Cyberattack on the National Health Laboratory Service of South Africa – implications, response and recommendations

S Cassim, MMed (Haem Path), FCPath (SA) Haem; **Z C Chapanduka**, FCPath (SA) Haem, MBA

Division of Haematology, Department of Pathology, Faculty of Medicine and Health Sciences, Stellenbosch University and National Health Laboratory Service, Tygerberg Hospital, Cape Town, South Africa

Corresponding author: *S Cassim (sumaiya@sun.ac.za)*

Cybersecurity is now an integral consideration in the management of healthcare institutions in this modern technological era. Cyberattacks primarily targeting healthcare institutions have increased exponentially. Recently, the information technology systems of the National Health Laboratory Service (NHLS) of South Africa (SA) were targeted by cyberterrorists using disruptive ransomware. As a result, all files on the affected computers and servers became inaccessible, thus affecting all NHLS operations. We share our experience of this cyberattack from the department of haematological pathology at Tygerberg Hospital, Cape Town, SA. We outline the negative impact on the NHLS and the immediate response, and make future recommendations, including a draft of a business continuity plan.

Keywords: cybersecurity, cyberattack, ransomware

S Afr Med J 2024;114(12):e2549. https://doi.org/10.7196/SAMJ.2024.v114i12.2549

Cybersecurity is now an integral consideration in the management of healthcare institutions in this modern technological era. This is due to the fact that healthcare institutions are increasingly becoming the primary targets of cyberattacks. They house sensitive personal data, have an urgent need for continuity of care and often have poor information technology (IT) security systems in place.[1,2]

The National Health Laboratory Service (NHLS) of South Africa (SA) is a public entity that comprises a network of modern diagnostic laboratories spanning across all nine provinces of SA. It has >8 000 employees and is the sole provider of diagnostic pathology services to >80% of the SA population. These services are rendered to the entire public sector, from academic and district hospitals to primary healthcare facilities, with the specialisation of services increasing from peripheral to central laboratories. The NHLS is also the custodian of patients' personal data and test results. These data are useful for patient care and disease surveillance, in addition to their value in healthcare research.[3]

The authors share experience of the recent cyberattack on the NHLS from the haematopathology department at Tygerberg Hospital, Cape Town, SA.

The attack

On Saturday 22 June 2024, at approximately 03h00, the NHLS' IT system was targeted by cyberterrorists using disruptive ransomware named BlackSuit.[4] Ransomware is a type of malware, i.e. malicious software, that utilises encryption technology, which prevents access to data until payment of a ransom is made.[5] Some applications on NHLS computers and servers were encrypted, resulting in a complete breakdown of all IT-related operations, including internet, intranet and TrakCare laboratory information system (LIS) (InterSystems, UK). The LIS functions, including test order entry, test result upload via laboratory analysers, test result entry and viewing of results, all became inaccessible following this disruptive attack. The NHLS Central Data Warehouse (CDW), the facility responsible for storing all historical pathology testing data for laboratory users, was also inaccessible. Decades of archived laboratory test results became inaccessible.

