Advances in Radiation Oncology (2021) 6, 100796

advances in radiation oncology

www.advancesradonc.org

Evolving Threats in Cybersecurity and Radiation Oncology

Emerging Cybersecurity Threats in Radiation Oncology

Christine Joyce, BS,[a] Faustin Laurentiu Roman, MSc,[b] Brett Miller, MS, MBA,[c] John Jeffries, BS,[d] and Robert C. Miller, MD, MBA, FASTRO[c,*]

[a]University of Tennessee Health Science Center College of Medicine, Memphis, Tennesse; [b]Medical IT Advisors, Auckland, New Zealand; [c]Division of Radiation Oncology, University of Tennessee Medical Center, Knoxville, Tennessee; [d]Information Security, University of Tennessee Medical Center, Knoxville, Tennessee

Received June 28, 2021; revised August 18, 2021; accepted August 22, 2021

Abstract

Purpose: Modern image guided radiation therapy is dependent on information technology and data storage applications that, like any other digital technology, are at risk from cyberattacks. Owing to a recent escalation in cyberattacks affecting radiation therapy treatments, the American Society for Radiation Oncology's *Advances in Radiation Oncology* is inaugurating a new special manuscript category devoted to cybersecurity issues.

Methods and Materials: We conducted a review of emerging cybersecurity threats and a literature review of cyberattacks that affected radiation oncology practices.

Results: In the last 10 years, numerous attacks have led to an interruption of radiation therapy for thousands of patients, and some of these catastrophic incidents have been described as being worse than the coronavirus disease of 2019 impact on centers in New Zealand.

Conclusions: Cybersecurity threats continue to evolve, making combatting these attacks more difficult for health care organizations and requiring a change in strategies, tactics, and culture around cyber security in health and radiation oncology. We recommend an assume breach mentality (threat-informed defense posture) and adopting a cloud-first and zero-trust security strategy. A reliance on computer-driven technology makes radiation oncology practices more vulnerable to cyberattacks. Health care providers should increase their resilience and cyber security maturity. The increase in the diversity of these attacks demands improved preparedness and collaboration between oncologic treatment centers both nationwide and internationally to protect patients.

Introduction

Modern, image guided radiation therapy is dependent on information technology and data storage applications that, like any other digital technology, are at risk from cyberattacks. In the fourth quarter of last year, America's health care institutions were subjected to a series of coordinated attempts to breach their cyber-defenses with criminal intent. Unfortunately, in some cases, these attempts were successful, resulting in a detriment to patient care. According to Cybercrime Magazine, global cybercrime damage in 2021 amounts to $16.4 billion a day, $684.9 million an hour, $11 million per minute, and $190,000 per second.[1] The World Economic Forum estimated that the likelihood of detecting and prosecuting the

Sources of support: None.

Disclosures: Dr Miller reports funding from the American Society for Radiation Oncology. There are no other conflicts of interest.

Research are available at public Internet sites as referenced.

*Corresponding author: Robert C. Miller, MD, MBA, FASTRO; E-mail: rcmiller@utmck.edu

https://doi.org/10.1016/j.adro.2021.100796

perpetrators of cyberattacks in the United States is at a dismal 0.05%.[1]

In the fall of 2020, the U.S. federal government issued a joint advisory warning that the Cybersecurity and Infrastructure Safety Agency, Federal Bureau of Investigation, and Department of Health and Human Services have credible information of an increased and imminent cybercrime threat to U.S. hospitals and health care providers.[2] More recently, the Director of the Federal Bureau of Investigations compared the increase in ransomware attacks on U.S. infrastructure to the threat of the September 11 terrorist attacks.[3] In New Zealand, ransomware incidents have been recently labeled as being worse than the coronavirus disease of 2019 (COVID-19) in terms of their impact on patients with cancer.[4]

As the worst disruptions of the COVID-19 pandemic have passed (at least in some regions), the next pervasive disruptive threat to our medical profession appears to be cybersecurity risks. In light of this development, the American Society for Radiation Oncology's *Advances in Radiation Oncology* is inaugurating a special manuscript category devoted to cybersecurity issues.

Emerging cybersecurity threats in 2021

A study in 2014 showed that 94% of health care institutions have been victims of cyberattacks.[5] Based on a Medical Information Technology Advisors Threat Information Platform analysis[6] of incidents related to the Asian-Pacific, United States, and European Union, as well as various other threat intelligence agencies reports,[7] the number of business e-mail compromise and ransomware incidents from phishing or dark web-compromised credentials are growing and quickly becoming the number one risk for health care organizations. Recent years have seen an increase in phishing occurrences from "trusted" organizations or services that are being abused. Phishing e-mails will often dangle a financial reward or something too good to be true with urgency or a strict deadline to perform an action. Other attempts could be a promise to show something exciting or forbidden or threating with negative consequences or punishment. The phishing e-mail will often have an unexpected attachment, spoofed website, or link to update your password. Call the sender to verify whether the e-mail is legitimate is often best before taking any action.

