Lessons learnt in medical laboratories during a disruptive cyber-attack

Giuseppe Lippi, Anna Ferrari

Section of Clinical Biochemistry, University of Verona, Verona, Italy

Correspondence to: Prof. Giuseppe Lippi, MD. Section of Clinical Biochemistry, University of Verona, Piazzale L.A. Scuro, 10, 37134 Verona, Italy. Email: giuseppe.lippi@univr.it.

Keywords: Laboratory medicine; hacker; cyber-attacks

Received: 11 November 2023; Accepted: 12 January 2024; Published online: 20 March 2024.

doi: 10.21037/jlpm-23-84

View this article at: https://dx.doi.org/10.21037/jlpm-23-84

Since healthcare institutions are progressively becoming primary targets of cyber-attacks that could compromise patient information and prevent medical personnel from providing diagnostics, treatments and other essential services, cyber security has become a mainstay in the field (1). On October 22, 2023 at 10:30 p.m., the information technology (IT) system of the University Hospital of Verona was the target of a disruptive cyber-attack, when a virus (likely a ransomware) was maliciously introduced by cyber terrorists. The virus rapidly encrypted several files on most of the servers that housed hospital's software applications. The immediate outcome was a complete breakdown in all informatics-related operations, including intranet, hospital information system (HIS; which also includes order entry for laboratory tests and the area where laboratory reports can be displayed in the wards) and laboratory information system (LIS). Order entry and test result visualization become immediately unavailable, and all laboratory equipment was no longer connected to the LIS, so that manual programming was the only means to operate the laboratory instrumentation.

The Laboratory Medicine Service of the University Hospital of Verona consists of two central laboratories that serve two hospitals on the opposite sides of town (north and south, totaling around 1,200 beds), as well as two emergency rooms, intensive care units, a trauma center, and several other acute care and regular wards. The complete disruption of IT system operations prompted the activation of a recovery plan, which had already been agreed upon with the medical direction, designed to face these issues and other potential emergencies. The main features of this recovery plan are summarized in *Figure 1*. All routine laboratory activities were interrupted for the entire duration of the emergency (which ended at 11:00 a.m. of October 26, 2023). To place laboratory test requests, the various wards could download an "emergency request module" from a folder stored in the desktop of all hospitals' local personal computers. The module contains a series of fields that phlebotomists must fill out, as summarized in *Table 1*. According to the recovery plan, the personnel in the wards was instructed to draw the blood, fill out the emergency request module, and handwrite the patient's surname, first name, date of birth, and identification code (if available) on each blood tube label. Each set of unique patient samples was placed in a plastic bag with the corresponding emergency request module and shipped to the two hospitals' laboratories. When the samples arrived, the laboratory staff recorded the arrival time on a dedicated form, prepared the blood tubes for testing (e.g., by centrifugation if necessary), and delivered the tubes with their corresponding emergency request module to the "Corelab", i.e., the open space where clinical chemistry, immunochemistry, hematology, coagulation tests, and urinalysis are performed in both laboratories. The Corelab technicians manually programmed the instrumentation based on the tests requested for each sample, loaded the tubes, and performed the analyses. Test results were then transferred to a specific "emergency results module", which was faxed to the wards.

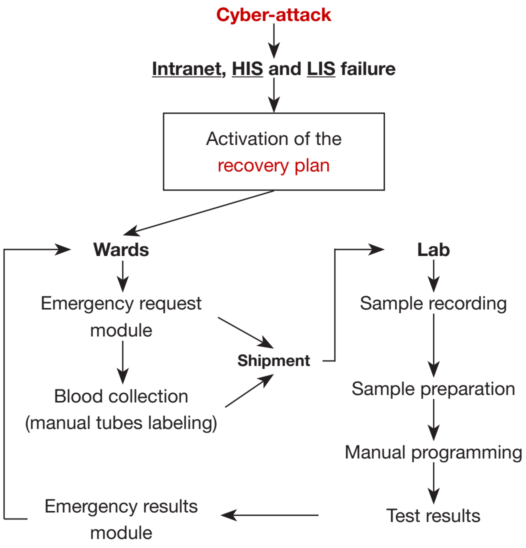

Figure 1 The "emergency" plan activated upon the combined failure of the HIS and the LIS. HIS, hospital information system; LIS, laboratory information system.

Table 1 Information contained in the emergency module for requesting laboratory tests

• Name and surname of the patient
• Date of birth of the patient
• Patient identification code (if available)
• Name of the ward
• Hospital code of the ward
• Fax number of the ward
• Telephone number of the ward
• List of urgent tests that could be selected (around 20 in total, encompassing basic clinical chemistry, immunochemistry, hematology, coagulation tests and urinalysis)

Table 2 Lesson learnt from a devastating cyber-attack

• Define an emergency plan for surrogating HIS and LIS failure
• Made available to all the wards an emergency request module, containing at minimum the information listed in *Table 1*
• Made available to all the wards a list where the type of tubes is specified for each analysis
• Optimize laboratory workflow according to the new organization
• Prepare an "emergency results module" to be stored in the lab
• Maintain a sufficient number of fax machines
• Consideration should be done to stop routine activity

HIS, hospital information system; LIS, laboratory information system.

This second module contains complete patient information, test results and the expected (general) reference range for each test. In this way, the diagnostic activity (limited to the panel of available tests) could continue uninterruptedly until the function of the HIS and LIS could be restored, after nearly 3 days of interruption.

This disruptive event, which could be efficiently managed through the availability of a predefined recovery plan, paves the way for a number of considerations (*Table 2*) that are becoming increasingly important as cyber-attacks and other environmental conditions that may lead to disruption of both HIS and LIS (e.g., power interruption due to natural disasters, wars, blackouts) increase in frequency (1-3).