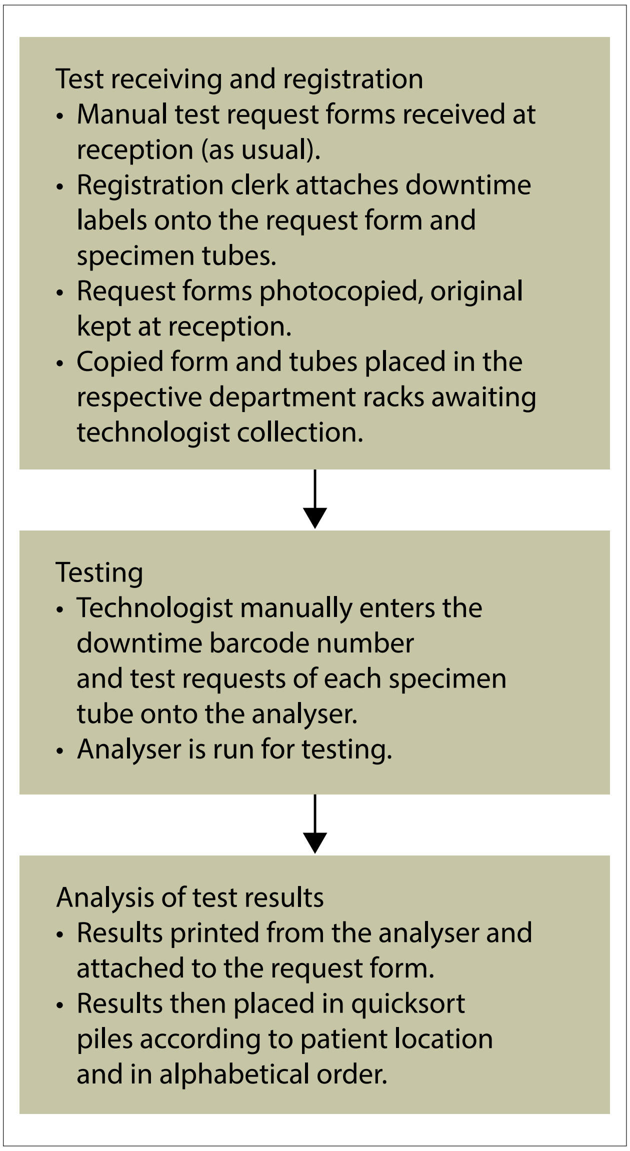
The impact

This disruptive cyberattack resulted in widespread negative implications on all operational aspects and stakeholders of the NHLS.

Service delivery: Following the cyberattack, service delivery needed to pivot from automated to manual procedures. The NHLS' downtime standard operating procedure (SOP) was instituted (Fig. 1). However, the SOP had no contingency plan for a cybersecurity breach, and was clearly not fit for purpose. Prolonged, complete shutdown of all network services ensued.

NHLS staff: All NHLS staff, including management, pathologists, registrars, technologists, scientists and support staff were unprepared for such an attack. As this cyberattack affected all aspects of the NHLS operations, a ready-to-apply business continuity plan was required, and unfortunately, such a plan was not available. Staff were left to their own devices because senior NHLS leadership had no ready solution. Adequate and timely additional support was not provided, which led to increased workloads and inevitable pressure. Staff levels of anxiety were exacerbated by uncertainty regarding income and job security. Furthermore, there was no informed indication as to when the situation would be resolved.

Clinicians and patients: Requesting clinicians from all centres expressed their frustration regarding the inability to request specific tests, inaccessible previous results, delay in current results and the inconvenience of manually collecting paper results. Turnaround times (TAT) for all analytes were immediately prolonged, and in most cases doubled. For instance, the TAT for full blood counts in hospital, which should be <2 hours, increased to 4 hours after the cyberattack. This directly affected the clinicians' ability to appropriately diagnose, manage and monitor their patients. Patient turnover in emergency centres and admission wards was reduced, with longer patient waiting times prior to admission or discharge.



Test receiving and registration

- Manual test request forms received at reception (as usual).
- Registration clerk attaches downtime labels onto the request form and specimen tubes.
- Request forms photocopied, original kept at reception.
- Copied form and tubes placed in the respective department racks awaiting technologist collection.

Testing

- Technologist manually enters the downtime barcode number and test requests of each specimen tube onto the analyser.
- Analyser is run for testing.

Analysis of test results

- Results printed from the analyser and attached to the request form.
- Results then placed in quicksort piles according to patient location and in alphabetical order.

Fig. 1. Immediate response plan in accordance with the downtime standard operating procedure.

This posed an undue burden and stress on clinicians who, in addition, had to counsel patients and their families regarding the situation. Such a crippling effect on the NHLS undoubtedly led to some level of increase in patient morbidity and mortality. Future studies should be able to confirm this.

Public opinion: Numerous SA news and government agencies reported on the devastating cyberattack on the NHLS. Follow-up articles were also posted weeks later headlining the faltering NHLS system, which is still not fully operational.[6-10] Despite continued reassurances from the NHLS, we hypothesise that trust in the SA healthcare system may be compromised.

Ethics: Test results were distributed by unconventional means, including Gmail-type email services, social media and electronic platforms, which may be in violation of the Protection of Personal Information Act 4 of 2013.[11] Delayed access to critical results and decreased access to all tests may also lead to medicolegal implications from aggrieved patients and their families.

Teaching: Teaching of registrars, i.e. Master of Medicine (MMed) postgraduate students, was significantly reduced due to the need for 'all hands on deck', with diversion of work time to assist laboratory staff. The lack of access to work computers, alternative devices, WiFi and data also negatively impacted on learning. All NHLS online teaching platforms utilising video conferencing tools such as Zoom (Zoom, USA) and Teams (Microsoft, USA) were unavailable. This included the NHLS Project ECHO weekly lectures, which are attended remotely by all academic centres, regional laboratories and attendees from outside SA.

Research: The ability to conduct research projects was considerably compromised owing to the loss of internet connectivity and inability to access patient data both from the LIS and the NHLS CDW. This had a significant impact on both investigator-initiated research projects and MMed students, who require archived NHLS data. It is feared that accumulated data that have not been entered on the NHLS LIS may be permanently lost to future researchers and disease surveillance activities.