The United States has seen an increase in ransomware, especially from ransomware as a service groups using double and even triple extortion tactics. Data are encrypted, exfiltrated from the attacked health care organization, and then the groups threaten to publish the data, sometimes directly extort patients, and finally threaten a distributed denial of service attack.[8] In fact, the U.S. Department of Health and Human Services, Health Sector Cybersecurity Coordination Center has found that 60% of global cyber incidents during the first half of 2021 targeting health care providers affected the U.S. health sector.[9] Ransomware incidents are becoming linked to data breaches because in at least 72% of ransomware incidents, victim data were leaked.[10]

In an analysis of 5275 reported cybersecurity breaches last year, the number one method used was social engineering, with 85% of breaches involving a human element in a targeted organization. The threat to health care organizations in recent years has shifted from malicious internal actors to external organization. Personal data, rather than medical data, is the most commonly stolen information in a security breach with financial motivation behind 91% of attacks.[11]

Usual scams tactics, including fear-based themes, prove to be successful with only a few changes in frequency and some techniques abusing legitimate services to bypass protections. Themes on COVID-19, the work from home initiative, registration renewals, secure document exchanges, and even local festivals are used to trick victims into allowing these attacks. Table 1 summarizes some of the COVID-19 themes used in e-crime phishing schemes during the pandemic.[12]

The existing disruptions in health care globally presented new vulnerabilities for cybercrime.[13] Some cybercrime organizations announced their intention to not intentionally impact health care organizations during the pandemic, although how well they adhered to those pledges is unclear. Other organizations, such as Wizard Spider, intentionally targeted health care organizations at the end of October of 2020 at a time of increased medical facility utilization when hospitals and clinics were under increasing pressure from the start of the influenza season and the pandemic fall surge, mirroring a similar approach used against other industries of deliberate targeting at times of institutional stress, such as educational institutions at the start of the 2019 school year.[12]

Table 1 Pandemic-Related Crime Phishing Themes

• Exploitation of individuals looking for details on disease tracking, testing, and treatment
• Impersonation of medical bodies, including the World Health Organization and U.S. Centers for Disease Control and Prevention
• Financial assistance and government stimulus packages
• Tailored attacks against employees working from home
• Scams offering personal protective equipment
• Passing mention of coronavirus disease of 2019 within previously used phishing lure content (eg, deliveries, invoices, and purchase orders)

Malicious actors have made phishing and malware smarter using new techniques to bypass sandbox detonations (ie, artificial network environments designed to trigger malware in a closed network), and are increasingly using "trusted" compromised accounts and services to launch their attacks. Third-party supply chain risks and the Internet of Things environment makes threat management complex and increases the attack surface. The World Economic Forum estimated that attacks on Internet of Things devices soared by 300% in 2019.The increase in the number of individuals now working from home has added additional risks and increased the complexity in combating attacks. Health care organizations are typically attacked by well organized crime and state-sponsored actors. The predicted cost of ransomware damage in 2021 ($20 billion) is 57 times more than the cost in 2015.[1]

Finally, the lack of correlation, collaboration, and communication between service providers and their information technology partners increases the ease with which attackers can affect a wide range of targets. Table 2 summarizes the major risks organizations face.[14]

Cyberattacks Affecting Radiation Oncology Providers

Technological advancements in the treatment of cancer continue to improve patient outcomes. However, due to the reliance on technology, radiation oncology practices are more vulnerable to cyberattacks. In the recent past, radiation therapy treatments could be delivered from information recorded entirely on paper printouts and hand-written charts. Localization was achieved based on gross anatomy or skin markings with wide margins to account for setup error. Therefore, treatment delivery could be isolated from treatment plan creation and was indeed the default paradigm before the invention of record and verification systems. Modern radiation therapy requires the loading and creation of 3-dimensional data sets for localization, and the delivery of a complex treatment plan includes hundreds of control points that each contain hundreds of nodes of data giving the linear accelerator instructions on the positioning of each of its subsystems. The delivery of a single treatment can require the loading, creation, and management of gigabytes of data. This has led to an exponential growth in radiation therapy data, but also to a critical dependence on these vulnerable network systems to deliver treatment.