First, a laboratory-specific recovery plan to be activated in the event of a hospital IT system failure must be developed in consultation with the local medical direction of the hospital, as these and other types of disruptive events can occur almost everywhere. An "emergency request module", with at least the information listed in *Table 1*, should then be made available to all hospital wards, along with another document indicating the type of tube to be collected for each analysis, so that the phlebotomist will know exactly how many and which samples must be drawn. Importantly, the emergency request module can also be prepared to include adhesive labels on the underside, indicating the number of the module and a field for writing patient information, so that patient samples can be labeled with a unique sequential number corresponding to a unique module. The laboratory workflow must also be completely reorganized in accordance with the new organization, with efficient integration among technicians from various laboratory sectors, to ultimately optimize sample processing and analysis under emergency conditions. Furthermore, an "emergency results module" should be prepared and kept in the laboratory, where test results can be transcribed as soon as they are ready, and then sent to the requesting wards. This module must include essential data such as patient information, laboratory test results, and a generic reference

Table 3 Measures that should be taken to protect medical laboratories from cyber-attacks

• Install valid antivirus software and reliable firewalls in the hospital and laboratory information systems to prevent outside intrusion
• Educate laboratory staff about cyberattacks: perform regular meetings and training sessions to inform the staff about the modalities used by cyber-terrorist to attack public and private facilities
• Pay close attention to unsolicited messages: be wary of emails, instant messages or phone calls from people you do not know. Be especially cautious and do not respond to requests for login credentials, requests requiring an urgent response, unpaid bill notices and appeals for donations
• Recognize suspicious emails and text messages: always check the reliability of the sender of emails, text or chat messages. If you have any suspicions, do not reply, do not click on links or open attachments and contact the Information Systems service immediately so that immediate countermeasures can be taken
• Learn to recognize suspicious sites: malicious websites can be very similar to the original ones, both in name and content. Before clicking on a link, check the actual destination and make sure you are visiting protected sites where there is a padlock symbol and the address always starts with https://
• Do not pass on your access data to third parties: do not pass on your access data to anyone, either inside or outside the company
• Never leave electronic devices assigned to you by the company to perform your duties unattended: if you are not at your workplace, make sure that your PC or other device is locked and cannot be accessed by third parties
• Only use tools or software approved by the company: do not use and download tools or software that have not been approved by the company and have not been checked beforehand by the Information Systems Service
• Only use IT tools approved by the company: do not use personal IT devices (e.g., laptops, tablets, etc.) to perform work tasks and to use them in connection with company IT tools

PC, personal computer; IT, information technology.

range that can aid in the interpretation of test results.

Another clear outcome of this crisis is that fax machines remain indispensable even in the digital age, as they have become our primary (and only) means of transmitting laboratory information to the wards. As the transmission of more than 1,200 faxes can cause very long bottlenecks, a minimum number of fax machines must be available in the laboratory (depending on the size of the hospital). The complete cessation of routine activity should then be locally considered. In our case, this was practically required because the two nearby laboratories perform nearly 800 different types of tests, which would be impossible to handle without informatics support. More importantly, the many routine requests and accompanying tests would not have allowed to handle the "real" clinical emergencies in a timely manner. In most cases, sensitive patient data that the cyber terrorists may have had access to and/or stolen is published on the "dark web" and is therefore inaccessible to the vast majority of internet users. This information is usually identified by the police or by certain companies operating in this field and passed on to the company, which then has a duty to inform all patients whose data has been breached.

Strengthening cybersecurity and, in particular, developing recovery plans that will allow laboratory operations to continue during prolonged periods of IT system failure are essential for the future (4). In this respect, a set of measures can be identified to reinforce the protection of medical laboratories from cyber-attacks, as listed in *Table 3*. We hope that the unfavorable hypothesis that other hospitals will encounter this and other comparable incidents could benefit from our experience and reflections.

Acknowledgments

Funding: None.

Footnote

Provenance and Peer Review: This article was a standard submission to the journal. The article has undergone external peer review.

Peer Review File: Available at https://jlpm.amegroups.com/article/view/10.21037/jlpm-23-84/prf

Conflicts of Interest: Both authors have completed the

ICMJE uniform disclosure form (available at https://jlpm.amegroups.com/article/view/10.21037/jlpm-23-84/coif). G.L. serves as the Editor-in-Chief of *Journal of Laboratory and Precision Medicine*. The other author has no conflicts of interest to declare.

Ethical Statement: The authors are accountable for all aspects of the work in ensuring that questions related to the accuracy or integrity of any part of the work are appropriately investigated and resolved.

doi: 10.21037/jlpm-23-84
Cite this article as: Lippi G, Ferrari A. Lessons learnt in medical laboratories during a disruptive cyber-attack. J Lab Precis Med 2024;9:18.

References

1. Aljuraid R, Justinia T. Classification of Challenges and Threats in Healthcare Cybersecurity: A Systematic Review. Stud Health Technol Inform 2022;295:362-5.
2. Lippi G, Favaloro EJ, Plebani M. Laboratory medicine and natural disasters: are we ready for the challenge? Clin Chem Lab Med 2010;48:573-5.
3. Lippi G, Cadamuro J, Danese E, et al. Results of the first survey of the EFLM Task Force Preparation of Labs for Emergencies (TF-PLE). Clin Chem Lab Med 2023;61:e235-8.
4. Patel AU, Williams CL, Hart SN, et al. Cybersecurity and Information Assurance for the Clinical Laboratory. J Appl Lab Med 2023;8:145-61.