


Selected Proceedings From the 11th International Congress of Arthroplasty Registries
Guest Editor: Ola Rolfson MD, PhD

The Irish National Orthopaedic Register Under Cyberattack: What Happened, and What Were the Consequences?

Shane P. Russell MB BCh BAO, MCh, MRCSI^{1,2} , Eoin Fahey MB BCh BAO, MCh, MRCSI¹, Mark Curtin MB BCh BAO, MCh, FRCS¹, Suzanne Rowley BSc, Grad Dip, MSc², Paddy Kenny MB BCh BAO, MFSEM, FRCSI, FRCS (Tr & Orth)^{1,2}, James Cashman MB BCh BAO, FRCS (Tr & Orth)^{1,2}

Received: 30 October 2022 / Accepted: 7 March 2023 / Published online: 10 April 2023
Copyright © 2023 by the Association of Bone and Joint Surgeons

Abstract

Background On May 14, 2021, a criminal cyberattack was launched against the Irish public healthcare system, the Health Service Executive, resulting in a complete shutdown of all national healthcare computer systems, including the Irish National Orthopaedic Register (INOR). Cyberattacks of this kind occur sporadically, and postevent analyses can inform future preparedness efforts, but few such analyses have been published.

Question/purpose What was the impact of the cyberattack in terms of (1) registry downtime, (2) harms to patients, and (3) costs to the INOR for data contingency and reconciliation?

Methods All nine hospitals using the INOR were included for data collection. Since establishment in 2014, the INOR has been rolled out to all eight public elective hospitals,

capturing all hip and knee arthroplasty procedures. One private hospital was also captured, with plans to expand the private sector coverage. Individual institutional records and central INOR records were queried with respect to downtime, potential harms to patients (including intraoperative complications because of a lack of data on existing implanted components and complications directly attributed to delayed or canceled procedures), and costs related to additional person-hours addressing data reconciliation. Objective data directly related to the uncontrolled INOR downtime were collected, including duration of downtime, contingency methods employed, quality of contingency data collected, adverse patient events, methods of data salvage and reconciliation, and the cost of data contingency and reconciliation measures. Costs were estimated by the additional person-hours of work completed, multiplied by the hourly rate of that employee. Employees at each of the nine hospitals were asked to provide their additional person-hours of work performed because of the attack. These hours were corroborated by observing the time taken at each unit to reconcile data for single cases multiplied by the number of cases at that unit. Employees included nurses, clinical nurse specialists, and doctors of various grades. Person-hour rates were calculated using the Health Service Executive's published salary scales. **Results** The INOR suffered a median downtime of 134 days (range 119 to 272 days) across nine sites. No serious adverse patient events were identified. The immediate implementation of a paperwork fallback method for the INOR successfully resulted in 100% case capture during the downtime. However, 2850 additional person-hours were required for data reconciliation at an estimated


Each author certifies that there are no funding or commercial associations (consultancies, stock ownership, equity interest, patent/licensing arrangements, etc.) that might pose a conflict of interest in connection with the submitted article related to the author or any immediate family members.

All ICMJE Conflict of Interest Forms for authors and *Clinical Orthopaedics and Related Research*® editors and board members are on file with the publication and can be viewed on request.

Ethical approval was not sought for the present study. This work was performed at the National Office of Clinical Audit, Dublin, Ireland.

¹Royal College of Surgeons in Ireland, Dublin, Ireland

²National Office of Clinical Audit, Dublin, Ireland

S. P. Russell , National Office of Clinical Audit, 2nd Floor, Block B, Ardilaun, 111 St Stephens Green, Dublin 2, D02 VN51, Ireland, Email: shanep Russell@rcsi.ie

cost of USD 181,000 to USD 216,000. More subjectively, as reported by interviews with INOR leads at each hospital, the cyberattack negatively impacted operating room efficiency with delays between procedures because of additional paperwork data collection, disrupted patient flow for paperwork data collection on the ward level and in the outpatient clinics, and disrupted resource allocations and staff capabilities because of additional paperwork requirements during the contingency period.

Conclusion Disruptions to data collection and data accessibility after this cyberattack were successfully countered by a contingency plan; however, substantial financial costs and additional resources were required for data conservation and reconciliation.

Clinical Relevance In addition to robust preventative security measures, national registers and other healthcare systems should have secondary data backup facilities and reliable fallback procedures prepared for such events.

