

Scientific Article

Effect of the Cyberattack Targeting the Irish Health System in May 2021 on Radiation Treatment at St. Luke's Radiation Oncology Network



Clare Faul, MB, MRCPI, FFRRCSI,*
Jacqueline Robinson, BSc, PG Dip Clin Pharm, MPSI, MBA,
Jennifer Carey, RGN, RCN, H DIP HRS, BSc, MBS HRS,
Orla McArdle, MB BCh BAO, FFRRCSI, MSc, Laoise Ryan, BSc, MSc,
Ruth Woods, BSc, MSc, and Brendan McClean, BSc, PhD, MBA

St. Luke's Radiation Oncology Network, Dublin, Ireland

Received December 15, 2021; accepted April 7, 2022

Abstract

On May 14, 2021, the Health Service Executive (HSE) of Ireland experienced a major ransomware cyberattack. The HSE initially took down all of its information technology systems to protect its core systems. All Internet connections within the HSE were unavailable from 7 AM for approximately three weeks which had a major effect on the radiation oncology service nationally within the public service. St. Luke's Radiation Oncology Network (SLRON) is a complex, 3-center radiation oncology service, and it is the largest in the country; with 14 linear accelerators, it is one of the largest radiation centers in Europe. This article details the response of SLRON to the outage resultant from the cyberattack. Although the outage affected all patient services, including laboratory, diagnostic imaging, and inpatient care, the article primarily focuses on our response to get the radiation oncology service restarted as quickly as possible and details the steps we took to reinstate our systems safely, how we prioritized patient treatments, and how we communicated with patients, staff, and the public without having access to standard communication pathways. All decisions were risk assessed and were made with the best resources available to us at the time to maximize the outcome for our patients and mitigate significant delays. The risk remains ongoing, and the onerous task of uploading backlogs and reconciling patient records is a continuing risk.

© 2022 The Authors. Published by Elsevier Inc. on behalf of American Society for Radiation Oncology. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

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: All data generated and analyzed during this study are included in this published article and its supplementary information files.

*Corresponding author: Clare Faul, MB, MRCPI, FFRRCSI; E-mail: clare.faul@slh.ie

<https://doi.org/10.1016/j.adro.2022.100993>

2452-1094/© 2022 The Authors. Published by Elsevier Inc. on behalf of American Society for Radiation Oncology. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

Introduction

On May 14, 2021, the Health Service Executive (HSE) of Ireland suffered a major ransomware cyberattack. The HSE initially disabled all of its information technology (IT) systems to protect its core systems. The IT network connections within the HSE were unavailable from 7 AM, for approximately three weeks which had a major effect on the Irish public radiation oncology service.

St. Luke's Radiation Oncology Network (SLRON) is a complex, 3-center radiation oncology service in Dublin, Ireland. With 14 linear accelerators, it is the largest center in the country and one of the largest radiation centers in Europe. The network consists of a hospital site called St. Luke's Hospital and 2 linked centers on acute hospital campuses: SLRON at St. James's and SLRON at Beaumont. There are 3 linear accelerator types across the network. St. Luke's Hospital has 2 Varian TrueBeams and 4 Elekta Synergy linear accelerators. The centers at Beaumont and St. James have 4 Varian Clinacs each. SLRON treats more than 5000 new patients per year and provides specialized services such as pediatric radiation, total body radiation, brachytherapy, SABR, and stereotactic radiosurgery treatment. As a single governance network across the 3 locations, we are very reliant on connected technology. This configuration made SLRON particularly vulnerable to the loss of connectivity experienced in response to the cyberattack. The resulting consequences of the cyberattack were severe and the process of resolution was complex.

St. Luke's Radiation Oncology Network uses Varian Medical Systems's Oncology Information System ARIA (version 16.0) as a single network-wide electronic health record. Beaumont and St. James operate a paperless environment. St. Luke's Hospital's radiation therapy department is paperless, and the remainder of the hospital uses minimal paper. ARIA also serves as the record and verification system for the 10 Varian linear accelerators in the network. The remaining linear accelerators—the 4 Elekta machines—use Elekta's system Mosaiq (version 2.5) record and verification system. Varian's Eclipse is used for all patient contouring and for treatment planning for all patients on the Varian linear accelerators. Patients on Elekta linear accelerators are planned using Elekta's Monaco or Oncentra Masterplan.