In 2016, a ransomware attack on a 10-hospital system in the national capitol region resulted in a hospital having to cancel 36 radiation oncology treatment appointments on day 1 of the attack, and all treatment sessions on days 2 and 3 after the attack.[15] In the fall of 2020, there was a series of cyberattacks on U.S. health care institutions nationwide, including one in October of 2020 where the University of Vermont health network experienced a cyberattack that subsequently halted radiation therapy at their facility.[16] In April of 2021, a cyberattack affected Elekta's cloud-based storage system for radiation oncology data and affected 42 sites across the United States out of 170 customers.[17] The Health Service Executive of Ireland was the target of a large-scale ransomware attack on May 14, 2021 that affected almost all of its clinical information technology systems. Two weeks after the attack, approximately 7000 patient appointments per day

Table 2 Cybersecurity Risks in 2021

1	Phishing, including business e-mail compromises
2	Ransomware attacks, including distributed denial of service
3	Hacking of unpatched software and external services (remote desktop protocol, virtual private network, file transfer protocol, databases)
4	Software vulnerabilities, misconfigurations
5	Lack of security logging and monitoring
6	Third-party supplier's security (cloud, Internet of Things, apps)
7	Inadequate processes (eg, patching, backup, change management)
8	Technical debt/legacy software and increased attack surface
9	User-based mistakes and cyber awareness (technical, operational, and user literacy)
10	Threat identification and incident response

were being canceled. *Advances in Radiation Oncology* hopes to soon publish a detailed account of how this incident affected radiation therapy services in Ireland as part of the new cybersecurity series.[18]

On May 18, 2021, a cyberattack at New Zealand's major medical center resulted in a disruption of cancer patient care and its radiation oncology clinics for 3 weeks, and even longer for other specialties. This event caused >350 radiation treatment sessions to be cancelled, delayed, or relocated, forcing physicians to coordinate with other facilities and providers to continue patient treatments. According to one source, this was potentially one of the largest cyberattacks in the country to date.[4] Many radiation oncology clinics have been affected similarly, although the total number has not been quantified. A list of health care institutions suffering a breach involving >500 patients due to a cyberattack and other causes, such as simple physical theft of laptop computers, can be found on the U.S. Department of Health and Human Services, Office for Civil Rights breach portal.

Most of these attacks prohibited providers from accessing the medical records system, causing delayed treatment for thousands of patients. These attacks pose a difficult situation for any health care provider and institution, but even more so for those involved in radiation oncology. Radiation therapy is essential in the treatment of many cancers, and must be completed in a timely fashion to ensure tumor control. For head and neck, cervical, vulvar, and anal cancers, as well as medulloblastoma, delays in therapy are particularly linked to inferior tumor control.[19,20] As these ransomware attacks become more prevalent, having robust cybersecurity and an emergency backup system is essential for these institutions to prevent lapses in radiation therapy service that may result in less effective treatment.

Discussion

Ransom attacks are particularly detrimental to the delivery of quality radiation therapy because the effectiveness of fractionated therapy is dependent on patients not incurring unnecessary breaks in treatment. In the case of a ransomware attack, this can affect the effectiveness

Table 3 Recommendations for Critical Controls

1	Require multifactor authentication for all identities and alert on unusual behavior
2	Update software, including operating systems, applications, and firmware on IT network assets, in a timely manner
3	Implement endpoint detection and response tools and systems that can block and alert on malicious activity
4	Enable strong e-mail protection filters to prevent phishing e-mails from reaching end users; filter e-mails containing executable files and macros from reaching end users
5	Maintain offline, encrypted backups of data, and regularly test backups
6	Implement a user awareness training program, and simulate attacks for phishing, ransomware, and other attack types
7	Review network segmentation and limit administrative access based on least privilege principles
8	Set antivirus/antimalware programs to conduct regular scans of IT network assets using up-to-date signatures
9	Filter network traffic to prohibit ingress and egress communications with known malicious Internet protocol addresses
10	Conduct regular cyber risk assessments on both external and internal assets
11	Review timely advisories sent by local and national cyber security and information sharing and analysis centers
12	Review third-party services risks, specifically those related to remote access and IT management
13	Practice business continuity and incident response plans
14	Increase vigilance in monitoring, detecting, and responding to suspicious activity
15	Implement centralized logging and managed security operation services
16	Ongoing staff education regarding cybersecurity threats, adapted to the nature of the most current threats

Abbreviations: IT = information technology.

of treatment for hundreds or thousands of patients at the same time, with cascading effects on other specialties and health care workers. Because of this temporal effect, radiation therapy clinics should prioritize the protection of data for patients currently under treatment in the case of a ransom attack. Clinics should develop plans that allow for continuity of care in the case of a prolonged computer systems outage. Some practical considerations include being able to know each patient's current and prescribed dose independent of the oncology information system (often an issue in today's paperless environment) and having a method to resume treatments for these patients as quickly as possible. Prioritized data backup and restoration for current treatment patients is necessary to accomplish this goal. The University of Maryland has outlined one method for this scenario.[15]

The diversity of threats and attacks demand improved collaboration between oncologic treatment centers nationwide and internationally. Facilities and practices need improved preparedness (Table 3 shows a nonexhaustive list of recommendations), incident response capabilities, communication, and threat intelligence sharing.[21] A system should be put in place to promote more meaningful action beyond mandatory annual compliance check-box exercises. Lastly, institutions need to allocate appropriate funding to adequately respond to these attacks and increase resilience against increasing cybersecurity threats. By making these changes, providers will be more prepared to face attacks resulting in improved patient outcomes.

