

Cybersecurity in Healthcare:

Protecting Patient Data, Care Continuity, and Public Trust

Xiaoyi Chen



Why Healthcare Cybersecurity Is Social

- Digital healthcare has broader access, efficiency and susceptibility.
- Ransomware affects privacy, safety and care continuity.
- Daily human activities affect cybersecurity exposure.
- Organization’s resources influence institutional security capacity.
- Policies set accountability, preparedness and response expectations.
- Cyber incidents have broader social impacts (Munoz Cornejo et al., 2024).
- Necessary to have cybersecurity technical and social governance.



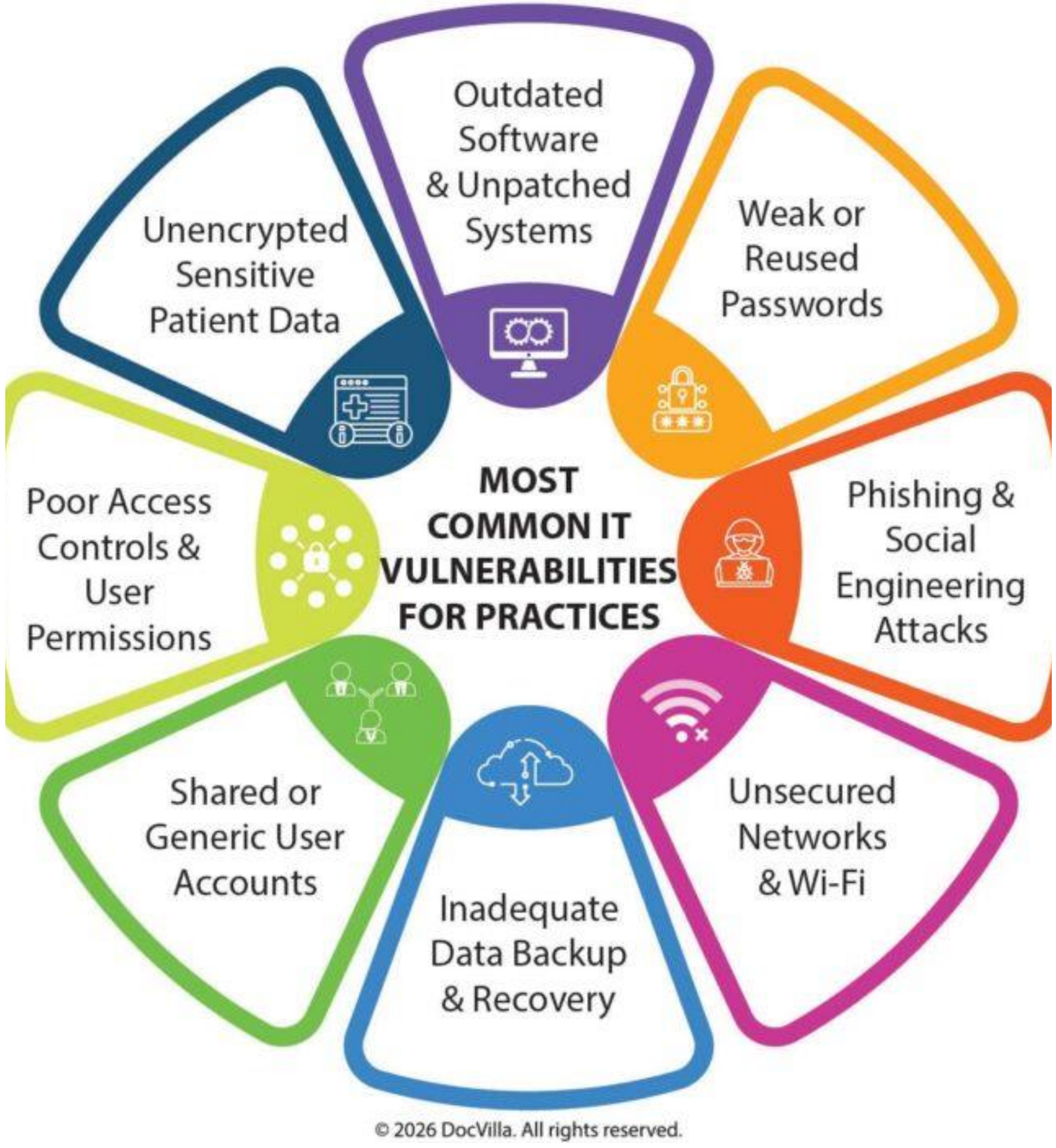
Privacy, Ethics, and Patient Trust

- Healthcare data crucial information with much personal data.
- Ransomware can affect clinical and financial information.
- Privacy breaches cause technological disruption among others (Munoz Cornejo et al. 2024).