This review article details the response of SLRON to the outage resulting from the cyberattack. Although the outage affected all patient services, including laboratory, diagnostic imaging, and inpatient care, this article primarily concentrates on our response to get the radiation oncology service operational as quickly as possible. The article gives details on the steps we took to reinstate our systems safely, how we prioritized patient treatments, and how we communicated with patients, staff, and the public without having access to standard communication pathways. All decisions were risk assessed and were made with

the best resources available to us at the time to maximize the outcome for our patients and mitigate significant delays. The risk remains ongoing, and the onerous task of uploading backlogs and reconciling patient records continues.

SLRON's response

The IT servers that host ARIA are all located in the center in St. James. All the servers were disconnected and, as a result, all the linear accelerators and planning terminals were shut down across SLRON. Wi-Fi, email access (internal or external), and web-based phone and video systems were all unavailable. Landline phones were working in St. Luke's Hospital and the center in Beaumont but not at the center in St. James. There was no access to patient information or contact details except for some limited information from the linear accelerators. At the time of the cyberattack, SLRON had 304 patients undergoing treatment across the 3 sites. An additional 17 patients were ready to start treatment on May 14 (day 1). A further 201 patients were within the planning care path (had undergone a planning scan).

A single emergency management group made up of senior management, clinical leads, physics, radiation therapy leads, administration, and IT (internet) leads was established early on day 1. This group, named the IT (Internet) emergency management group, was tasked with making all the critical decisions in the network. All other management committees were suspended. The key decisions made during the first days of the outage to ensure patient safety are outlined in [Table 1](#).

Restoring Connectivity

St. Luke's Radiation Oncology Network has two IT groups: Clinical IT (ICT) and Network IT. Both groups started working immediately on a solution to get ARIA and the linear accelerator machines functioning safely. Contact was established and help was provided by the 2 linear accelerator companies, along with other external IT providers. Contract cyber security consultants provided an experienced incident manager to make essential changes on the IT network, to build up an action plan, and to help make sensitive decisions. A point-to-point virtual private network was set up on the firewalls to make the ARIA and Elekta equipment accessible for the support teams.

The IT groups commenced the large task of loading software on each device to sweep the system and detect compromised devices. IT management decided the surest way of restoring some ARIA access was to create an internal closed IT network for ARIA in SJC where the ARIA servers are located. On Saturday, May 16 (day 2), ARIA

