Proceedings of the Informing Science + Information Technology Education Conference

An Official Publication of the Informing Science Institute
InformingScience.org

InformingScience.org/Publications

July 26 – 31, 2026

MITIGATING CYBERSECURITY RISKS IN LEGACY HEALTHCARE SYSTEMS: POLICY, TECHNOLOGY, AND RESPONSE STRATEGIES FOR CRITICAL INFRASTRUCTURE [ABSTRACT]

Angela Wells *	City University of Seattle, Washington, United States	arwells@cityu.edu
Maurice Dawson Jr.	Illinois Institute of Technology, Chicago, Illinois, United States	mdawson2@illinoistech.edu
Philip Adewuyi	Wigwe University, Isiokpo, Nigeria	solaadewuyi@gmail.com
Tony Williams	Ashford University – UAGC	Williamscaddola@gmail.com
Danny Bruce	City University of Seattle Washington, United States	brucedanny@cityu.edu
Samson Quaye	Illinois Institute of Technology, Chicago, Illinois, United States	squaye@hawk.illinoistech.edu

* Corresponding author

ABSTRACT

Aim/Purpose	The purpose of this paper is to mitigate cybersecurity risks that are prevalent in legacy healthcare systems from the perspective of policy, technology, and behavior of critical infrastructure that are involved.
Background	Many healthcare organizations are still depending on outdated legacy IT systems for their day-to-day operations. These legacy IT systems are vulnerable to attacks from external sources. Inability and unwillingness to upgrade infrastructures have left the safety of patients and practitioners to ransomware attacks. So, there is an urgent need to expediate actions in fixing these identifiable lapses in the legacy healthcare systems.

Accepted by Editor Michael Jones | Received: May 14, 2026 | Revised: May 28, 2026 | Accepted: June 2, 2026.

Cite as: Wells, A., Dawson, M., Jr., Adewuyi, P., Williams, T., Bruce, D., & Quaye, S. (2026). Mitigating cybersecurity risks in legacy healthcare systems: Policy, technology, and response strategies for critical infrastructure [Abstract]. In M. Jones (Ed.), *Proceedings of InSITE 2026: Informing Science and Information Technology Education Conference, USA*, Article 32. https://doi.org/10.28945/5797

(CC BY-NC 4.0) This article is licensed to you under a Creative Commons Attribution-NonCommercial 4.0 International License. When you copy and redistribute this paper in full or in part, you need to provide proper attribution to it to ensure that others can later locate this work (and to ensure that others do not accuse you of plagiarism). You may (and we encourage you to) adapt, remix, transform, and build upon the material for any non-commercial purposes. This license does not permit you to use this material for commercial purposes.

Methodology	This work uses open-ended questions with in-depth focus group interviews while observing the participants to gain insights into the causes and effects of the subject matter which is the healthcare system failure. Then, a 5-Dimension risk framework is developed to analyze risks that are associated with legacy healthcare systems, cyberattacks reports, capacity of the concerned healthcare organization to respond to cyberattacks, and the role of infrastructure interdependencies.
Contribution	(i) A 5-Dimension risk framework is introduced to proffer solutions to the issue of cyberattack to improve the backbone of cybersecurity to improve the backbone of cybersecurity to build Healthcare Cyber Resilience Model (HCRM). (ii) An introduction of a 3-layer cybersecurity architecture that encompasses technical controls, training, and reliable backup systems.
Findings	Legacy healthcare systems experiences cyberattack due to technical and latent organizational actions. Strong proactive measures by an organization prevent external cyberattack and make apparent the need for continual infrastructure upgrade as and when due.
Recommendations for Practitioners	This work strongly recommends that upgrade of infrastructure should be carried out as and when necessary by healthcare organizations. Safety of the infrastructure should be tested daily for vulnerabilities and a well-defined action plan must be in place. Backup systems is non-negotiable at all times.
Impact on Society	Strengthening cybersecurity in legacy healthcare systems directly improves patient protection, reduces treatment delays, and increases trust in healthcare services. It also reduces the societal and economic damage caused by cyberattacks.
Future Research	Future studies could seek how AI could be used to monitor hospital systems in real time, compare cybersecurity across different countries, and measure hospital systems failure and recovery rate during cyberattacks.
Keywords	legacy healthcare, cybersecurity, ransomware, AI threats, healthcare cyber resilience model, HCRM

