A Planned Study on Physician Attitudes to Cybersecurity risks and Implementation Barriers

Dr Njideka Nto MBBS,MRCGP,MBA
Medical Director, Mediclinic Dubai Mall, UAE

MEDICLINIC
DUBAI MALL

Declarations and Acknowledgements

No conflicts of interest

MEDICLINIC
DUBAI MALL

INTRODUCTIONS & CONTEXT

Mediclinic Group, is an international private hospital group. It operates seven hospitals and over 20 clinics with over 900 inpatient beds across the United Arab Emirates

Mediclinic Dubai Mall is Dubai's largest ambulatory care medical centre, housing a day surgery unit, outpatient consultation and treatment facilities and a comprehensive diagnostic imaging centre

The contents of the subsequent slides relates to a study which is currently in progress and exploring Physician Awareness of Cybersecurity risks and the Barriers to Implementation of Cybersecurity Measures in a Private Healthcare Setting

Views expressed in these slides are mine and not necessarily those of the organisation

MEDICLINIC
DUBAI MALL

TECHNOLOGY AND HEALTHCARE

Technological advancements and the associated exponential growth of healthcare data, presents both opportunities and threats

Big data analytics hold immense potential for accelerating medical research, improving patient care, and generating value for healthcare organizations

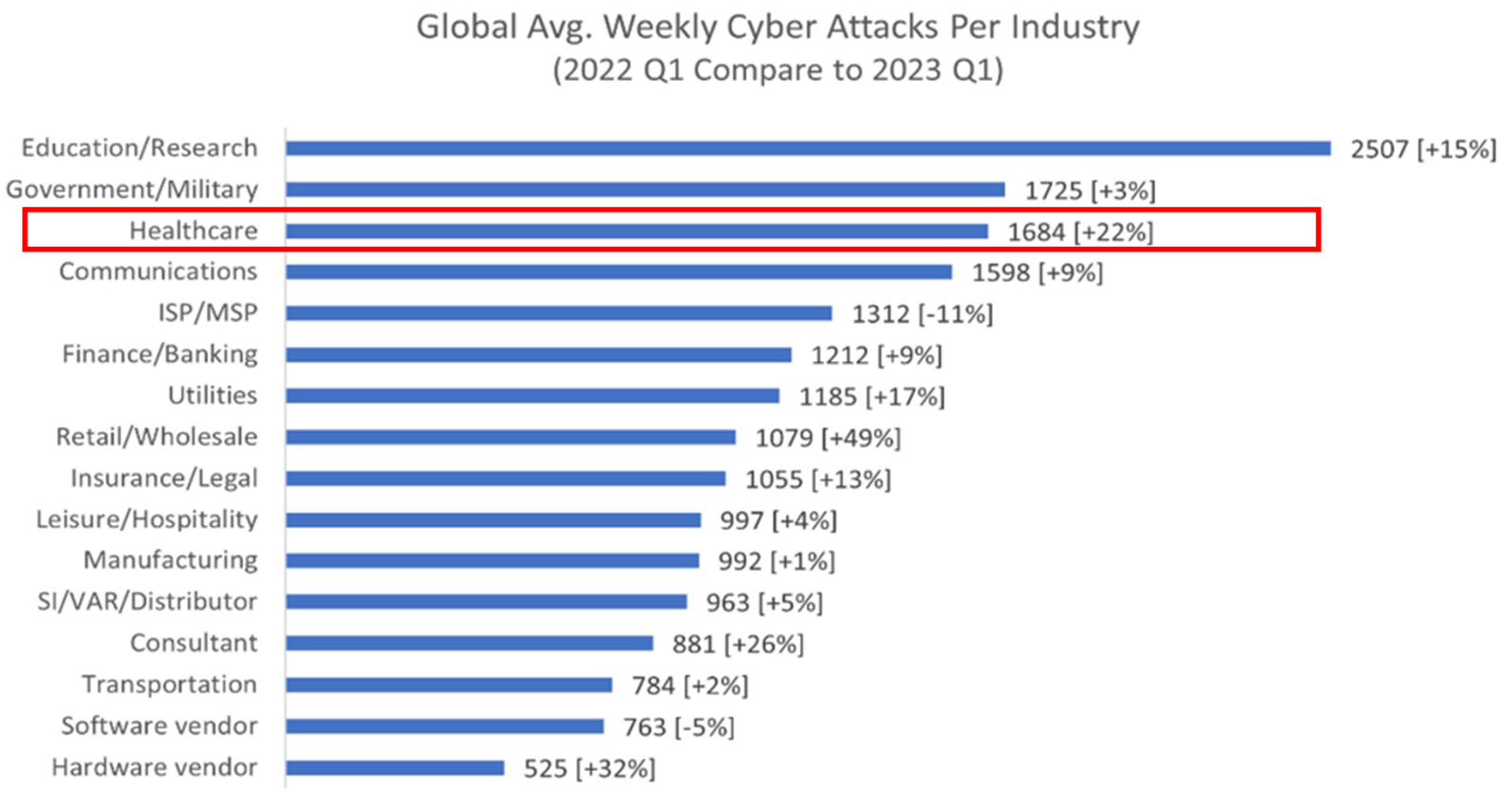
However, the proliferation of health data, the increasing interconnectedness of health systems, and integration into networked environments, comes with a risk of exploitation