Table 1 SLRON key decisions

<p>Governance</p> <p>A single emergency management group was established.</p> <ul style="list-style-type: none"> • Chaired by the network director and met daily • Oversight of decisions made on prioritizing patient treatment (Appendix E1) • Decisions made to send emergency/urgent patients to private sector <p>The NCCP established a cyberattack group.</p> <ul style="list-style-type: none"> • Chaired by director of NCCP • Forum for communication among Irish public radiation oncology centers and the HSE • Included clinical leads, radiation therapist leads, and physicist leads of radiation oncology centers in Ireland
<p>Operational issues regarding treatment delivery</p> <ul style="list-style-type: none"> • Pathways were set up for patients to transfer to the private sector. • BC, SJC, and SLH clinical leads and radiation service managers communicated daily to prioritize patient categories and review the available capacity. • BC and SLH hubs were set up in SJC, which were staffed by the local RTSM and clinical lead once SJC had ARIA access. • Once some connectivity was restored in SJC, rotas were created for access to the limited personal computers with ARIA. • Staff agreed to an extended working day from 8 AM to 8 PM. • Treatment details were manually recorded on paper charts when required (SLH Elekta). • Immobilization equipment was transferred between radiation centers. • Systems were introduced in ARIA to indicate patients on hold, and quality assurance systems continued and were prioritized to mitigate risk: weekly chart checks, treatment verification, and additional final dose checks. • A new paper booking form and processes for new referrals were established. • All diagnostic scans had to be burnt onto CDs for planning because the National Integrated Medical Imaging System was unavailable.
<p>Communication</p> <ul style="list-style-type: none"> • Communication with patients <ul style="list-style-type: none"> ○ Those who were on treatment were contacted, and their treatments were initially canceled until further notice. Updates were given by treatment unit staff to these patients regularly during the outage. ○ A central phone number for patients was established and circulated via HSE communication pathways (eg, HSE webpage, Twitter). • Communication with staff <ul style="list-style-type: none"> ○ Managers set up contact lists for staff to communicate using the WhatsApp and Facebook Messenger apps. ○ Regular walk-arounds were carried out by line managers to keep staff updated. ○ The single emergency management group communicated using a messaging app. • External communication <ul style="list-style-type: none"> ○ Media queries were processed centrally through the general manager’s office and directed to the HSE ○ The Siilo medical messenger platform was set up in SLRON for communication with doctors in the private radiation centers and with doctors making new patient referrals.
<p>Clinical care</p> <p>As there was no access to patient information, urgent medical clinics were established in all 3 centers.</p> <ul style="list-style-type: none"> • Paper charts were created to record decisions on patients and were subsequently uploaded to ARIA when available; patient visits were manually recorded. • A nursing or advanced nurse practitioner phoned patients to ensure no review appointments were missed. • Urgent results were communicated through the medical messaging app. • A cardiac bleep system backup was established in SJC because the phones in SJC were not connected. This is a secure and real-time communication solution over radio frequency in the SLH’s Rathgar site. <p><i>Abbreviations:</i> BC = Beaumont center; HSE = Health Service Executive; NCCP = National Cancer Control Program; RTSM = Radiation Therapy Services Manager. SJC = St. James center; SLH = St. Luke’s Hospital.</p>

was isolated and connected to 1 clean computer. The radiation therapy service manager and administration staff printed patient lists for all 3 centers.

Once the isolated network was established and deemed safe, the 4 linear accelerators in SJC were connected and limited treatment recommenced using 6 MV on Monday, May 18 (day 4). The site that was

least compromised was St. James. This was because the ARIA servers were located on that site, so a closed network could be created on that site without any reliance on external servers.

Once St. James was operational, IT began working on connecting St. Luke’s Hospital and Beaumont to the same closed network without using the HSE network cables. St.

Table 2 Patient categories resuming radiation therapy treatment in SLRON (excludes new patients)

Day	Date	Patient categories	Centers with operational linear accelerators
Day 1	Friday, May 14, 2021	None	None
Day 2	Saturday, May 15, 2021	None	
Day 3	Sunday, May 16, 2021	None	
Day 4	Monday, May 17, 2021	Category 1 in SJC, BC Urgent palliative from SJC, SLH, BC	SJC
Day 5	Tuesday, May 18, 2021	Pediatric from SLH Category 1 from SLH TrueBeams	
Day 6	Wednesday, May 19, 2021	Category 1, 2A, 2B from SLH Elekta Category 2A (excluding breast) from SJC, BC	SJC, SLH Elekta
Day 7	Thursday May 20, 2021		
Day 8	Friday, May 21, 2021		
Day 9	Saturday, May 22, 2021	6 SABR lung, 2 SABR prostate (SJC)	
Day 10	Sunday, May 23, 2021		
Day 11	Monday, May 24, 2021	Category 1, 2A, 2B in BC (most had treatment day 4-8 in SJC)	BC, SJC, SLH Elekta
Day 12	Tuesday, May 25, 2021		
Day 13	Wednesday, May 26, 2021		
Day 14	Thursday, May 27, 2021		SLH TrueBeams
Day 15	Friday, May 28, 2021		

Abbreviations: BC = Beaumont center; SJC = St. James center; SLH = St. Luke's Hospital.

Luke's Hospital resumed treatment on the Elekta machines on Wednesday, May 20 (day 6) by creating a closed network for Mosaiq. Beaumont was connected to ARIA on Monday, May 24 (day 11), and the TrueBeams in St. Luke's Hospital finally resumed treatment on Thursday, May 27 (day 14). Access to ARIA on personal computers was very limited because many were corrupted. This proved to be one of the most challenging issues once treatment resumed because ARIA is required by every health care professional to provide care to patients.

