Cybersecurity in healthcare

Mohd Nawawi Mustafa

ICT Consulting Division, Malaysian Administrative Modernization and Management Planning Unit (MAMPU), Malaysia

SUMMARY
COVID-19 has transformed our way of doing things, where digital transformation is prevalent. The healthcare industry has embraced technological advancements to deliver better patient care and streamline operations. However, these innovations also open the door to cybersecurity threats that can compromise patient data and disrupt services. In delivering fast and efficient healthcare services to the clients, highly sensitive electronic health information is at risk. It is handled by most clinics and hospitals in numerous digital systems without proper ICT security assessment. Providers such as physicians and pharmacists use electronic health records and other software working with medical information. And this data is a very tempting target for cybercriminals. Even though the advancements in ICT technologies such as adoption of public clouds and usage of personal electronic devices in managing and accessing patients' data enables physicians to deliver healthcare services to the patients at any time, it also introduces risk of data breach and other cybersecurity threats to the health data if not properly addressed. This session discusses an in-depth explanation of the challenges in the healthcare industry in Malaysia from the perspective of people, process and technology, the importance of cybersecurity in healthcare, emerging cybersecurity threats and best practices to protect healthcare data as required by laws, government circulars and ICT security best practices.