No surprises therefore that healthcare systems face risks, such as data breaches, theft, and damage

MEDICLINIC
DUBAI MALL

RISING INCIDENTS OF CYBER ATTACKS

In the US alone, over the past five years, there has been a 256% increase in large health-related breaches, involving hacking and a 264% increase in ransomware



Source: Check Point Software Technologies (https://www.weforum.org/agenda/2023/05/cyber-attacks-on-healthcare-rise-zero-trust)

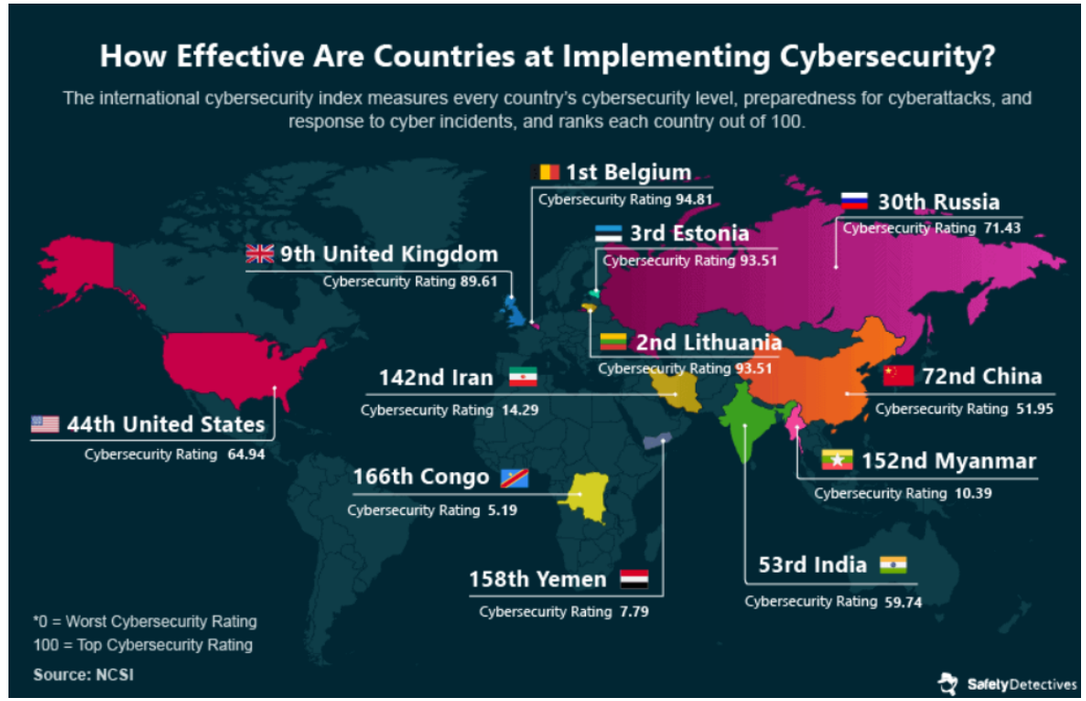
MEDICLINIC DUBAI MALL

THREAT TO CYBERSECURITY

The critical role of cybersecurity in healthcare delivery: protect patient privacy, safeguard medical infrastructure, secure connected devices, and preserve data integrity

Common techniques used by attackers to assess healthcare data includes:

- Ransomware
- Malware
- Social engineering e.g. phishing
- System vulnerabilities
- Unauthorised internal disclosures
- Distributed Denial of Service (DDoS)



Source: Healthcare Cybersecurity: The Biggest Stats and Trends in 2024 (https://www.safetydetectives.com/blog/healthcare-cybersecurity-statistics/)

