Letter to the Editor

Giuseppe Lippi*, Janne Cadamuro, Elisa Danese, Emmanuel J. Favaloro, Julien Favresse, Brandon M. Henry, Snezana Jovicic, Tomris Ozben, Jecko Thachil and Mario Plebani

EFLM Task Force Preparation of Labs for Emergencies (TF-PLE) survey on cybersecurity

https://doi.org/10.1515/cclm-2024-0727
Received June 21, 2024; accepted June 22, 2024;
published online July 4, 2024

Keywords: laboratory medicine; cybersecurity; cyber-attacks

To the Editor,

According to the Oxford online dictionary, a cyber-attack is usually defined as “an attempt by hackers to damage or destroy a computer network or system”. In other words, it encompasses all forms of malicious activity intentionally conducted for collecting, disrupting, denying, compromising or even destroying data from information systems or the information system itself [1].

***Corresponding author: Prof. Giuseppe Lippi**, MD, Section of Clinical Biochemistry, University Hospital of Verona, Piazzale LA Scuro, 37134 Verona, Italy, E-mail: giuseppe.lippi@univr.it. https://orcid.org/0000-0001-9523-9054
Janne Cadamuro, Department of Laboratory Medicine, University Hospital Salzburg, Paracelsus Medical University, Salzburg, Austria. https://orcid.org/0000-0002-6200-9831
Elisa Danese, Section of Clinical Biochemistry, University of Verona, Verona, Italy. https://orcid.org/0000-0002-2454-0410
Emmanuel J. Favaloro, Haematology, NSW Health Pathology, Sydney Centres for Thrombosis and Haemostasis, ICPMR, Westmead Hospital, Sydney, Australia. https://orcid.org/0000-0002-2103-1661
Julien Favresse, Services of Clinical Biology, Clinic Saint-Luc, Bouge, Belgium
Brandon M. Henry, Clinical Laboratory, Division of Nephrology and Hypertension, Cincinnati Children’s Hospital Medical Center, Cincinnati, OH, USA
Snezana Jovicic, Department for Medical Biochemistry, Faculty of Pharmacy, University of Belgrade, Belgrade, Serbia
Tomris Ozben, Department of Medical Biochemistry, Faculty of Medicine, Akdeniz University, Antalya, Türkiye
Jecko Thachil, Immune Thrombocytopenic Purpura (ITP) Clinic, Haematology Department, Manchester University NHS Foundation Trust – Manchester Royal Infirmary, Manchester, UK
Mario Plebani, Department of Medicine, University of Padova, Padova, Italy. https://orcid.org/0000-0002-0270-1711

Cyber-attacks in healthcare have become increasingly common over the past decade, causing significant risk to patient safety, data privacy and the functioning of the healthcare system as a whole [2]. Regardless of type of malware and severity of attack, these cyber-attacks very often flood healthcare systems with huge traffic causing disruptions in service delivery, encrypt healthcare information, subtract sensitive patient information (including personal, medical and financial data), and demand a ransom for restoring data access or for preventing their sale on the black market or publication in the so-called “dark (deep) web”. The consequences are often devastating for the institution, and include several aspects from clinical (i.e., disruption of services, delayed diagnoses and treatments), financial (costs for remediation, legal actions, regulatory fines and loss of revenue due to unavailability of services) and even reputational (trust, loyalty and reputation in healthcare providers can be seriously undermined) standpoints [2, 3].

Due to the high degree of computerization and digitalization (i.e., computerized physician order entry, clinical decision support systems, bidirectional communication with laboratory equipment, generation and permanent storage of digital laboratory reports, remote instrument monitoring and maintenance, digital data sharing within networks of laboratories, etc.), clinical laboratories are among the most vulnerable areas to cyber-attacks within the entire healthcare industry [4]. To this end, the Task Force Preparation of Labs for Emergencies (TF-PLE) of the European Federation of Clinical Chemistry and Laboratory Medicine (EFLM) has conducted a specific survey to determine the current state-of-the art on cyber-attacks of laboratory medicine in Europe.

The survey, which consisted of a series of general questions on local organization, perceptions of and experiences with cyber-attacks (as summarized in Supplementary File 1), was sent out on 20 December 2023 with an official EFLM newsletter to the email addresses of the over 12,000 potential EFLM contacts from Europe and abroad. The survey remained open for nearly 2 months, i.e., until March 1, 2024. All responses from European centers were transferred to an Excel spreadsheet and analyzed graphically. This survey was

endorsed by the EFLM and did not involve any medical treatment, so that no ethics committee approval was needed.