Conclusions

Socially engineered ransomware attacks are the primary threat to medical organizations at this time. In particular, these attacks target unsuspecting individuals within health care entities rather than directly attacking a system's technical defenses. Routine reeducation of staff on best security practices while working in an electronic environment can reduce the risk of a successful ransomware attack.

References

1. Finances Online. 119 impressive cybersecurity statistics: 2020/2021 data & market analysis. Available at: https://financesonline.com/cybersecurity-statistics/. Accessed June 4, 2021.
2. U.S. Cybersecurity and Infrastructure Security Agency. Alert (AA20-302A): Ransomware activity targeting the healthcare and public health sector. Available at: https://us-cert.cisa.gov/ncas/alerts/aa20-302a. Accessed February 1, 2021.
3. Viswanatha A, Volz D. FBI director compares ransomware challenge to 9/11. Available at: https://www.wsj.com/articles/fbi-director-compares-ransomware-challenge-to-9-11-11622799003?mod=e2twp. Accessed June 4, 2021.
4. Ensor J. 'Catastrophic failure': Cyber attack on Waikato DHB 'worse than COVID', significant impact on radiation patients - expert. Available at: https://www.msn.com/en-nz/news/national/catastrophic-failure-cyber-attack-on-waikato-dhb-worse-than-covid-significant-impact-on-radiation-patients-expert/ar-AAKsC9j?ocid=entnewsntp. Accessed June 4, 2021.
5. Filkins B. Health care cyberthreat report: Widespread compromises detected, compliance nightmare on horizon paper. Available at: http://www.sans.org/reading-room/whitepapers/firewalls/paper/34735. Accessed June 24, 2021.
6. Roman F. Private communication, Medical Information Technology Advisors Threat Intelligence Platform. Available at: http://www.meditadvisors.com. Accessed June 4, 2021.
7. FireEye Inc. The UNC2529 triple double: A trifecta phishing campaign. Available at: https://www.mandiant.com/resources/unc2529-triple-double-trifecta-phishing-campaign. Accessed June 14, 2021.
8. Tanner J. Finland shocked by therapy center hacking, client blackmail. Available at: https://abcnews.go.com/Health/wireStory/finland-shocked-therapy-center-hacking-client-blackmail-73817011. Accessed June 4, 2021.
9. U.S. Department of Health and Human Services. Ransomware trends 2021 report. Available at: https://www.hhs.gov/sites/default/files/ransomware-trends-2021.pdf. Accessed June 14, 2021.
10. U.S. Department of Health and Human Services, Office for Civil Rights. Cases currently under investigation. Available at: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf. Accessed June 24, 2021.
11. Verizon. 2021 data breach investigation report. Available at: https://www.verizon.com/business/en-fi/resources/reports/dbir/2021/masters-guide/introduction/. Accessed June 14, 2021.
12. Crowdstrike. 2021 global threat report. Available at: www.crowdstrike.com/resources/reports. Accessed June 24, 2021.
13. Muthuppalaniappan M, Stevenson K. Healthcare cyber-attacks and the COVID-19 pandemic: An urgent threat to global health. *Int J Qual Health Care*. 2021;33:mzaa117.
14. Public Health Emergency. Health industry cybersecurity practices. Available at: https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf. Accessed June 4, 2021.
15. Nichols EM, Rahman SU, Yi B. The impact of cybersecurity in radiation oncology: Logistics and challenges. *Appl Rad Oncol*. 2018;7:14–18.
16. 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.
17. HIPAA Journal. Radiation treatments disrupted after cyberattack on software vendor. Available at: https://www.hipaajournal.com/healthcare-providers-postpone-radiation-treatments-cyberattack-elekta/. Accessed June 25, 2021.
18. 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 August 12, 2021.
19. Paulino AC, Wen BC, Mayr NA, et al. Protracted radiotherapy treatment duration in medulloblastoma. *Am J Clin Oncol*. 2003;26:55–59.
20. Petereit DG, Sarkaria JN, Chappell R, et al. The adverse effect of treatment prolongation in cervical carcinoma. *Int J Radiat Oncol Biol Phys*. 1995;32:1301–1307.
21. U.S. Cybersecurity and Infrastructure Security Agency. Ransomware guide and similar guidance. Available at: https://www.cisa.gov/publication/ransomware-guide. Accessed February 1, 2021.