Introduction

On May 14, 2021, the Irish public awoke to the global news that the Irish public healthcare system, the Health Service Executive (HSE), was the target of an ongoing, large-scale cyberattack through the criminal infiltration of its information technology (IT) systems with “Conti” ransomware (an advanced ransomware tool observed to be used by criminals since 2020 that uses a unique encryption routine to encrypt users files, blocking access to data until a decryption key is provided). This resulted in a complete shutdown of virtually all national public healthcare IT systems, including the Irish National Orthopaedic Register (INOR) [12, 15]. In response to the attack on the state, a Critical Incident Process was invoked. Consequently, 70,000 devices across 4000 locations were disconnected from the National Healthcare Network to control the spread of the ransomware virus through the thousands of IT systems integrating across the HSE network, including electronic patient medical records, telephone and email systems, payroll, laboratory and radiology systems, and national databases such as the INOR.

Cyberattacks on healthcare systems saw a sharp increase during the Coronavirus-19 pandemic [3]. A similar attack by the Conti ransomware group occurred in the United States on the Colonial Pipeline in May 2021 and on the United Kingdom’s National Healthcare Service in the same year [14]. The National Healthcare Service had also previously suffered massive disruptions to service after a similar style of attack with the 2017 WannaCry ransomware virus [11].

With the cessation of virtually all HSE IT systems overnight, widespread organizational chaos and disruptions to patient care resulted in serious and prolonged clinical consequences, such as disrupted patient flow and canceled or postponed procedures and appointments. The return of systems was a slow and costly



Fig. 1 This map shows the nine Irish hospitals enrolled in the INOR: Red indicates public hospitals (n = 8) and purple indicates the private hospital evaluated in this study (n = 1). A color image accompanies the online version of this article.

process, with various locations and systems returning on a phased basis over the following year. On the day of this attack, the Irish government confirmed that it would not pay a ransom of USD 20,000,000 in bitcoin to the attacker, whose aims were to “disrupt health services, steal data, and demand a ransom for the non-publication of stolen data” [12, 15].

Cyberattacks on large healthcare systems and registries are well documented [3, 5, 8, 11]. Despite similar attacks on healthcare systems abroad, the HSE was largely unprepared and lacked the structures to deal with this incident [12]. In contrast, however, we observed that one system in the HSE’s National Healthcare Network, the INOR, maintained overall function using contingency methods and avoided adverse patient events. To help inform future preparedness efforts, this study examined the effects of this cyberattack on the INOR and its function during this time.

We therefore performed a postevent analysis in which we asked: What was the impact of the cyberattack in terms of (1) registry downtime, (2) harms to patients, and (3) costs to the INOR for data contingency and reconciliation?

Patients and Methods

Study Design and Setting

We performed a retrospective analysis of the events that followed the cyberattack at each INOR-enrolled hospital.

National Office of Clinical Audit and INOR

The National Office of Clinical Audit established the INOR in 2014; the primary objective was to monitor the

quality and safety of arthroplasty in Ireland. The INOR is currently live in all eight public elective arthroplasty hospitals and one private hospital (Fig. 1). There are plans to extend the rollout to all public and private hospitals in Ireland [9]. It is not known what proportion of arthroplasty procedures nationally are captured by the INOR because private hospital data are not available. The register captures all patients undergoing elective hip and knee arthroplasty, both primary and revision procedures [9]. No INOR data are stored at local institutions, and healthcare workers use a secure online portal to access a central database for data input to the electronic register. The INOR is an exclusively electronic database using both manual (typed) electronic data entry and automated (barcode) data entry, reporting excellent data accuracy and completeness [13].

A national service-level agreement exists between the Quality Improvement Team of Ireland's publicly funded healthcare system, the HSE, and the Royal College of Surgeons in Ireland. Under this agreement, the Royal College of Surgeons in Ireland provides the clinical, administrative, and technical resources necessary for INOR implementation and maintenance [9]. However, the primary IT servers and associated INOR patient database are located in the HSE IT infrastructure. Secondary data backup is maintained by a private third party. Before the cyberattack, standard IT security procedures were used according to local hospital and HSE policies. Patient data collection and processing were General Data Protection Regulation-compliant [7, 10]. Contingency methods in the event of unplanned downtime included reversion to printed paper forms capturing identical data to the electronic form. These paper forms were used for all stages of data capture: preoperative assessments, operative notes, component logs, and postoperative assessments at various patient pathway timepoints. Contingency forms were prospectively maintained and stored locally for later reconciliation with the central electronic database. Arthroplasty clinical nurse specialists in each unit were trained in contingency methods in the event of unplanned downtime for any cause.