AUTHORS



Angela Wells is a distinguished scholar, innovator, and internationally acclaimed project coordinator. She possesses a Master of Business Administration (MBA) with specialization in Health/Health Care Administration/Management from Ashford University. She is Chief Warrant Officer of Louisiana State Guard Cyber Reserve and InfraGard Board Member of Louisiana, In her quest for growth and development, she attended Harvard University for specialized training at The Harvard Medical School and was certified with Advanced Teaching Skills certificate in 2016. Professionally, she is a Certified Project Management Professional, an Ethics Training for Public Servants Certified, Mediation Worlds, PLLC certified on Basic Mediation, Certified DevOps/Cloud Engineer, and Certified Fraud Examiner. Prof. Angela is an associate faculty (MBA Healthcare Administration) at the City University of Seattle and a visiting lecturer at CETYS University. Her career has been a journey from Education sector to medical sector

to Computing and AI application and integration sectors. She is passionate about women healthcare, robotics, and deployment of AI solutions across underserved communities.



Dr. Maurice E. Dawson Jr., Associate Professor and Director, Illinois Institute of Technology. Maurice E. Dawson Jr. is an Associate Professor of Information Technology and Management and Director of the Center for Cyber Security and Forensics Education (C²SAFE) at Illinois Institute of Technology. He is a multiple-time Fulbright Scholar and Specialist, with international engagements in 2025, 2023, 2021, 2018, 2017, and 2014. He has also served as a U.S. Agency for International Development Visitor Speaker Program participant in 2024 and a United States Department of State U.S. Speaker Program participant in 2023. Dr. Dawson holds multiple advanced degrees, including a Ph.D. in Computing from London Metropolitan University and a Doctor of Computer Science from Colorado Technical University.

His research focuses on cybersecurity, software assurance, artificial intelligence, Internet of Things security, cyber warfare, and critical infrastructure protection. He has more than 25 years of combined academic, government, military, and industry experience, including service with the Iowa National Guard, U.S. Navy Reserve and professional roles with BAE Systems, Rockwell Collins, and higher education institutions. His international work includes cybersecurity education, applied research, training, and capacity building across Africa, Latin America, the Middle East, Europe, and Asia.



Philip Adewuyi bagged his PhD degree in Control Systems Engineering. He has handled various industrial and domestic designs execution across Nigeria. Philip is a seasoned lecturer with supervised undergraduate and postgraduate projects that are multi-disciplinary in nature which informed his deep interest in multi-disciplinary researches. His research interests cut across the use of AI to solving diverse human challenges. He has attended and presented papers in many workshops and conferences. He loves coordinating research projects and presentation, especially, at conferences and workshops. He is a sought-after facilitator at various professional fora. Philip loves traveling and meeting people.



Tony T. Williams is a retired military veteran and community leader. He earned his post graduate in Curriculum Development and Leadership (Ed.S.) from Liberty University, Master of Arts in Health Care Administration (MHA), and Bachelor of Arts (Magna Cum Laude) in Gerontology Nursing, both from Ashford University.He has completed continuous education courses with Harvard, John Hopkins, and Yale in the areas of COVID-19, global health, and pandemic prevention. His military career centered on telecommunication help desk operations, network architecture and security, and overall signal support systems and networks.



Danny L. Bruce is an active duty service member in the United States Army with over 23 years of leadership experience. He currently serves as the operations manager for a field hospital that delivers battlefield medicine to the U.S. Army Pacific Command. He earned his undergraduate degree in biology from Western Kentucky University and is currently enrolled in the Healthcare Administration graduate program at City University of Seattle with an expected graduation date of June 2026. His military education includes graduation from the Licensed Practical Nurse Course, Advanced Leaders Course, Senior Leaders Course, Instructor Trainer Course, and Operations Manager Course.



Samson Quaye is currently pursuing the Ph.D. degree in information technology with the Illinois Institute of Technology, Chicago, IL, USA, where he serves as a Teaching and Research Assistant and is affiliated with the Center for Cybersecurity and Forensics Education (C²SAFE) under the supervision of Dr. Maurice Dawson. He received the M.Sc. degree in applied mathematics from the Illinois Institute of Technology and a double M.Sc. degree in mathematical engineering from the University of L'Aquila, Italy, and the Brno University of Technology, Czech Republic. He obtained the B.Sc. degree in mathematics from the Kwame Nkrumah University of Science and Technology (KNUST), Kumasi, Ghana. His research interests focus on AI security and privacy through robust machine learning, deep learning, and large language models (LLMs). His developing areas include cybersecurity in hyperconnectivity (IoT ecosystems) and threat modeling, with a current focus on malware. His recent work investigates AI-powered cybersecurity models for training and testing IoT devices to enhance intrusion detection capabilities in modern network environments.