Cost: The NHLS suffered financial losses for several reasons. These include loss of income due to reduced testing, inefficient procurement of stock, perishable stock expiry, consumable costs for manual reporting (e.g. labels, paper, toner), IT software and hardware costs (e.g. upgraded Windows (Microsoft, USA), antivirus, laptop computers and WiFi routers, etc.) and additional staff for administration and IT support. The full cost is yet to be determined.

Time: More service delivery time was needed to perform only essential tests using manual protocols, with distribution of results taking the longest time. Academic time was also lost due to the lack of internet, resulting in no email access, online teaching or research activities.

Data integrity: All tests performed during the downtime period will eventually need to be uploaded back onto the LIS. It is assumed that all analyser results will automatically upload onto the LIS when back online. All other written and typed results will be manually captured onto the LIS, which will inevitably lead to some unentered data and human error resulting in potentially serious entry errors. As a result, retrieval of all data created during this period will be compromised.

The response

The downtime SOP was promptly implemented. This SOP is for laboratory tests only, and details the practical steps to be followed in the event of users being unable to access the TrakCare LIS. There were no SOPs for human resources and salaries management (i.e. Oracle), research and travel funding (i.e. research management system), staff health monitoring, billing and debt collection, nor supplies management and inventory control.

In the haematology laboratory, analyser-printed results could only be obtained for automated full blood counts, differential counts and coagulation tests. All other tests that required manual reporting, including manual differential leucocyte counts, peripheral blood smear comments, flow cytometry and bone marrow reports, were written on the analyser print-out or typed on Word (Microsoft, USA) documents and saved on work desktops.

Clinical management of all affected healthcare facilities were informed of the compromised NHLS IT systems telephonically. All testing was then de-escalated to only urgent and critical tests. In order to reduce the amount of work, pathologists created new criteria for pathologist referrals and peripheral blood smear-making, and rules for electronic gate-keeping were changed. The NHLS' expert committees (ECs), discipline-specific committees of heads of academic departments, were central in determining the changes and contingency plans required. ECs compiled and disseminated essential test lists. The test results were disseminated to clinicians via

Table 1. Business continuity plan (BCP) (pre disruption)

Task team

- Assemble a team that will take lead in the event of disruption
- Ensure the BCP is kept updated and communicated to all staff

Resources – hardware

- Upgraded desktop computers and laptops for daily use
- Stored laptops for emergency use
- External hard drives for data storage
- Back-up servers, including the Cloud
- WiFi routers for internet access
- Fax machines for communication and distribution of test results
- Consumables (e.g. paper, toner, downtime labels)

Resources – software

- Valid and updated Windows (Microsoft, USA) operating system
- Valid and updated antivirus software
- Network segmentation
- Firewalls
- Essential test lists, predefined and updated
- Test reporting template with NHLS letterhead, on Word (Microsoft, USA) or Excel (Microsoft, USA), predefined and updated (must include patient details, test results, units of measurement, reference ranges)
- Downtime SOPs for all operational departments

Training

- Methods used by cyberterrorists (e.g. malware, phishing, artificial intelligence)
- Cyberattack simulations

General

- Employee login with personal credentials, not to be shared
- Complex password, changed regularly
- Remote network connection should be multi-factor authenticated
- Log off when work is completed
- Regular back-up of data, scheduled every 24 hours
- Suspicious emails must never be opened
- Personal IT devices should not be used to perform work-related tasks
- Unauthorised software should not be downloaded onto work computers

NHLS = National Health Laboratory Service; SOP = standard operating procedure; IT = information technology.

Table 2. Business continuity plan (post disruption)

Immediate response

- Task team takes lead
- Activate downtime SOPs for all operational departments
- Inform clinical managers of all healthcare centres, and send out essential test lists
- De-escalate testing to only urgent and critical tests

Test registration

- Downtime labels should be used on specimens and request forms
- Copies of all request forms must be stored

Testing and reporting

- Downtime barcode number and test requests should be manually entered onto the analyser
- For automated tests, results should be printed directly from the analyser
- For manual tests, reports should be typed on predefined templates

Test result distribution

- Telephone, WhatsApp messenger (Meta, USA), email via alternative email addresses, fax machine, courier delivery or hand collection of paper results
- Alternative electronic test result viewer (e.g. eLabs, Single Patient Viewer)

Recovery

- Eliminate offending malware from all computers
- Rebuild IT infrastructure to ensure safety and resistance to future attacks
- Restore all data and operational services
- Upload all results obtained during downtime back onto LIS

SOP = standard operating procedure; IT = information technology; LIS = laboratory information system.

telephone, WhatsApp messenger (Meta, USA), courier delivery and laboratory collection of paper results.

