy of the electronic record and the paper record.

A summary of the major challenges faced by our group along with their effects and possible solutions are presented in Table 1. It should be noted that a recent report of 3 cyberattacks at facilities noted that 1 of the 3 facilities had treatments delivered by +/− 1 fraction, which is a potential effect for 2 of the major challenges included in Table 2.

## Future Preparedness and Mitigation Strategies

The IT department has significantly enhanced our network security by creating local initiatives, such as making

**Table 2 Contingency plan components for a plan without OIS availability**

| Contingency plan component | Responsible parties | Description |
|---|---|---|
| Understanding your equipment | MP, RT, IT | Understand your local TPS, OIS, and linear accelerator configuration and determine how your clinic could safely operate without TPS, OIS, or TPS and OIS. |
| Recover patient information for on treatment patients | RT, IT | Develop a plan to have an offline repository of all required patient information (name, date of birth, identification, site, fractionation, current status within treatment, other medical info). |
| Develop safe pretreatment QA checks for operation without OIS | MP, RT | Develop plan for QA checks for treatment without OIS, including patient-specific QA and pretreatment plan verification. |
| Develop plan to treat without OIS | MP, RT | Understand the capabilities of treating without records and verify for each linear accelerator type and develop plan.<br>Develop secure repository of setup and imaging instructions for all sites.<br>Printout (preferably electronically) setup instructions for all patients from TPS. |
| Develop plan to record patient treatments without OIS | MP, RT, RO | Develop a plan to treat patients currently on treatment and patients who need emergent treatment. |
| Develop plan to prioritize patients on treatment | RO | Develop an evidence-based plan to prioritize which patients cannot sustain a break in their treatment course based on best available evidence.[12] |
| Understand and monitor vendor recommendations for IT security and unexpected downtime | IT, MP | Understand vendors' expectations of IT security, backup frequency, and unexpected downtime recovery scenarios. |

*Abbreviations:* IT = information technology; MP = medical physicists; OIS = oncology information system; QA = quality assurance; RO = radiation oncologists; RT = radiation therapists; TPS = treatment planning system.

staff aware of the dangers of clicking on unknown links within email, increasing the complexity and frequency of password updates for domain level access, and improving network security protocols. The specific initiatives undertaken by our IT team are outside of the scope of this report, but an in-depth review of our IT vulnerabilities was done after the cyberattack to better secure our IT infrastructure.

The main elements required for a contingency plan to treat without OIS include a number of elements that are summarized in Table 2.

We have considered how to be better prepared for knowing the current status of patients on treatment, and to that end the RT manager pulls 2 reports from our OIS on a weekly basis. The first is a report that outlines all patients scheduled for treatment for the current week, including their treatment unit appointment time, name, patient ID, and contact information. This is also done on a daily basis by the booking staff to include any changes and/or updates. The second report contains all patients for a given radiation oncologist, including their name, ID, and current fractionation status. A date and time stamp on the report allows the information to be reconciled with log files if required. A daily report is also automatically produced multiple times a day that shows any hold, stop, or resume orders.

We have developed contingency plans for 2 common Varian LINAC models: TrueBeam and Clinac iX for both patient on treatment and for new patient starts. The improvements upon the contingency plan described include the ability to perform daily CBCT and apply shifts and the ability to start new patients. In order for the contingency plan to work, the data from the TPS needs to be processed through an in-house developed Python code, so that the LINAC console will accept it. In the case of the Truebeam LINAC, the initial table top positions are populated before being sent to the treatment console. In the case of the Clinac iX, a tolerance table is added, an imaging CBCT beam is added, and extended interface data that are needed for the 4DITC console are added as a private DICOM tag in XML format. The downtime procedures and a repository of the necessary code are kept off the hospital network so that it will remain accessible in the event of a cyberattack. The downtime procedures are to be tested annually and after any major upgrade of the TPS, OIS, or LINAC console software.

An additional contingency plan that we are exploring is to have an offline backup OIS installation with no patient records, configured with our local settings (user profiles and machine characterizations) and able to communicate with the linear accelerators. In the event of OIS downtime, the backup OIS can be powered up and brought online to act as a temporary OIS, allowing for full functionality including CBCT imaging and record and verify capabilities, opening the door for safe and seamless delivery across all linear accelerator types, assuming that the TPS treatment plans can be transferred over safely. The disadvantages to using an offline backup configuration would be cost, time to configure, and time required to maintain the system with routine upgrades and testing.

One final point is that IT departments should work closely with radiation oncology departments and understand the latest recommendations from vendors. Recently, 2 of the largest radiation oncology companies have released recommendations related to cybersecurity. In 2020, Varian released a customer technical bulletin that outlined the general security guidelines around ransomware for Varian products.[13] A 2021 document that was released by Elekta outlines good antimalware strategies, disaster recovery suggestions, and a process to restore Elekta's MOSAIQ OIS after a catastrophic loss.[14]

## Discussion

Although this document explicitly details our experience with a cyberattack, a more correct term should be "unexpected downtime" of the OIS, which can result because of a number of factors including a cyberattack, natural disaster, flood, fire, failed upgrade, or other causes.