- Patients need to be assured of in information security.
- Ethical Security balances confidentiality and access needs.
- Clear communication can reinforce responsible breaking good practices.
- Protection of privacy is thus an ethical duty.



Ransomware and Continuity of Care

- Ransomware disrupts critical health care functions.
- Digital availability necessary in clinical services (Neprash et al., 2024).
- A remarkable reduction in activity in the U.S. hospitals follows.
- Access for rural communities is more problematic.
- A longer travel time might be necessary in alternative facilities.
- So, any cybersecurity issues can exacerbate inequities in healthcare.
- Necessary coordinated continuity and recovery planning to build resilience.



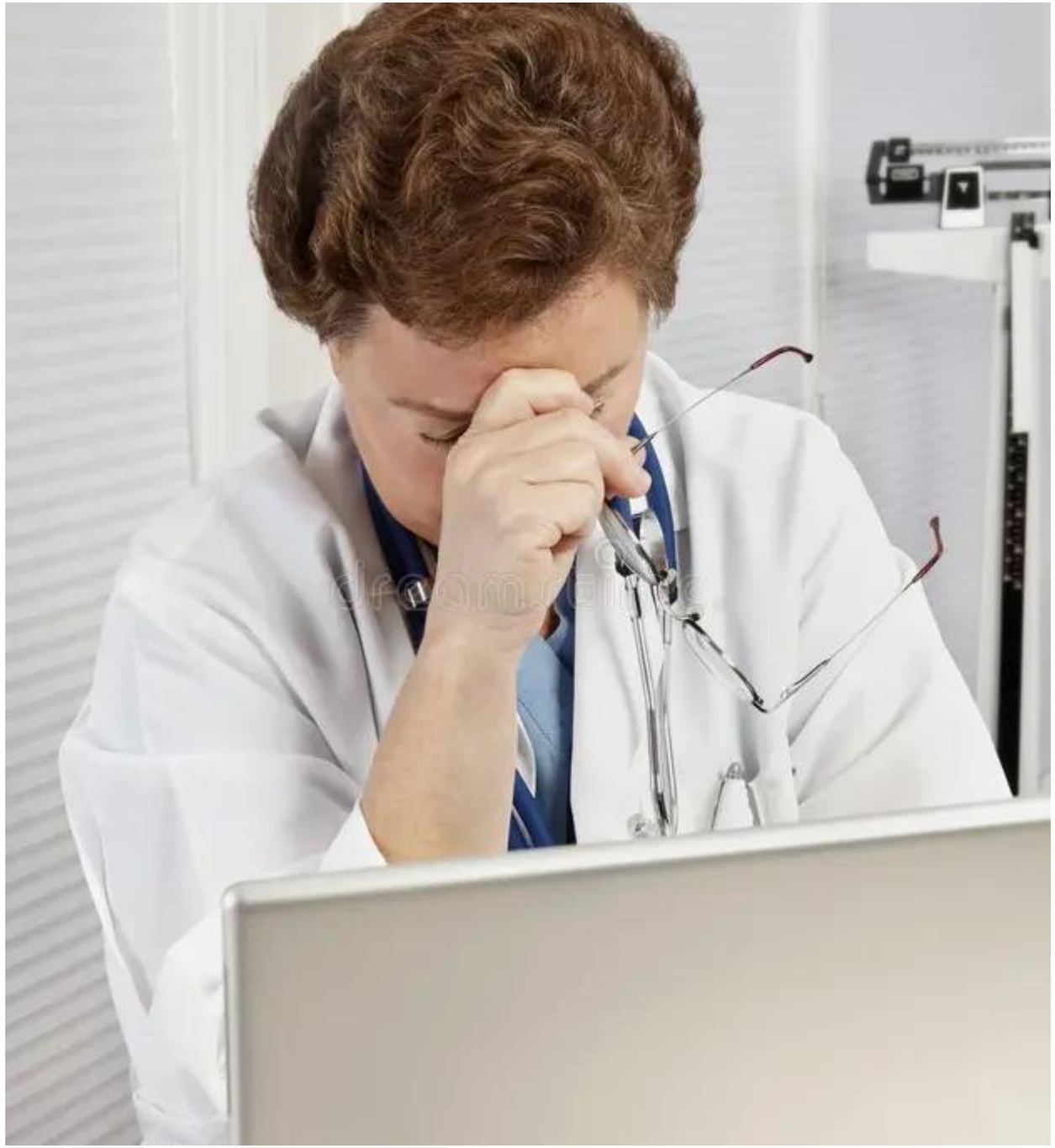
Organizational Vulnerability and Governance