The questionnaire received 126 responses from Europe; seven additional responses from abroad were excluded from this analysis. The most represented countries were Italy (21.4 %) and Serbia (19.0 %), followed by Ireland (7.1 %), Croatia (4.8 %), Romania and the United Kingdom (both 4.0 %), Belgium, Germany, Slovenia and Spain (all 3.2 %), etc. A total of 35/41 EFLM countries took part in the survey. The results of the EFLM TF-PLE survey are summarized in Supplementary File 1, and will be briefly discussed in the following part of this article.

The first three questions concerned respondents' familiarity with malware, cyber-attacks and cybercriminals' strategies, to which 68.3 , 68.3 and 53.2 % replied that they were moderate/very familiar. The next two questions concerned the personal experience with cyber-attacks; 34.1 % of respondents answered that they had already been the victim of one or more cyber-attacks at their institution, and 65.1 % thought it was likely that they would be the victim of a cyber-attack in the future. The next two questions concerned the location of the hospital information system (HIS) and the laboratory information system (LIS); only 11.1 and 15.9 % of respondents stated that the servers were physically located in the cloud, while the rest did not know their exact location (42.1 and 27.8 %), or stated that the servers were physically located in the hospital (46.8 and 56.3 %). A remote connection to access hospital domains was available to 60.3 % of respondents, but 2-factor identification was only used (or is programmed to be available in the future) by 57.1 % of facilities. Antivirus programs and firewalls were running on 84.1 % and 82.5 % of hospital computers, respectively. Nevertheless, only 69.8 % of respondents reported receiving recommendations from their healthcare facility about security measures to prevent cyber-attacks. Regarding the existence of a recovery plan to defend the facility and laboratory against cyber-attacks, 22.2 % of respondents stated that it was in place for the entire hospital and 18.3 % only for the laboratory. To the last question about the willingness to receive EFLM suggestions/recommendations for prevention/management of cyber-attacks in the healthcare facility/laboratory, 81.7 % responded positively.

Although the modest number of responses and their specific geographical location must be considered as limitations, some important conclusions can be drawn from the results of this EFLM TF-PLE survey. First, a significant percentage of respondents (over 30 %) stated that they were somewhat unfamiliar with malware, cyber-attacks and strategies of cybercriminals, which combined with a similar percentage of respondents who had never received cybersecurity instructions from their institution, and with the vast majority of respondents who expressed a willingness to receive formal guidance from the EFLM on this topic, highlights the important point that increased cybersecurity training for laboratory staff is both necessary and critical, and that incident response planning must be considered a priority for all European hospitals and clinical laboratories. This reasoning is also supported by the evidence that the surveyed institutions appear quite vulnerable to cyber-attacks (e.g. low number of servers in the clouds, which would make them less accessible to cybercriminals, almost 50 % of respondents do not use multi-factor identification), and that almost two-thirds of respondents consider the possibility of becoming a victim of a cyber-attack in the future. Another survey conducted in the US between April 2019 and May 2021 generated similar evidence, as the authors concluded that US hospitals are still not adequately prepared for cybersecurity disasters [5], which would lead us to extrapolate our conclusions to a larger number of worldwide countries.

Research ethics: This survey was endorsed by the EFLM and did not involve any medical treatment, so that no ethics committee approval was needed.
Informed consent: Not applicable.
Author contributions: All authors have accepted responsibility for the entire content of this manuscript and approved its submission.
Competing interests: The authors state not conflict of interest.
Research funding: None declared.
Data availability: Data will be available upon reasonable request tot he corresponding author.

References

1. National Institute of Standards and Technology (NIS). Cyber attack. https://csrc.nist.gov/glossary/term/cyber_attack [Accessed 18 Jun 2024].
2. Niki O, Saira G, Arvind S, Mike D. Cyber-attacks are a permanent and substantial threat to health systems: education must reflect that. Digital Health 2022;8:20552076221104665.
3. Abbou B, Kessel B, Ben Natan M, Gabbay-Benziv R, Dahan Shriki D, Ophir A, et al. When all computers shut down: the clinical impact of a major cyber-attack on a general hospital. Front Digit Health 2024;6: 1321485.
4. Patel AU, Williams CL, Hart SN, Garcia CA, Durant TJS, Cornish TC, et al. Cybersecurity and information assurance for the clinical laboratory. J Appl Lab Med 2023;8:145–61.
5. Sullivan N, Tully J, Dameff C, Opara C, Snead M, Selzer J. A National Survey of hospital cyber attack emergency operation preparedness. Disaster Med Public Health Prep 2023;17:e363.

Supplementary Material: This article contains supplementary material (https://doi.org/10.1515/cclm-2024-0727).