In this document, we have dealt explicitly with OIS downtime, which we believe is the most likely downtime possibility for our clinical configuration; however, it is possible that a future downtime event could include any combination of TPS/OIS//LINAC console, resulting in different crippling scenarios. However, a recent report that outlines 3 cyberattack scenarios at cancer centers denotes 2 cases of OIS alone being offline and 1 case of both OIS and TPS being affected by a cyberattack.[15]

The effect of the COVID-19 pandemic on the workforce has resulted in a shift from workers working in person to working remotely by being able to connect and attend meetings using virtual connections. However, cybercriminals are using these increased potential connections to infiltrate network resources. The International Criminal Police Organization has issued a press release specifically detailing how cybercriminals are using COVID-19−specific messaging through online scams and phishing, disruptive malware including ransomware, data harvesting malware, and malicious domains.[16]

This article adds to the literature describing individual radiation oncology departments involved in cyberattacks.[4,15,17] The common messages across all articles are to develop contingency plans, store patient information out of the OIS for review, store policies and procedures for imaging and treatment, and consider offline backup offline OIS servers. The novel points brought forward in our experience are the value of LINAC log files in recreating the patient treatment record, to work closely with IT to understand the frequency and usability of important backups, and, finally, to monitor vendor recommendations regarding cyber security and work with them and IT to protect mission critical software systems.

## Conclusion

In addition to IT personnel, radiation oncologists, medical physicists, radiation therapists, and hospital administrators should be aware of a potential cyberattack in a radiation oncology department and have a contingency plan in place. This paper outlines how our department was unprepared to deal with a cyberattack, yet we were able to safely treat patients without an OIS largely because of hard work and teamwork. We also outline our future preparedness by presenting a contingency plan to be put in place for a future unexpected downtime event such as a cyberattack.

## References

1. U.S. Department of Health and Human Services. Fact sheet: Ransomware and HIPAA. Available at: https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf. Accessed October 30, 2021.
2. Bhuyan SS, Kabir UY, Escareno JM, et al. Transforming healthcare cybersecurity from reactive to proactive: Current status and future recommendations. *J Med Syst*. 2020;44:98.
3. Sophos Annual Ransomware Survey. The state of ransomware 2021. Available at: https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf. Accessed October 30, 2021.
4. 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.
5. Recent Cyberattack Disrupted Cancer Care Throughout U.S. Available at: https://www.webmd.com/cancer/news/20210720/recent-cyberattack-disrupted-cancer-care-us. Accessed February 14, 2022.
6. McNamee MS. HSE cyber-attack: Irish health service still recovering months after hack. Available at: https://www.bbc.com/news/world-europe-58413448. Accessed October 30, 2021.
7. New Zealand Herald. Radiation therapy resumes for cancer patients. Available at: https://www.nzherald.co.nz/nz/waikato-dhb-cyber-attack-radiation-therapy-resumes-for-cancer-patients/OZY274V5UL3F2KWBATCR2RDNEM/. Accessed October 30, 2021.
8. Zhang B, Chen S, Nichols E, D'Souza WD, Prado K, Yi B. A practical cyberattack contingency plan for radiation oncology. *J Appl Clin Med Phys*. 2020;21:181–186.
9. Nelson C, Gifford K, Kisling K, Kirsner S. SU-E-T-215: A technique for treating patients outside the Mosaiq R&V System for TrueBeam Users (or 4DTC). *Med Phys*. 2012;39:3752–3753.
10. Varian Medical Systems, Inc.. *Clinac DICOM-RT Mode Reference Guide*. Palo Alto, CA: Varian; 2017.

11. Varian Medical Systems, Inc.. *Truebeam 2.7 Instructions for Use*. Palo Alto, CA: Varian; 2017.
12. Royal College of Radiologists (UK). The Timely Delivery of Radical Radiotherapy: Guidelines for the Management of Unscheduled Treatment *Interruptions*. 4th ed. London: The Royal College of Radiologists; 2019.
13. Varian Medical Systems, Inc. *Recommendations on Securing Customer Purchased Varian Products from Ransomware*. Palo Alto, CA: Varian; 2020.
14. Elekta AB. *MOSAIQ® 1.1 - 3.1 System Requirements for Elekta Oncology Management System*. Stockholm, Sweden: Elekta; 2021.
15. Pinkham DW, Sala IM, Soisson ET, Wang B, Deeley MA. Are you ready for a cyberattack? *J Appl Clin Med Phys*. 2021;22:4–7.
16. INTERPOL. INTERPOL report shows alarming rate of cyberattacks during COVID-19. Available at: https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19. Accessed October 30, 2021.
17. 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. S1879-8500(21)00275-7.