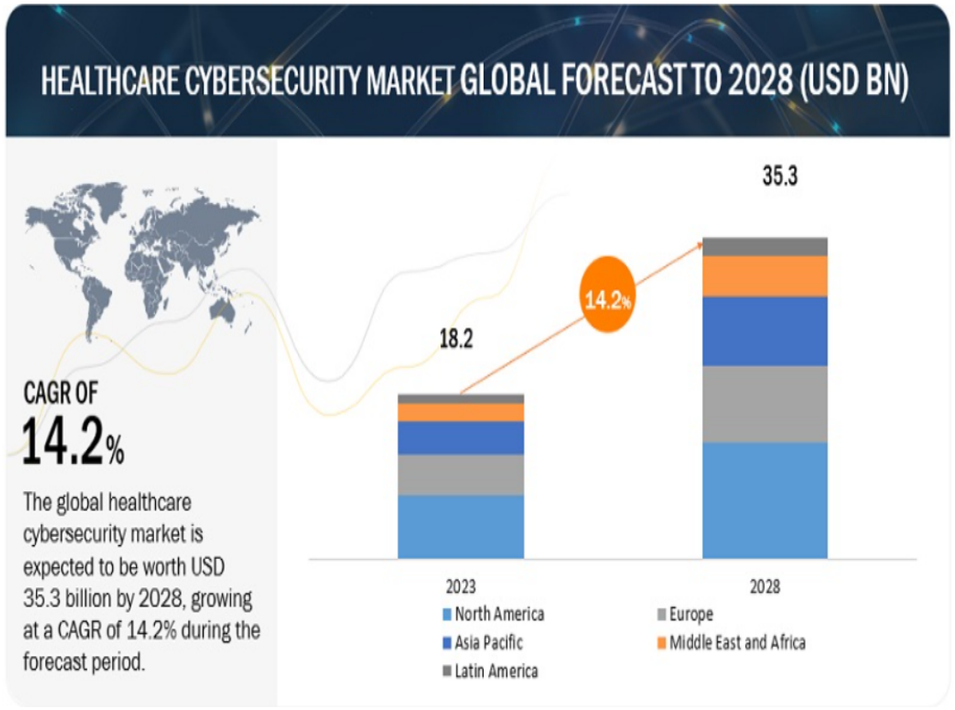
MEDICLINIC DUBAI MALL

HEALTHCARE CYBERSECURITY MARKET

Personal Health Information is often considered more valuable on the illegal market than credit or regular personal information, hence the attraction to cyber criminals

The growth seen in the healthcare cybersecurity market has been driven by:

- Rising data security and privacy concerns
- Increasing risks of healthcare cybersecurity attacks and data breaches
- Increasing utilization of cloud-based healthcare options
- Medical databases attractiveness as a large reservoir of sensitive & personal information



Source: Markets And Markets: Healthcare Cybersecurity Market: (https://www.marketsandmarkets.com/Market-Reports/healthcare-cybersecurity-market-215097518.html)

MEDICLINIC DUBAI MALL

THE OBJECTIVES OF OUR STUDY

Previous research have shown that human error is the most common cause of data breaches, ahead of other factors like theft, malware, hacking and misuse of data

Despite the well-documented cyber threats to patients' PHI, sparse evidence exists about the state of cybersecurity behaviour of health care workers and medical private practices

This has informed the study objectives i.e.,:

- Assess medical professionals' perception of cybersecurity threats in healthcare
- Assess the awareness of medical professionals, of cybersecurity measures and applicable regulations
- Assess medical professionals' experience of challenges and barriers in implementing cybersecurity measures

WHY THEMATIC ANALYSIS?

Thematic Analysis is recognized as a credible research method for identifying, analysing, organizing, describing, and reporting themes found within a data set

The study will adopt the Braun and Clarke protocol

- step 1- becoming familiar with the data
- step 2- generating initial codes
- step 3- searching for themes
- step 4- reviewing the identified themes
- step 5- defining the themes
- step 6- write up of the interpretation

ASSURING DATA QUALITY

Pre implementation of the study, there will be a validation of understanding and applicable assumptions around the chosen themes and response categorizations

Steps to be taken to assure quality of data collected

- Supplement/validate survey themes through literature review and qualitative discussions at Senior Leadership (SLT) meetings
- Implement pretesting of the survey questionnaire and the channel of data collection
- Maintain survey duration to less than 10 minutes to avoid respondent fatigue
- Routine data collection checks to ensure credibility and quality of data
- Secured storage of the study data in encrypted and password-protected files
- Maintain anonymity of responses and study participants

MEDICLINIC DUBAI MALL

STUDY TIMELINES

The study is currently at the Institutional Review Board (IRB) application stage, with scheduled completion of the final report by Q3 2024

Current Actions:

- Finalisation of study protocol [Ongoing]
- IRB application / approval [Ongoing]
- SLT Consultations [Ongoing]
- Consultation of cybersecurity stakeholders [Ongoing]

Next Steps:

- Finalisation of themes and study questionnaire based on expert feedback
- Deployment of study questionnaire
- Analysis and report development

MEDICLINIC DUBAI MALL

CONCLUSIONS

As technological advancements continue to revolutionise healthcare delivery, cybersecurity is indispensable in safeguarding the sanctity of patient data and the integrity of medical systems

The generated insight will add to the existing body of knowledge in supporting removal of barriers to the practical implementation of cybersecurity measures in healthcare

This ongoing study can be considered as an "*ideas contribution*" to this conference; therefore, today's presentation is also intended to generate feedback on our objectives and methodology from the listening audience

MEDICLINIC DUBAI MALL

COMMENTS & FEEDBACK

THANKS FOR LISTENING

MEDICLINIC
DUBAI MALL