Cyber-attacks, Infectious Diseases and the Next Global Public Health Emergency

Dr Saif F Abed BSc MBBS MPhil MSc
Information Risk Consultant
Biosecurity and Health Security Protection (BSP) Unit, World Health Organization

Sophie Allian Ioos
Nahoko Shindo
Matthew Lim

3-5 April 2023
Maison de la Chimie, Paris, France
During the Covid-19 pandemic hospitals experienced...
During the Covid-19 pandemic hospitals experienced...
During the Covid-19 pandemic hospitals experienced...
During the Covid-19 pandemic hospitals experienced...
During the Covid-19 pandemic hospitals experienced...
During the Covid-19 pandemic hospitals experienced…

DELAYED CANCER TREATMENTS
Because of...
MASSIVE AND CATASTROPHIC CYBER-ATTACKS
Cyber-attacks are increasingly linked to patient harm and even deaths.
Cyber-attacks are increasingly linked to patient harm and even deaths.
WHAT ARE THE EMERGING CYBER THREATS?
What is Cybersecurity?

- Cybersecurity can be explained as the protection of digital data, systems, assets and processes from:
  - Data breaches
  - Loss of Access
  - Tampering
What is Cybersecurity?

• Cybersecurity can be explained as the protection of digital data, systems, assets and processes from:
  
  • Data breaches
  • Loss of Access
  • Tampering

• Basically, this means any digital product (hardware/software) that connects to an organizational network or the internet will be of concern
Why does it matter?
Why does it matter?

- Attacks against healthcare increased dramatically during the Covid-19 pandemic

- Cyber-attacks have caused ambulance diversions, delayed cancer care, cancelled appointments and operations at national scales
Why does it matter?

• The entire biomedical ecosystem - including research laboratories, diagnostic centers, vaccine manufacturers and biotech contractors – is at risk.

• Security researchers are uncovering new and novel ways to exploit existing facilities and new technologies.
Why does it matter?

- The entire biomedical ecosystem—including research laboratories, diagnostic centers, vaccine manufacturers and biotech contractors—is at risk.

- Security researchers are uncovering new and novel ways to exploit existing facilities and new technologies.
WHO Activities

• Since July 2021, the Biosecurity and Health Security Protection (BSP) Unit has been analysing cybersecurity risks to public health

• Internal reports examining the impact of cyber-attacks during the Covid-19 pandemic like ransomware have been produced (publication in pipeline)

• An informal Information Risk Working Group has been formed including stakeholders from UN agencies, law enforcement, academia and NGOs
Key Observations

• This is a global problem and rapidly evolving threat

• It is too often seen as a purely ‘tech’ problem

• Public health agencies, Ministries of Health and scientific institutions do not have enough awareness of the potentially catastrophic risks to critical infrastructure

• Cyber-preparedness and resiliency are immature and underfunded
Solutions

• Development of capacity building tools, frameworks, checklists, simulation exercises and alerting mechanisms to support Member States aligned with Joint External Evaluation (JEE) tools as part of a One Health approach

• Greater Member State engagement to raise awareness

• Development of a World Health Assembly/UN norm or convention denouncing cyber-attacks against health and biological critical infrastructure
Thank you

Dr Saif Abed
Information Risk Consultant, Biosecurity and Health Security Protection (BSP) Unit
World Health Organization

Dr Saif Abed: abeds@who.int
Dr Sophie Ioos: iooss@who.int

This event is supported by funding from:
Reference List

10. https://thebulletin.org/2023/01/researchers-hacked-a-labs-pathogen-containment-system-was-it-a-good-idea-to-publish-the-results/