Plans had to be devised and revised several times to maintain adequate service delivery. This inevitably led to longer turnaround times in registration, testing and reporting.

The future

The response of the NHLS to this cyberattack was reactive and, not unexpectedly, inadequate. An organisation of the size and public health importance as the NHLS should have a business continuity plan (BCP). A BCP is a framework for a business that provides procedural guidance to prevent, prepare for, respond to, manage and recover from any disruption.[12]

We propose the following requirements in preparation for inevitable future attacks:

(*i*) BCP for both pre-disruption and post-disruption, summarised in Table 1 and Table 2, respectively[2,13]

(*ii*) national and legal policies

(*iii*) insurance.

A BCP folder with all updated procedures should be stored on all computers and as a hard copy in the main laboratory.

Conclusion

The NHLS IT systems were wholly inaccessible for 40 days, and only partially functional at the time of writing this article. The human and material cost of this cyberattack is still to be determined. Future cyberattacks of this nature are likely to occur, hence the urgent need for investment in cybersecurity and the development of a well-structured BCP.

Data availability. N/a.

Declaration. None.

Acknowledgements. None.

Author contributions. SC conceptualised and wrote the manuscript; ZCC reviewed and edited the manuscript.

Funding. None.

Conflicts of interest. None.

1. Lippi G, Ferrar A. Lessons learnt in medical laboratories during a disruptive cyber-attack. J Lab Precis Med 2024;23(84):1-4. https://doi.org/10.21037/jl
2. Lippi G, Akhvlediani S, Cadamuro J, et al. EFLM Task Force Preparation of Labs for Emergencies (TF-PLE) recommendations for reinforcing cyber-security and managing cyber-attacks in medical laboratories. Clin Chem Lab Med 2024;8(3):1-8. https://doi.org/10.1515/cclm-2024-0803
3. National Department of Health, South Africa. National Health Laboratory Service Annual Report 2022 - 2023. https://nationalgovernment.co.za/entity_annual/3326/2023-national-health-laboratory-service-(nhls)-annual-report.pdf (accessed 10 July 2024).
4. SentinelOne. BlackSuit ransomware: In-depth analysis, detection, and mitigation. Mountain View: SentinelOne, 2024. https://www.sentinelone.com/anthology/blacksuit/ (accessed 1 August 2024).
5. O'Brien N, Ghafur S, Sivaramakrishnan A, Durkin M. Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that. Digit Health 2022;8(1):1-3. https://doi.org/10.1177/20552076221104665
6. Bateman C. How the NHLS computer hack will cost lives. Johannesburg, SA: Health-e News, 2024. https://health-e.org.za/2024/07/01/how-the-nhls-computer-hack-will-cost-lives/ (accessed 1 August 2024).
7. South Africa Government News Agency. NHLS apologises for blood result delays. SA News, 2024. https://www.sanews.gov.za/south-africa/nhls-apologises-blood-result-delays (accessed 1 August 2024).
8. McCain N. National health lab estimates systems will only be online by mid-July after cyber attack. News24, 2024. https://www.news24.com/news24/southafrica/news/national-health-lab-estimates-systems-will-only-be-online-by-mid-july-after-cyber-attack-20240704 (accessed 1 August 2024).
9. Francke RL. NHLS ransomware attack endangered safety and wellbeing of millions of public health patients. IOL News, 2024. https://www.iol.co.za/news/crime-and-courts/nhls-ransomware-attack-endangered-safety-and-wellbeing-of-millions-of-public-health-patients-b77b355d-6904-4d70-a13d-e27033e3742b (accessed 1 August 2024).
10. Kahn T. NHLS still not fully operational after cyberattack. BusinessDay, 2024. https://www.businesslive.co.za/bd/national/health/2024-07-16-nhls-still-not-fully-operational-after-cyberattack/ (accessed 1 August 2024).
11. South Africa. Protection of Personal Information Act No. 4 of 2013. Government Gazette No. 37067:912. 2013. https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf (accessed 7 July 2024).
12. Fani SV, Subriadi AP. Business continuity plan: Examining of multi-usable framework. Procedia Comput Sci 2019;161(1):275-282. https://doi.org/10.1016/j.procs.2019.11.124
13. Patel AU, Williams CL, Hart SN, et al. Cybersecurity and information assurance for the clinical laboratory. J Appl Lab Med 2023;8(1):145-161. https://doi.org/10.1093/jalm/jfac119

Received 19 August 2024; accepted 4 September 2024.