SY03

Update on laboratory support for typhoid

Aziah Ismail

Institute for Research in Molecular Medicine (INFORMM), Universiti Sains Malaysia, Kubang Kerian, Kelantan

SUMMARY

Typhoid fever has subsequently been largely controlled in many parts of the world due to considerable developments in water, sanitation, and hygiene (WASH), although it was still estimated to have caused 10.9 million illnesses and 116,800 deaths globally in 2017. As the threat of emerging infectious diseases grows, it is crucial to detect illnesses early and prevent further spread. The genetic diversity and relatedness of the Salmonella isolates were determined using culture and genotyping methods. A pattern in the spread of typhoid is also discovered using spatial analysis. With the capability of whole-genome comparisons, we were able to gather data from biologically similar organisms. The illness screening process uses antibody-based detection, whereas the confirmation test uses a molecular approach. Data from diagnostic laboratories, point-of-care test readers, and devices must be linked to health practitioners in order to provide timely information for the early diagnosis of infectious disease epidemics.

SY04

Innovative digitalization of prison registry system: The cyber risk and resilience

Solahuddin Shamsuddin

Cybersecurity Malaysia

SUMMARY

Digitalization has opened new possibilities in various sectors, enabling advancement in the management and organization's facilities, streamlined processes, and improved outcomes. By leveraging digital technologies and electronic communications, the prison registry system has transitioned from traditional paper-based record-keeping to a digital platform. This evolution allows for the seamless integration of detainee's information, tracking of detainee's movement, and real-time updates on critical data. As a result, administrator's personnel can access accurate and up-to-date information promptly, leading to faster decision-making and improved detainees' management. However, this digitalization effort also creates significant cyber risk challenges that need to be addressed with effective cyber resilience strategies. The transition to a digital prison registry system opens potential vulnerabilities that malicious actors may exploit. Cyber threats, such as data breaches, unauthorized access, and ransomware attacks, pose significant risks to the confidentiality and integrity of sensitive information. Addressing these cyber risks, it emphasizes how critical it is for organizations to create an ecosystem that is resilient to cyberattacks. This entails the implementation of strong cybersecurity measures, regular risk assessments, and ensuring staff training are essential steps to safeguard the prison registry system from cyber threats. Incident response plans should be in place for effective responses in the event of a cyber-attack, ensuring minimal disruption to prison operations and data integrity. Furthermore, it is important to understand the significance of collaboration and information sharing among entities to bolster collective cyber resilience efforts. Platforms for disseminating relevant information can help spread Threat Intelligence and best practices while maintaining data privacy and compliance, fostering a community-based defence against cyber threats. However, to achieve solid cyber defence is difficult due to resource shortages, budgetary restrictions, and a constantly changing cyber threat landscape. It urges organizations to take a forward-thinking stance by integrating cutting-edge technologies such like Biometric Security Controls, Cyber Security solutions powered by Artificial Intelligence, Digital Risk Protection, Attack Surface Management, and regular penetration testing to discover vulnerabilities and proactively address potential breaches. Embracing cyber resilience as part of the digitalization journey is essential for safeguarding digital information, maintaining trust in organization's systems, and ensuring uninterrupted delivery of quality services in the presence of persistent cyber threats. By acknowledging the need for a proactive Cyber Security culture, fostering collaboration, and prioritizing cyber risk management, organizations can navigate the digital landscape securely and create a resilient future against cyber threats.