The timeline showing which centers were operational and which categories of patients resumed treatment is shown in [Table 2](#).

Clinical Prioritization

The St. James and Beaumont centers have the same treatment machines, so urgent patients from both centers could restart treatment in St. James without replanning. The option of replanning patients mid-treatment in the private sector without access to initial plans or images was deemed high risk, so with 4 machines available, category 1A patients were prioritized to restart treatment.

St. Luke's Radiation Oncology Network is the only radiation therapy department in Ireland that treats pediatric patients, so these patients were deemed a priority group for resuming treatment (a total of 9 children). The emergency management group and pediatric radiation oncologists risk assessed the options of breaking the children's treatment or replanning and moving the patients, anesthetic equipment, and immobilization equipment to the available linear accelerators in St. James. The IT management group determined that continuing their treatment was the best solution. The radiation therapist treatment planners and pediatric radiation oncologists replanned all 9 patients. The consulting anesthetist was indemnified by the HSE and agreed to move to the available center. The anesthetic equipment was transported to St. James and all the pediatric patients restarted radiation therapy on Tuesday, May 18 (day 5).

All patient groups and options for providing safe care were considered. All urgent stereotactic radiosurgery patients were outsourced to the private sector, as stereotactic radiosurgery is normally only available in Beaumont. These patients included those in mid-treatment. All category 1 and 2A patients from Beaumont and St. James had restarted treatment by day 5. Twice-daily treatment was introduced as gap compensation, and 1 such treatment was needed for this group.

Replans were required for several patients: Elekta category 1 and pediatric patients on Eclipse for Clinacs in St. James; patients from the TrueBeam in Eclipse for Clinacs in St. James and from TrueBeam on Oncentra Masterplan for the Elekta linear accelerators; and patients on the stereotactic radiosurgery unit in Beaumont with ExacTrac imaging with larger margins in Eclipse for Clinacs in St. James.

The next group to be prioritized category 1 were those patients who had been due to start treatment. Planning urgent new category 1 patients restarted on Wednesday, May 19 (day 6).

High-dose-rate brachytherapy and contact radiation therapy (CXT) patients restarted in St. Luke's Hospital because these machines are not linked to the HSE network and were not affected by the cyberattack. Clinical details were accessible via ARIA on a limited number of computers in St. James. Patients with cervical cancer were prioritized for high-dose-rate brachytherapy. The nuclear medicine restarted in St. Luke's Hospital on Monday, May 24. A backup uncorrupted, calibrated personal computer was available for nuclear medicine.

Patients with lung and prostate cancer already planned for SABR were treated out of standard hours over the weekend (May 22 and 23, days 9 and 10). Outsourcing to the private sector continued and expanded to include all available capacity in the private sector.

All new referred category 1 patients began radiation treatment by the end of week 1, and new category 2A patients began treatment by week 2. Once a patient started or resumed treatment, they continued until their treatment course was completed.

As the weeks went on, more personal computers were deemed safe and became available for use. Extra checks on the final dose delivered were instigated to mitigate any risks in view of changes introduced in the patients' care paths. Linear accelerators not in use were used by clinical engineering for preventative maintenance so that machine downtime would be minimal once connectivity was restored.

The IT staff involved in managing the cyberattack included 5 permanent IT staff in SLRON who worked with 2 outsourced technicians. An IT incident manager was recruited to oversee the IT work during the cyberattack. Firewall engineers worked on a shift rota over 2 weeks. External companies providing support included information security companies (Kedington [part of the Excel/Redstone Group], Vodafone, Accenture plc, Mandiant, Caveo) and the Varian Quadris cloud service. The physics staff included 10 clinical engineers and physicists.

For smaller radiation centers, we would recommend a support contract with a third-party security specialist as well as a managed firewall service contract. This support would allow an incident manager to schedule actions based on the priorities for the hospital's operations.