Interviews and Records

At each of the nine hospitals using the INOR, we interviewed arthroplasty clinical nurse specialists and examined local institutional data. We also examined central INOR records. Local institutional data consisted of an electronic datasheet held by each arthroplasty clinical nurse specialist, which included data such as a record of adverse patient events, records of missing forms for patients, if any, and the volume of paper forms that required electronic reconciliation once the INOR was restored (for each stage of the

patient's journey, the INOR uses a separate form for data input: two preoperative, two intraoperative, and two for each postoperative visit).

Endpoints of Interest

We included the following for data collection:

Objective Data

Objective data included the duration of INOR downtime, methods of data collection during the contingency period, quantification of inaccurate or incomplete data, adverse patient events caused by the attack, methods of data reconciliation or salvage, and the overall financial cost of contingency procedures and data reconciliation. Two observers (SPR and EF) examined data provided by the arthroplasty clinical nurse specialist from the locally held, prospectively maintained datasheet. We cross-referenced each hospital's operating room records and outpatient attendance records to identify potential missing episodes. In this way, completeness of procedures was measurable; however, completeness or accuracy of data within procedures was not measurable because no control forms existed for comparison. Costs were estimated by the additional person-hours of work completed, multiplied by the hourly rate of that employee. Employees at each of the nine hospitals were asked to provide their additional person-hours of work performed because of the attack. These hours were corroborated by observing the time taken at each unit to reconcile data for single procedures, multiplied by the number of procedures at that unit. Employees included arthroplasty clinical nurse specialist and senior house officer doctors of various paygrades. Person-hour rates were calculated using the HSE's published salary scales.

Subjective Data

Second, we collated nonquantifiable reports of opportunity costs, resource costs, staff workload, impaired patient flow, and patient dissatisfaction for review. During the interview, each arthroplasty clinical nurse specialist was asked to comment on these qualitative areas. Comments that were consistent among interviewees, of interest to surgeons and other healthcare professionals, and relevant to describing the effects of a cyberattack were included and collated for subjective reporting only.

Results were assigned to one of four phases of disaster response: preparation, response, recovery, and mitigation [6]. Staffing costs were estimated using the HSE's published salaries [4]. Additional person-hours spent

reconciling hardcopy data to electronic data were multiplied by that person's hourly rate before overall summation.

Primary and Secondary Study Outcomes

Our primary study goals were to quantify the duration of INOR downtime at each site and describe the efficacy of the contingency methods used during that period. To achieve this, we collected data from local hospital records as described.

Our secondary study goals were to identify any harms to patients caused by the INOR downtime, attempt to quantify the cost of data maintenance and data reconciliation because of the downtime, and report on any other adverse effects of the INOR downtime as reported by local staff. To achieve this, we collected data from local hospital records and interviewed each of the INOR local hospital leads.

Statistical Analysis

We used Microsoft Excel (Microsoft Corp) for database management and descriptive statistical analysis.

Results

Registry Downtime

The median downtime for the registry after the cyberattack was 134 days (range 119 to 272 days). The one private hospital was a statistical outlier at 272 days of downtime because of additional IT security requirements by that hospital. No hospital had access to the INOR database for upload during the downtime. Limited data download capabilities became available to units on a sporadic and interrupted basis approximately 8 weeks after the attack as IT personnel worked to restore systems.

Data capture using the hardcopy contingency methods resulted in 100% capture of all patients visiting the hospital for surgery, outpatient assessments, or virtual appointments compared with local institutional electronic or hardcopy records (the procedure capture rate during normal operation has been reported by one INOR hospital to be 100% [13]).

Harms to Patients

No adverse patient events because of INOR downtime were recorded at any site. Because there were duplicate hardcopy operating room logbooks or hardcopy medical

charts, historical component data were available for all revision surgeries needing component explanation.

Costs of Data Contingency and Reconciliation

Approximately 2850 additional overtime hours were required of hospital staff, and in some units, data reconciliation was achieved by the employment of additional nurses, medical staff, and retired staff during weekend hours at a total estimated healthcare worker overtime cost of USD 181,000 to USD 216,000 (Supplemental Table 1; <http://links.lww.com/CORR/B80>).

