Peer Review File

Article information: https://dx.doi.org/10.21037/jlpm-23-84

Reviewer Comments

Comment 1: The article is very valuable from the point of view of the topic of cybersecurity. I would like to ask you to make the following changes to the manuscript: I will ask you to prepare a more extensive Figure 1.

Reply 1: We are thankful for these valuable comments on our work. We will do our best to improve the manuscript according to the suggestions. Thanks for this comment. Figure 1 explains exactly what has been done in the lab after the cyberattack. Nothing else needs to be added to our side. Therefore, figure 1 is left unchanged.

Comment 2: How can we defend laboratory systems against cyberattacks?

Reply 2: Thanks for this comment, very useful. We have included a new table (Table 2) that lists most of the measures that should be taken to protect medical laboratories from cyber-attacks, as follows:

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.

Comment 3: How and how should the laboratory develop a procedure for dealing with a cyber attack?

Reply 3: See new table 3.

Comment 4: Can a cyber attack be prevented by introducing security measures in the HIS and LIS systems?

Reply 4: See new table 3.

Comment 5: How can a patient verify whether his sensitive data has been disclosed?

Reply 5: In most cases, sensitive patient data 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. This information has been included in the text of the article.