- Cybersecurity vulnerability goes beyond problem-related technical aspects (McGlave et al., 2023).
- Hospital characteristics affect exposure to ransomware.
- Hospitals characteristics associated with attacked hospitals.
- Vulnerability not fully understood based on the technology capability.
- Resources affect prevention, preparedness and recovery capacity.
- Leadership role is to be accountable for cybersecurity decisions.
- Governance needs to incorporate organizational and technical risk.



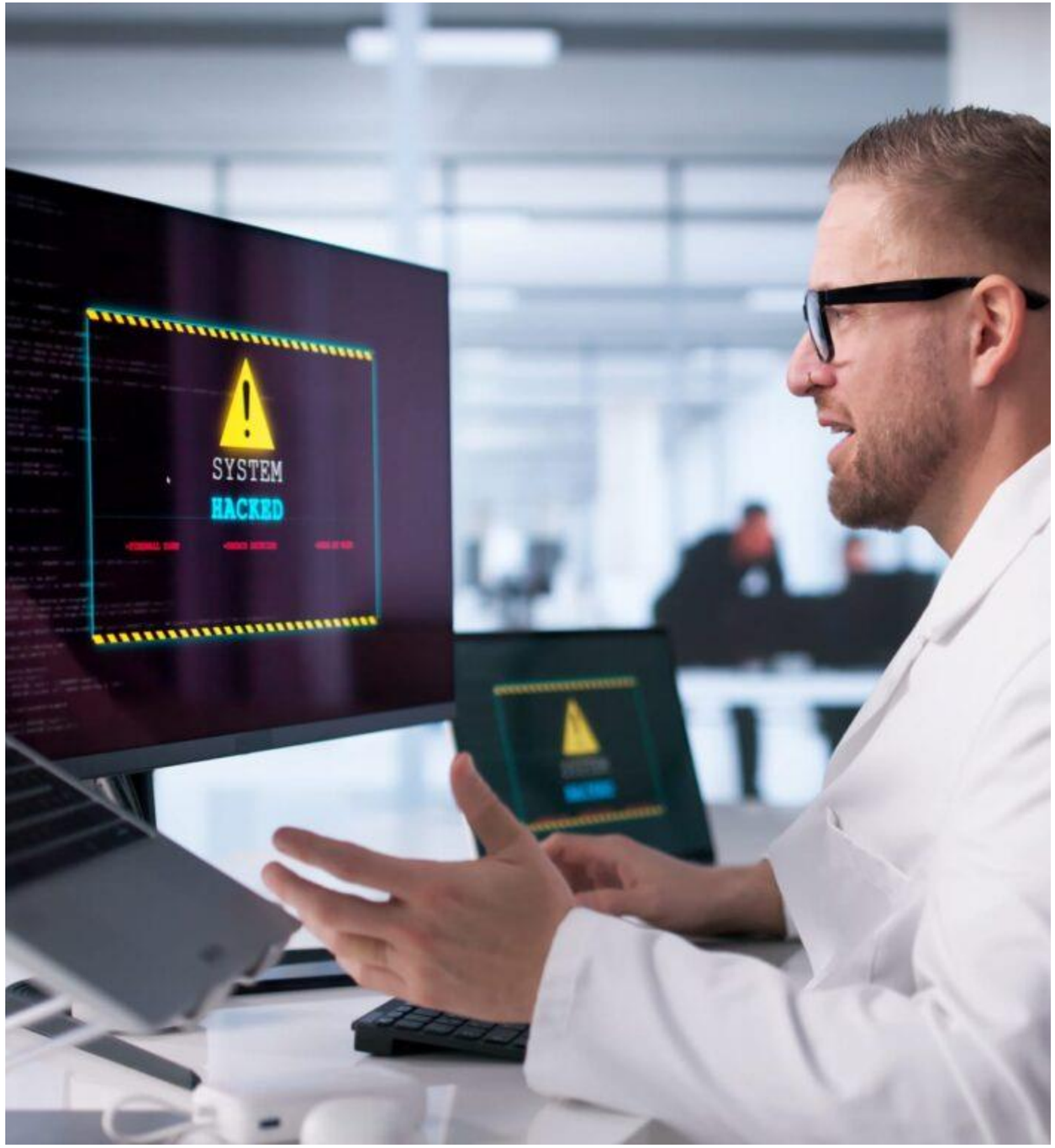
Human Behavior and Security Culture

- Cybersecurity systems constantly engaged with by employees.
- Phishing can be based on trust, urgency and attention (Munoz Cornejo et al., 2024).
- Human actions can add to cyber exposure for an organization.
- Punitive attitudes towards employees negatively impacts security reporting cultures.
- Training oriented towards recognizing, verifying and reporting.
- Escalation routes respond confidently to incidents.
- Security culture relates to organizational resilience.



Regional Spillover and Health-System Resilience

- Cyberattacks on organizations is wide (Dameff et al., 2023).
- Disruption may exist at neighboring emergency departments.
- Patients' diversions used to spread healthcare system burden.
- There may be a rise in workloads in nearby Institutions.
- Consequently, cybersecurity has level-2 impacts on the network.
- Coordinated emergency communication good for region preparation.
- Resilience is contingent on interdependent capacity building.



Mitigation Through Governance

- Several layers of defense for effective cybersecurity important.
- Identity and Access controls should be addressed to prevent.
- To detect, monitor and have effective reporting tools (Munoz Cornejo et al., 2024).