Discussion

In May 2021, the Irish public healthcare system was subjected to a devastating cyberattack, resulting in the immediate and sustained unplanned downtime of all HSE IT systems, including the INOR's electronic database. Although cyberattacks on other healthcare systems have been reported, no in-depth analysis we are aware of has described how systems such as large registries were affected by an attack of such scale. To help inform future preparedness of other healthcare systems, this study examined the effects of that event on the INOR by describing the duration of downtime and the data contingency and reconciliation methods used during that time, describing whether patients were harmed by the attack and providing a cost analysis for data reconciliation.

We found there was a prolonged period of registry downtime during which a contingency plan provided excellent data capture, that no patients were directly harmed because of the INOR downtime, and that data reconciliation was a painstaking and costly process. Surgeons and those working in healthcare registries will be keen to implement robust preventative security measures, ensure data are appropriately backed up, and ensure effective contingency plans are in place in the event of future attacks.

Limitations

Although we initially aimed for objective data reporting, this study encountered a number of limitations. Although the immediate fallback to contingency methods resulted in the uninterrupted capture of data at equivalent points in the patient pathway, the accuracy of the data in these episodes remains under investigation. An audit is underway of component log accuracy and completeness using hardcopy operating room logbooks as a standard; however, no such standard exists for patient-reported outcome measures. It

will not be possible to retrospectively compare these entries against a control.

In addition, we were unable to precisely quantify the increased employer costs as a direct result of the attackers' actions because of innumerable immeasurable variables for example, the increased work rate during routine working hours and the exact salary of employees on a chronologically incremental pay scale. However, we believe a reasonable conservative estimate was made for overtime expenses after interviewing each unit and using published pay scales for calculation.

This study found that data reconciliation was a costly process in terms of overtime billing to the employer. However, the overall price of the attack on the INOR is immeasurable because areas such as opportunity costs and increased workloads are virtually impossible to calculate. In addition, unbundling the technical restoration costs of the INOR from the HSE overall was not possible.

This cyberattack occurred during the global Coronavirus-19 pandemic. Staff shortages, resource reallocations, patient satisfaction, and reduced planned elective procedures, among other changes because of the disruption by the pandemic, may all have influenced our findings. Further studies would be needed to compare, for example, volumes of operations being performed, staff workloads, and operating room efficiency during the pandemic compared with during both the pandemic and the cyberattack.

Discussion of Key Findings

The cyberattack on the INOR was disruptive and expensive but not disabling to the INOR's function, and no patients were harmed. Preparedness for cyberattacks by large healthcare databases such as orthopaedic registers is essential. We found that a contingency plan was immediately implemented and no patient data were left uncaptured. However, the duration of downtime resulted in a mass of paper forms that required manual upload to the electronic database once the system was restored. We emphasize that meticulous data capture and maintenance of records is of utmost importance because datapoints left uncaptured may not be acquirable at later dates.

Although we found that no patient harms were recorded during the downtime, patients were certainly disadvantaged by canceled procedures and appointments. However, quantifying the patient experience during the attack was not a primary endpoint of this study, and we recognize that future studies are needed to report on this.

This study identified a costly overtime bill for data reconciliation. In the event of future attacks requiring mass data reconciliation, we suggest exploring the option of recruiting clerical or third-party labor for the task, which may reduce costs and allow healthcare workers to return to

normal duties sooner. The final financial cost of the attack on the HSE overall will be largely immeasurable because of innumerable, incalculable variables; however, conservative estimates of at least USD 119,000,000 have been made [1]. Although the attackers provided a decryption key 6 days after the attack, it is unknown how this impacted recovery of the INOR database or influenced costs. Additionally, there is no way to know whether paying the USD 20,000,000 ransom would have resulted in reduced overall costs to the HSE [2].

An independent postincident report commissioned by the HSE concluded that (referring to the HSE overall) there was "a lack of structures and processes in place to deal with this incident" [13]. In contrast to this finding of the HSE, this current study highlights the resilience of one subsystem within the HSE against such an attack: the INOR. Although major disruptions to the delivery of patient care were endured at a high financial and resource cost and the effects of the attack are being felt today, the immediate introduction of containment and contingency measures resulted in no breach of INOR patient data, no loss of existing patient data, and no serious adverse patient events during an extended period of electronic downtime.