Risks Remaining After Connectivity Was Restored

SLRON had to (and continues to) consider the risks that remained after connectivity was restored in those initial weeks. These risks include the following:

- Potential future cyberattacks and the need for additional funding to build resilience both internally and nationally
- Reliance on small numbers of key staff
- Uploading backlogs and reconciling all patient records
- Identifying, reporting, and managing incidents without access to online reporting software
- Difficulties in reconciling manual (paper) reports to online reports, increasing the risk of transcription errors
- Potentially introducing delays for clinical reviews of patients when routine outpatient clinics are canceled (which may have clinical consequences for patients)
- Potentially introducing administrative errors when staff relies on paper records and limited information during the attack; this risk includes loss of patient data and General Data Protection Regulation (GDPR) breaches
- Potential for staff burnout and stress overload

Lessons Learned: What Went Well?

As the acute phase of the effect of the cyberattack passed and the network worked to address residual risks, the staff reflected on what went well. The following points summarize some of the key areas that worked well and what we learned in the speedy resumption of safe services for our patients:

- The most important decision in managing this emergency was initially establishing a high-level emergency governance group of key staff members who had the ability to make quick decisions. Introducing a stable communication pathway using the WhatsApp messaging app between leads and staff, as well as the use of a medical messaging App (Siilo) for doctor-to-doctor communication, allowed decisions to be disseminated quickly, which worked very well. In our case, dynamic decision-making in a stressful environment was important. Experienced staff members took leadership roles that were enhanced by the previous management of an ARIA outage in 2019.
- Having skilled IT and clinical IT staff available on-site with in-depth knowledge of the complex IT system in the network was critical to getting the

radiation service back in a short timeframe. SLRON recognized that in-house knowledge was vital to getting the network back online without delays that could have ensued if SLRON were fully reliant on HSE IT, which has limited knowledge of the complexity of the IT network in SLRON. Waiting for central HSE decisions would have delayed our recovery.

- Representation from IT/clinical IT at senior management hospital level is required and will be introduced in the future.
- The fact that we had a previous ARIA outage (after an ARIA upgrade) in 2019 provided us with experience in prioritizing staff access to limited ARIA terminals.
- SLRON advises that radiation centers introduce protocols in the event of limited online access to patient records. These protocols should also be accessible outside of a potential outage.
 - Reliance on key staff with knowledge of the IT network was important for reinstating service as quickly as possible. However, this reliance remains a risk because of the potential of the limited number of staff members undergoing undue stress and developing burnout. We set up a well-being program for staff led by our Arts Center coordinator. Examples of events included a staff portrait project, a day of music and art in SLH, establishing a mindfulness walkway in SLH, and mindfulness rooms in BC and SLH. Rest days were introduced for IT and clinical engineering staff to help reduce burnout.
- SLRON recommends that additional key IT and clinical IT staff be recruited. These staff members could be trained and resourced to serve as an expert hub in radiation oncology for the NCCP/HSE nationally.
- External companies' support to SLRON's IT service was critical. We recommend that this support remains a key component of service contracts.
- It would be helpful if agreements for extended work hours—longer workdays and weekend work hours—were in place nationally for emergencies.

- Use of messaging apps for patient communication is very helpful and should be encrypted for sharing patient data.
- Prior agreements prioritizing patient categories should be established both nationally and internationally to ease management of future crises.
- Each key decision should be risk assessed using a predetermined template.
- Central communication with patients and the media by the HSE worked well to reduce stress on frontline staff in the network.
- HSE daily briefings were helpful in informing the network of the progress of the cyberattack nationally.

Conclusion

The ransomware cyberattack had an unprecedented effect on the safe and ongoing delivery of a vital radiation oncology service within SLRON and throughout Ireland. The fact that the network was up and running so quickly is testament to the resilience and quick action of our staff—clinical, administrative, operational, and managerial. The management of the previous ARIA outage and the COVID-19 pandemic had provided the senior decision-makers with crisis experience, which helped us set up our pathways quickly. Significant help and advice was provided by the Dublin Midlands Hospital Group, the HSE, our host hospitals, and the National Cancer Control Program. We hope our report on the cyberattack and some of the key decisions we made will help other radiation centers both nationally and internationally. Our management team and IT services are available for any advice moving forward.

Supplementary materials

Supplementary material associated with this article can be found in the online version at [doi:10.1016/j.adro.2022.100993](https://doi.org/10.1016/j.adro.2022.100993).