- Clearly-defined decision-making authority required for response.
- Tests of backups and downtime needed for recovery.
- Vendors have clear security expectations and oversight.
- Learning turns incidents into better organizational changes.



Implications for Leadership and Policy

- Multidisciplinary leadership responsibility in Healthcare Cybersecurity necessary.
- Privacy protection fosters patient trust and accountability.
- Workforce attitude has a bearing on organization daily security.
- Cyberattacks consequences impacts healthcare care equity access.
- Preparedness planning coordination coordinated across the region.
- Policy should increase institutions accountability level for cybersecurity.
- Sustainable resilience takes a holistic approach.

References

Dameff, C., Tully, J., Chan, T. C., Castillo, E. M., Savage, S., Maysent, P., ... & Longhurst, C. A. (2023). Ransomware attack associated with disruptions at adjacent emergency departments in the US. JAMA network open, 6(5), e2312270. https://doi:10.1001/jamanetworkopen.2023.12270

McGlave, C. C., Nikpay, S. S., Henning-Smith, C., Rydberg, K., & Neprash, H. T. (2023). Characteristics of short-term acute care hospitals that experienced a ransomware attack from 2016 to 2021. Health Affairs Scholar, 1(3), qxad037. https://doi.org/10.1093/haschl/qxad037

Munoz Cornejo, G., Lee, J., & Russell, B. A. (2024). A thematic analysis of ransomware incidents among United States hospitals, 2016–2022. Health and Technology, 14(6), 1059-1070. https://doi.org/10.1007/s12553-024-00890-3

Neprash, H. T., McGlave, C. C., Rydberg, K., & Henning-Smith, C. (2024). What happens to rural hospitals during a ransomware attack? Evidence from Medicare data. The Journal of Rural Health, 40(4), 728-737. https://doi.org/10.1111/jrh.12834


Thank You