Healthcare systems are attractive targets for cyber criminals. They are well documented to have underfunded cyber security defenses compared with other industries. They are underwritten by states and therefore capable of paying large ransoms. They are technology-saturated industries. Finally, disruption of healthcare systems causes widespread political and emotional chaos because of cessation of healthcare delivery and, moreover, fear of sensitive personal data publication [5, 8, 15]. The described Conti ransomware attack on the HSE was technically extremely similar to recent attacks on its neighboring healthcare system, the United Kingdom's National Healthcare Service. Although the 2017 WannaCry attack and 2021 Conti attack on the National Healthcare Service resulted in substantial disruptions to services, the devastation caused by the described May 2021 attack on the HSE was more widespread across systems and was of a far longer duration.

Conclusion

This study described the effects of a large-scale criminal cyberattack on a national orthopaedic register. Our results described the duration of unplanned downtime and demonstrated how the immediate implementation of a contingency plan resulted in no uncaptured cases by the register and how no patients were harmed as a direct result of register disruptions. Finally, we provided a cost analysis for data reconciliation after system restoration. Those working with registers should ensure appropriate

preventative security measures are in place to prevent such attacks by following professional cybersecurity advice, use secure data backup facilities, and have an effective contingency plan prepared. Further studies are required to examine the quality of data collected during the contingency phase and to examine patient experiences and quality of care provided during and after such attacks.

Acknowledgments We thank all staff at the National Office of Clinical Audit and the associated arthroplasty clinical nurse specialists for their diligent work.

References

1. Cullen P. Cyberattack: HSE faces final bill of at least € 100m. *The Irish Times*. Available at: <https://www.irishtimes.com/news/health/cyberattack-hse-faces-final-bill-of-at-least-100m-1.4577076>. Accessed February 3, 2023.
2. Devane JWM. Decryption key received from HSE hackers but reason why unknown, says Taoiseach. Available at: <https://www.breakingnews.ie/ireland/government-did-not-pay-ransom-for-decryption-key-after-hse-hack-says-martin-1130980.html>. Accessed February 3, 2023.
3. He Y, Aliyu A, Evans M, Luo C. Health care cybersecurity challenges and solutions under the climate of COVID-19: scoping review. *J Med Internet Res*. 2021;23:e21747.
4. Health Service Executive. Consolidated salary scales in accordance with the FEMPI acts, the public service agreements and the Public Service Pay and Pensions Act 2017. Available at: https://healthservice.hse.ie/documents/2331/Pay_scales_for_2.2.22_and_1.10.22_adjustments_V2.pdf. Accessed February 3, 2023.
5. Jalali MS, Kaiser JP. Cybersecurity in hospitals: a systematic, organizational perspective. *J Med Internet Res*. 2018;20:e10059.
6. Klein TA, Irizarry L. EMS disaster response. In: *StatPearls*. StatPearls Publishing LLC; 2022.
7. McLaughlin S. Ireland: a brief overview of the implementation of the GDPR. *Eur Data Prot L Rev*. 2018;4:227.
8. Millard WB. Where bits and bytes meet flesh and blood: hospital responses to malware attacks. *Ann Emerg Med*. 2017;70:A17-A21.
9. National Office of Clinical Audit. Statement of purpose: Irish National Orthopaedic Register. Available at: http://s3-eu-west-1.amazonaws.com/noca-uploads/general/ST-5_Statement_of_Purpose_INOR_V_2_July_2020.pdf. Accessed October 27, 2021.
10. National Office of Clinical Audit. GDPR. Your data matters to us. Available at: <https://www.noca.ie/about-noca/gdpr>. Accessed October 25, 2022.
11. Oxford Analytica. UK NHS attack underlines ransomware risk. Emerald Expert Briefings. Available at: <https://doi.org/10.1108/OXAN-ES272139>. Accessed February 3, 2023.
12. PriceWaterhouseCooper. Conti cyber attack on the HSE independent post incident review, 2022. Available at: <https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf>. Accessed February 3, 2023.
13. Russell SP, Broderick JM, O'Dea SD, Fahey E, Kenny P, Cashman J. Can bar code scanning improve data capture in a national register? Findings from the Irish National Orthopaedic Register. *Clin Orthop Relat Res*. 2022;480:1971-1976.
14. Shear MD, Perloth N, Krauss C. Colonial pipeline paid roughly USD 5 million in ransom to hackers. *The New York Times*. Available at: <https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline-ransomware.html>. Accessed: February 3, 2023.
15. Stritch MM, Winterburn M, Houghton F. The Conti ransomware attack on healthcare in Ireland: exploring the impacts of a cybersecurity breach from a nursing perspective. *Canadian Journal of Nursing Informatics*. 2021;16. DOI: <https://cjni.net/journal/?p=9383>.